AIMS Mathematics, 10(11): 27535–27559.
DOI: 10.3934/math.20251211
Received: 15 September 2025
Revised: 09 November 2025
Accepted: 20 November 2025
Published: 26 November 2025

https://www.aimspress.com/journal/Math

Research article

Various structures of cyclic codes and LCD codes over $GR(p^3, m)[v]/\langle v^2 - p^2\alpha, pv\rangle$

Sami Alabiad*and Alhanouf Ali Alhomaidhi

Department of Mathematics, College of Science, King Saud University, P.O. Box 2455, Riyadh 11451, Saudi Arabia; aalhomaidhi@ksu.edu.sa

* **Correspondence:** Email: ssiaf1@ksu.edu.sa.

Abstract: Let p be a prime and m a positive integer. This paper investigates cyclic and self-dual codes of length n over the local Frobenius non-chain ring $R = \mathrm{GR}(p^3, m)[v]$, with $v^2 = p^2\alpha$, $\alpha \in \mathbb{F}_{p^m}^*$, and $pv = 0$. First, we characterize the algebraic structure of cyclic codes of arbitrary length over R. When $\gcd(n, p) = 1$, explicit generator polynomials are determined, and the corresponding dual and self-orthogonal structures are derived. A key result of this study is the proof that self-dual cyclic codes do not exist over R. In addition, the enumeration formula for cyclic LCD codes is given by $2^{e_1+\frac{e_2}{2}}$. Several examples and tables are provided to illustrate the theoretical findings and the derived mass formulas for cyclic self-orthogonal and LCD codes.

Keywords: frobenius rings; cyclic codes; self-dual codes; LCD codes classes
Mathematics Subject Classification: 16L30, 94B05, 16P20, 94B60

1. Introduction

Cyclic codes are one of the first categories of block codes and have been thoroughly examined over the last sixty years [1]. During this period, research has shown their substantial uses in mathematics and other disciplines. A substantial amount of study on cyclic codes and their generators has been undertaken with the presumption that the ring R is a Frobenius ring, a category that includes Galois rings and finite chain rings, among others. Hammons et al. [2] performed seminal research on cyclic codes over $\mathbb{F}_4$ and $\mathbb{Z}_4$. Gradually, the emphasis broadened to encompass a wider variety of ring classes. The authors of [3] and [4] investigated (self-dual) cyclic codes over $\mathbb{Z}_{p^n}$. Bonnecaze and Udaya [5] examined such codes over $\frac{\mathbb{F}_2[u]}{\langle u^2\rangle}$, whereas Dinh and López-Permouth [6] conducted an extensive analysis of these codes over finite chain rings.

Yildiz and Karadeniz [7] furthered this research by examining cyclic codes within the ring $\frac{\mathbb{F}_2[u,v]}{\langle u^2, v^2, uv - vu\rangle}$, which is a Frobenius non-chain ring. Singh and Kewat [8] analyzed cyclic codes over $\frac{\mathbb{F}_p[u]}{\langle u^k\rangle}$,

obtaining findings on the minimum Hamming distance and minimal generating sets for these codes. Recently, Kim and Lee [9] delineated the generators of all cyclic self-dual codes over $\frac{\mathbb{Z}_2[u]}{\langle u^3\rangle}$ of length 2^k, therefore augmenting the existing literature on self-dual codes.

Self-dual codes and self-orthogonal codes have garnered significant interest from researchers because of their relationships with various mathematical domains, including invariant theory [10], among others. Since the 1970s, extensive study has been conducted on the enumeration of self-dual and self-orthogonal codes (see [11–13]). Linear complementary dual (LCD) codes were initially proposed by Massey in 1992 [14]. These codes have attracted considerable interest owing to their multiple benefits in coding theory and cryptography [15–17]. A significant application of LCD codes is their capacity to offer protection against Side-Channel Attacks (SCAs) and Fault-Injection Attacks (FIAs) in cryptographic systems (see [18]).

Recent years have seen substantial research into the features and architectures of LCD codes across multiple algebraic structures, and the investigation of such codes over non-chain Frobenius rings offers greater structural flexibility and richer enumeration possibilities compared with traditional chain rings. Moreover, these rings naturally support Calderbank–Shor–Steane (CSS) type constructions, which combine pairs of classical linear codes to produce quantum error-correcting codes. This connection, as also demonstrated in [19, 20], highlights how the algebraic framework of non-chain rings contributes to the development of superior quantum and cryptographic code families; for more on LCD over finite rings, see [21–23]. Considering the current literature on non-chain rings [24, 25], it is reasonable to broaden these studies to encompass other semi-local and local non-chain rings.

Building on the existing literature on non-chain rings [26–28], this work extends current investigations to a broader class of local non-chain rings. Motivated by these prior studies, we focus on the finite commutative local non-chain ring $R = \frac{\mathrm{GR}(p^3,m)[v]}{\langle v^2-p^2\alpha,pv\rangle}$, characterized by the relations $v^2 = p^2\alpha$, $p^3 = 0$, and $pv = 0$.

Our contribution lies in extending and refining structural and enumerative techniques for cyclic, LCD, and self-dual codes beyond traditional chain and prime-characteristic settings. By adapting these methods to the mixed and higher-characteristic framework of the local Frobenius non-chain ring R, we uncover new algebraic interactions between its nilpotent and unit components. This approach not only generalizes classical results from simpler base fields, but also establishes a unified methodology for analyzing and enumerating families of cyclic codes over more intricate ring environments, revealing both theoretical depth and practical potential.

We begin by characterizing all ideals of R. Subsequently, we describe diverse constructions of cyclic codes over $R_1 = \frac{\mathrm{GR}(p^2,m)[v]}{\langle v^2,pv\rangle}$ (Theorem 5) for any finite length $n = p^s$. We then derive the generators of cyclic codes over R (Theorem 11) and present additional results for the case $\gcd(n, p) = 1$ (Theorem 12). Furthermore, we establish necessary and sufficient conditions for the existence of self-dual and linear complementary dual (LCD) codes over R. We also enumerate self-orthogonal codes of length n over R with $\gcd(n, p) = 1$, along with LCD codes of identical length. Finally, we demonstrate that these classes of codes offer enumerative advantages (Theorem 13). The ring R has attracted significant attention, with several categories of codes already examined in prior works [24, 26, 29, 30].

This paper is organized as follows: Section 2 presents essential definitions and Gray maps. Section 3 addresses the structure and enumeration of the ring $\frac{GR(p^3,m)[v]}{\langle v^2-p^2\alpha,pv\rangle}$. Section 4 presents an analysis of the

structure of cyclic codes over R of length n and provides an enumeration of self-dual and LCD codes. We first examine the ring $R_1 = GR(p^2, m) + vGR(p^2, m)$ with the condition $v^2 = pv = 0$, focusing on cyclic codes, self-dual codes, and LCD codes defined over this structure. We then present their structures over R for general n, with particular emphasis on the case where $\gcd(n, p) = 1$. Section 5 provides several significant examples of cyclic codes, self-dual codes, and LCD codes over R, which are derived from those over $\mathbb{F}_{p^m}$.

2. Preliminaries

Let p be a prime number and m a positive integer. Throughout this work, we consider the Galois ring $GR(p^3, m)$ as the basic structure. We extend it by adjoining an indeterminate v subject to the relations $v^2 = p^2\alpha$ and $pv = 0$, which gives rise to the ring

$$R = \frac{GR(p^3, m)[v]}{\langle v^2 - \alpha p^2,\ pv\rangle}. \tag{2.1}$$

It was established in [29] that R is a local but non-chain ring, and its unique maximal ideal is generated by p and v, i.e., $M = \langle p, v\rangle$. Every element of $GR(p^3, m)$ can be written in p-adic form as $\beta_0 + p\beta_1 + p^2\beta_2$, where each coefficient belongs to the set $\Gamma(m)$. Consequently, every element of R can be uniquely expressed as $\gamma = \gamma_0 + v\gamma_1$ with $\gamma_0, \gamma_1 \in GR(p^3, m)$, so that R is isomorphic to $GR(p^3, m) + vGR(p^3, m)$.

The group of units of R contains $(p^m - 1)p^{3m}$ elements, while the remaining $p^{4m} - (p^m - 1)p^{3m}$ elements are non-units. An element $\gamma = \gamma_0 + v\gamma_1$ is invertible in R exactly when both γ_0 and γ_1 are nonzero in $GR(p^3, m)$. If ξ is a primitive element of the multiplicative group $\mathbb{F}_{p^m}^*$ of order $p^m - 1$, then each unit u of R can be expressed in the form $u = \omega(1 + p\beta_0 + p^2\beta_1 + v\beta_3)$ with $\omega \in \Gamma^*(m)$ and $\beta_i \in \Gamma(m)$. Here, we denote $\Gamma(m) = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\}$, $\Gamma_1 = \{\xi^{2i+1} : 1 \le i \le \frac{p^m-1}{2} - 1\}$, which corresponds to the set of nonsquares in $\Gamma^*(m)$, and $\Gamma_2 = \{\xi^{2i} : 1 \le i \le \frac{p^m-1}{2} - 1\}$, which corresponds to the set of squares.

A linear code of length n over R is defined as an R-submodule of R^n. In this setting, codewords are vectors of the form $(c_0, c_1, \ldots, c_{n-1})$ with entries from R. The cyclic shift operator π on R^n is defined by $\pi(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2})$. A code C is called cyclic if $\pi(C) = C$. More generally, if the length of a code is mt, then C is said to be quasi-cyclic of index t when $\pi^{(t)}(C) = C$, where $\pi^{(t)}$ denotes the t-fold application of π. The smallest such t is the index of the code, and in particular, cyclic codes are quasi-cyclic codes of index one. Finally, every codeword $(c_0, c_1, \ldots, c_{n-1})$ can be associated with the polynomial $c_0 + c_1 z + \cdots + c_{n-1}z^{n-1}$ in $\mathfrak{R}(R, n) = \frac{R[z]}{\langle z^n-1\rangle}$, which shows that cyclic codes of length n correspond to ideals of $\mathfrak{R}(R, n)$ (cf. [30]).

We consider the module R^n endowed with the standard Euclidean inner product. For a code $C \subseteq R^n$ of length n, its dual is defined as $C^\perp = \{\, y \in R^n : c \cdot y = 0 \text{ for all } c \in C \,\}$. A code is called *self-orthogonal* if $C \subseteq C^\perp$, and *self-dual* if $C = C^\perp$. Moreover, C is said to be a *linear complementary dual (LCD)* code if $C \cap C^\perp = \{0\}$. For a polynomial $\theta(z) \in \mathbb{F}_{p^m}[z]$, the *reciprocal polynomial* is given by $\theta^*(z) = z^{\deg(\theta)}\theta\left(\frac{1}{z}\right)$. It is straightforward to check that for any $\theta(z), \vartheta(z) \in \mathbb{F}_{p^m}[z]$, one has $(\theta(z)\vartheta(z))^* = \theta^*(z)\,\vartheta^*(z)$. This identity also holds in the quotient ring $\mathfrak{R}(\mathbb{F}_{p^m}, n) = \frac{\mathbb{F}_{p^m}[z]}{\langle z^n-1\rangle}$, provided that $\deg(\theta\vartheta) < n$. Now, let C be a cyclic code of length n over R, and let I denote the ideal of $\mathfrak{R}(R, n)$ corresponding to C. Then, the dual code $C^\perp$ is associated with the ideal $\{\, \theta^*(z) : \theta(z) \in \mathrm{Ann}(I) \,\}$.

3. Classification and ideals of the ring R

Recall that an element $x \in R$ is called a *zero-divisor* if there exists a nonzero element $y \in R$ such that $xy = 0$. An element of R that is not a zero-divisor is said to be *regular*. A finite commutative ring R is referred to as a *Frobenius ring* if it is an injective R-module. Equivalently, this condition holds when $\mathrm{Ann}(M) \cong \mathbb{F}_{p^m}$, where I denotes the Jacobson radical of R. In what follows, we focus on the ring $R = \frac{\mathrm{GR}(p^3,m)[v]}{\langle v^2-\alpha p^2,\, pv\rangle}$, which is a finite ring of order p^{4m} with residue field $F = \mathbb{F}_{p^m}$. The structural properties of this ring will be established, as they play a crucial role in the subsequent developments.

Theorem 1. *The ring R is a Frobenius local non-chain ring of order p^{4m}.*

Proof. First, observe that the order of R follows from $R = GR(p^3, m) + vGR(p^3, m)$ together with the relation $pv = 0$. It is then not difficult to verify that $\mathcal{M} = \langle p, v\rangle$, which in turn gives $R/\mathcal{M} \cong \mathbb{F}_{p^m}$. Hence, R is a local but non-chain ring. Furthermore, since the element p^2 annihilates $\mathcal{M} = (p, v)$, particularly because $pv = 0$ and $p^3 = 0$, we deduce that $p^2\mathcal{M} = 0$, and thus $p^2 \in \mathrm{Ann}(\mathcal{M})$. Now, suppose $z \in \mathrm{Ann}(\mathcal{M})$ with $z \neq 0$. Then, $z\mathcal{M} = 0$, which in particular implies $zv = 0$. Consequently, $z \in \langle p\rangle$. Moreover, since $zp = 0$, it follows that $z \in \langle p^2\rangle$. Therefore, $\mathrm{Ann}(\mathcal{M}) = \langle p^2\rangle$, and hence R is a Frobenius ring. □

An exhaustive characterization of all rings $\frac{GR(p^3,m)[v]}{\langle v^2-p^2\alpha,pv\rangle}$ is given by Theorem 2.

Theorem 2. *The classification of R is given in Table 1.*

Table 1. Classes of R.

$p \neq 2$	$p = 2$
$\frac{GR(p^3,m)[v]}{\langle v^2-p^2\alpha,pv\rangle}$	$\frac{GR(8,m)[v]}{\langle v^2-4,2v\rangle}$
$\frac{GR(p^3,m)[v]}{\langle v^2-p^2,pv\rangle}$	

Proof. Elements of R are $\gamma_0 + \gamma_1 v$, where $\gamma_0 \in GR(p^3, m)$ and $\gamma_1 \in \Gamma(m)$. As $pv = 0$, then its minimal polynomial is $g(z) = z^2 - p^2\alpha$, where $\alpha \in \Gamma^*(m)$. Now suppose $p = 2$. Because $\gcd(2, 2^m - 1) = 1$, thus $(\Gamma(m))^2 = \Gamma(m)$, and hence there is unique class of such rings, represented by $\frac{GR(8,m)[v]}{\langle v^2-4,2v\rangle}$. □

From now on, we assume that $p \neq 2$. Consider the usual partition on $\Gamma^*(m)$ by Γ_1 and Γ_2. It is worth noting that $|\Gamma_1| = \frac{p^m-1}{2} = |\Gamma_2|$. We next proceed with the proof with two cases.

Case a. We show that $\frac{GR(p^3,m)[v]}{\langle v^2-p^2\xi,pv\rangle}$ and $\frac{GR(p^3,m)[v]}{\langle v^2-p^2,pv\rangle}$ are not isomorphic, that is, they are not in the same class when $\xi \in \Gamma_1$. In contrast, suppose that they are isomorphic, and let ϕ be the ismorphism. Assuming the radical is $\langle p, v\rangle$, and for some $\gamma \in \Gamma^*(m)$, set $\phi(v) = \gamma v$. Note that $(\phi(v))^2 = \phi(v^2)$, and so $(\gamma v)^2 = \phi(p^2\xi)$. This implies that $\gamma^2 v^2 = p^2\phi(\xi)$, and also $\gamma^2(p^2) = p^2\phi(\xi)$. Consequently, $p^2\gamma^2 = p^2\phi(\xi)$, thus $\gamma^2 = \phi(\xi)$. We have $\phi(\xi) = \xi$, because ϕ restricted to $\Gamma(m)$ is a fixed isomorphism. Furthermore, because $p \neq 2$, this contradicts the assumption about ξ, and thus $\xi \neq \gamma^2$. Therefore, the result follows.

Case b. When $\alpha \in \Gamma_3$. In such a case, there exists $\gamma \in \Gamma^*(m)$ such that $\alpha = \gamma^2$. Observe $g(z) = z^2 - p^2\alpha = z^2 - p^2\gamma^2 = \gamma^2[(\gamma^2)^{-1}z^2 - p^2] = \gamma^2[(\gamma^{-1}z)^2 - p^2]$. As v is a root of $g(z)$, then $g(v) = 0$, and

hence $v^2 - p^2\alpha = 0$. From the above argument, $\gamma^2[(\gamma^{-1}v)^2 - p^2] = 0$. Thus, $(\gamma^{-1}v)^2 - p^2 = 0$. This suggests that $g(z)$ can take $g(z) = z^2 - p^2$. This ends the argument. To sum up, we have two classes of such rings that are not isomorphic:

$$\Omega_1 : \text{ All rings with associated polynomials } g(z) = z^2 - p^2\alpha, \text{ where } \alpha \in \Gamma_1;$$
$$\Omega_2 : \text{ All rings with associated polynomials } g(z) = z^2 - p^2\alpha, \text{ where } \alpha \in \Gamma_2.$$

The first class is represented by

$$\frac{GR(p^3, m)[v]}{\langle v^2 - p^2\xi, pv\rangle}, \tag{3.1}$$

and the second class is represented by

$$\frac{GR(p^3, m)[v]}{\langle v^2 - p^2, pv\rangle}. \tag{3.2}$$

Now, every unit u of R is of the form,

$$u = \gamma_0 + p\gamma_1 + p^2\gamma_2 + v\gamma_3, \tag{3.3}$$

where $\gamma_0 \in \Gamma^*(m)$.

Theorem 3. *The ideals of R are given by the following lattice:*

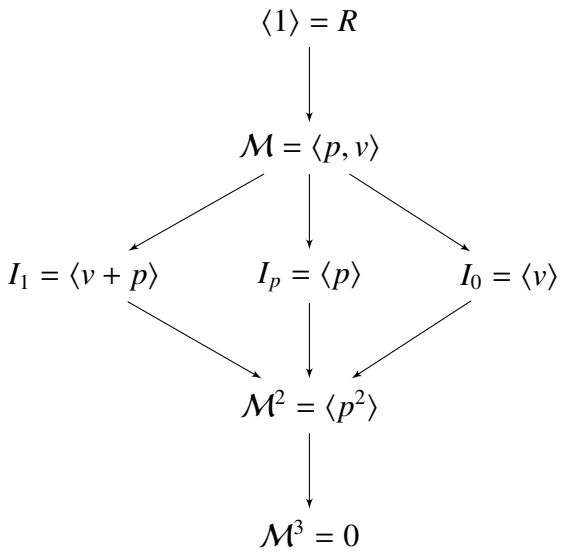


Figure 1. Lattice of ideals of R.

Proof. Since every element of a proper ideal of R is of the form $p\gamma_1 + p^2\gamma_2 + v\gamma_3$, where γ_1, γ_2 and γ_3 are in $\Gamma(m)$, the equation $v^2 = p^2\alpha$ forces $\langle p^2, v\rangle = \langle p^2 + v\rangle = \langle v\rangle$. Thus, we are left with proper ideals M, $\langle p\rangle$, $\langle v\rangle$, $\langle p + v\rangle$, $\langle p^2\rangle$ and 0. □

4. Various structures of cyclic codes over R

First, we define $\mathfrak{R}(R, n)$ as $\frac{R[z]}{\langle z^n - 1\rangle}$. In the subsequent analysis, we examine the fundamental structural characteristics of $\mathfrak{R}(R, n)$ along with the generators of its ideals. A prime ideal P in a commutative ring

R is defined as *minimal* if the only prime ideal of R that is contained within P is P itself. A commutative ring where every prime ideal is also a maximal ideal is defined as a zero-dimensional ring, indicating that it has a Krull dimension of zero. In the context of commutative rings, if a ring R is characterized by not being zero-dimensional while simultaneously ensuring that every prime ideal within it is classified as either minimal or maximal, it follows that R is defined to possess a Krull dimension of one. Given that R possesses a Krull dimension of 0, it can be concluded that $R[z]$ has $\mathcal{M}R[z]$ as its maximal ideal, which consequently indicates that the dimension of $R[z]$ is 1. Additionally, since $z^n - 1 \notin \mathcal{M}R[z]$, we can deduce that $\mathfrak{R}(R, n)$ is a zero-dimensional ring.

Lemma 1. *The units of* $\mathfrak{R}(R, n)$ *are*

$$\gamma_1(z) + \gamma_2(z)p + \gamma_3(z)p^2 + v\gamma_4(z), \tag{4.1}$$

where $\gamma_1(z) \neq 0, \gamma_2(z), \gamma_3(z)$, *and* $\gamma_4(z)$ *belong to* $\mathfrak{R}(\mathbb{F}_{p^m}, n)$.

Proof. Suppose $\alpha(z)$ is a unit. Then, it can be expressed as

$$\alpha(z) = \gamma_1(z) + p\gamma_2(z) + p^2\gamma_3(z) + v\gamma_4(z), \tag{4.2}$$

with $\gamma_1(z), \gamma_2(z), \gamma_3(z), \gamma_4(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$. Since $\alpha(z)$ is a unit, it must be a regular element of $\mathfrak{R}(R, n)$. Consequently, $\gamma_1(z)$ cannot divide $z^n - 1$. Indeed, suppose there exists $\beta(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$ such that $\gamma_1(z)\beta(z) = z^n - 1$. Then, it would follow that $\beta(z)\alpha(z) = 0$. If $\beta(z) \neq 0$, this would force $\alpha(z)$ to be a zero-divisor, contradicting the assumption that $\alpha(z)$ is a unit. Thus, we must have $\beta(z) = 0$, which implies that $\deg(\gamma_1) = 0$ and $\gamma_1(z) \neq 0$.

Conversely, suppose $\alpha(z) = \gamma_1(z) + \gamma_2(z)p + \gamma_3(z)p^2 + v\gamma_4(z)$, where $\gamma_1(z), \gamma_2(z), \gamma_3(z), \gamma_4(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$, and assume either that $\deg(\gamma_1(z)) = 0$ with $\gamma_1(z) \neq 0$, or that $\gamma_1(z) \nmid z^n - 1$. In either case, $\gamma_1(z)$ is a regular element of $\mathfrak{R}(\mathbb{F}_{p^m}, n)$, and therefore $\alpha(z)$ is regular in $\mathfrak{R}(R, n)$, which means $\alpha(z)$ is a unit. □

Representation (A)

Let $\theta_i(z)$ be in $\mathfrak{R}(\mathbb{F}_{p^m}, n)$, and suppose that $\hat{\theta}_i(z) = \frac{z^n-1}{\theta_i(z)}$. Also, let I be an ideal in $\mathfrak{R}(R, n))$ with the following form:

$$\begin{aligned} I = \langle\, & \theta_0(z) + p\vartheta_1(z) + v\vartheta_2(z) + p^2\vartheta_3(z), \\ & p\theta_1(z) + v\vartheta_4(z) + p^2\vartheta_5(z), \\ & v\theta_2(z) + p^2\vartheta_6(z), \\ & p^2\theta_3(z)\rangle. \end{aligned} \tag{4.3}$$

(i) Conditions involving $\theta_1(z)$:

$$\begin{cases} \theta_1(z) \mid \theta_0(z) \mid (z^n - 1), \quad \deg(\vartheta_1) < \deg(\theta_1) \text{ or } \vartheta_1(z) = 0, \\ \theta_1(z) \mid \vartheta_1(z)\,\hat{\theta}_0(z), \end{cases}$$

(ii) Conditions involving $\theta_2(z)$:

$$\begin{cases} \theta_2(z) \mid \theta_0(z), & \deg(\vartheta_4) < \deg(\theta_2) \text{ or } \vartheta_4(z) = 0, \\ \theta_2(z) \mid \vartheta_4(z)\,\hat{\theta}_1(z), & \deg(\vartheta_2) < \deg(\gcd(\vartheta_4, \theta_2)) \text{ or } \vartheta_2(z) = 0, \\ \theta_2(z) \mid \vartheta_2(z)\,\hat{\theta}_0(z)\hat{\theta}_1(z), & \end{cases}$$

(iii) Conditions involving $\theta_3(z)$:

$$\begin{cases} \theta_3(z) \mid \theta_i(z), \quad i = 0, 1, 2, & \deg(\vartheta_6) < \deg(\theta_3) \text{ or } \vartheta_6(z) = 0, \\ \theta_3(z) \mid \vartheta_6(z)\,\hat{\theta}_3(z), & \deg(\vartheta_5) < \deg(\gcd(\vartheta_6, \theta_3)) \text{ or } \vartheta_5(z) = 0, \\ \theta_3(z) \mid \vartheta_5(z)\,\hat{\theta}_1(z)\hat{\theta}_2(z), & \deg(\vartheta_3) < \deg(\gcd(\vartheta_5, \vartheta_6, \theta_3)) \text{ or } \vartheta_3(z) = 0, \\ \theta_3(z) \mid \vartheta_3(z)\,\hat{\theta}_0(z)\hat{\theta}_1(z)\hat{\theta}_2(z). & \end{cases}$$

Assume $\eta_v : R \longrightarrow GR(p^2, m)$ is the mapping such that $\eta_v(r) = \bar{r} = r \pmod{v}$. Since $v^2 = p^2\alpha = 0$, it follows that the images of η_v lie in $R_1 = \frac{GR(p^2,m)[v]}{\langle v^2, pv\rangle}$. Our next goal is to identify the generators of cyclic codes over $GR(p^2, m)$. Using this foundation, we explicitly describe the generator structures of the ideals in $\mathfrak{R}(R, n)$, which represent cyclic codes over R. Initially, no assumption is made regarding $\gcd(n, p) = 1$. However, by later imposing this condition, the algebraic structure becomes more manageable, facilitating the analysis of these codes.

4.1. Constructions of cyclic codes over R_1

In this section, we present structural results concerning cyclic codes of length n over

$$R_1 = \frac{GR(p^2, m)[v]}{\langle v^2, pv\rangle}.$$

Theorem 4. *Let C be a cyclic code of length n defined over R_1. Then, C can be described by a generating set of the form*

$$C = \langle \theta_0(z) + p\vartheta_1(z) + v\vartheta_2(z),\ p\theta_1(z) + v\vartheta_3(z),\ v\theta_2(z)\rangle. \tag{4.4}$$

Proof. Define the natural homomorphism

$$\eta_v : \mathfrak{R}(R_1, n) \longrightarrow \mathfrak{R}(GR(p^2, m), n) \tag{4.5}$$

by extending linearly as

$$\eta_v(\gamma_0(z) + p\gamma_1(z) + v\gamma_2(z)) = \gamma_0(z) + p\gamma_1(z), \tag{4.6}$$

for all $\gamma_0(z), \gamma_1(z), \gamma_2(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$. Then, $\ker(\eta_v) \cap C$ forms an $\mathfrak{R}(\mathbb{F}_{p^m}, n)$-submodule of $v\mathfrak{R}(\mathbb{F}_{p^m}, n)$. Consequently, there exists some $\theta_2(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$ with $\theta_2(z) \mid (z^n - 1)$ such that

$$\ker(\eta_v) \cap C = \langle v\theta_2(z)\rangle.$$

Since η_v is surjective, the image $\eta_v(C)$ is an ideal of $\mathfrak{R}(GR(p^2, m), n)$. By Theorem 4,

$$\eta_v(C) = \langle \theta_0(z) + p\vartheta_1(z),\ p\theta_1(z)\rangle$$

for some $\theta_0(z), \theta_1(z), \vartheta_1(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$ satisfying Representation (A). This implies $\theta_1(z) \mid \theta_0(z)$ and $\theta_1(z) \mid \vartheta_1(z)\hat{\theta}_0(z)$, with either $\deg(\vartheta_1) < \deg(\theta_1)$ or $\vartheta_1(z) = 0$.

Hence, we can express

$$C = \langle \theta_0(z) + p\vartheta_1(z) + v\vartheta_2(z),\ p\theta_1(z) + v\vartheta_3(z),\ v\theta_2(z) \rangle,$$

for some $\vartheta_i(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$, noting that $v\theta_0(z) = v(\theta_0(z) + p\vartheta_1(z)) \in \ker(\eta_v) \cap C = \langle v\theta_2(z) \rangle$.

Next, define the map $\eta_p : \mathfrak{R}(R_1, n) \to \mathfrak{R}(\mathbb{F}_{p^m} + v\mathbb{F}_{p^m}, n)$ as

$$\eta_p(\gamma_0(z) + p\gamma_1(z) + v\gamma_2(z)) = \gamma_0(z) + v\gamma_2(z),$$

for each $\gamma_0(z), \gamma_1(z), \gamma_2(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$. A similar argument shows that

$$\eta_p(C) = \langle \theta_0(z) + v\vartheta_2(z),\ v\vartheta(z) \rangle,$$

where $\vartheta(z) = \gcd(\vartheta_3(z), \theta_2(z))$, which implies $\deg(\vartheta_2) < \deg(\gcd(\vartheta_3(z), \theta_2(z)))$.

Finally, it follows that

$$v\vartheta_3(z)\hat{\theta}_0(z)\hat{\theta}_1(z) = \hat{\theta}_0(z)\hat{\theta}_1(z)\hat{\theta}_2(z)[\theta_0(z) + p\vartheta_1(z) + v\vartheta_2(z)],$$

and

$$v\vartheta_3(z)\hat{\theta}_1(z)\hat{\theta}_2(z) = \hat{\theta}_0(z)\hat{\theta}_1(z)[p\theta_1(z) + v\vartheta_3(z)],$$

which implies $\theta_2(z) \mid \vartheta_2(z)\hat{\theta}_0(z)\hat{\theta}_1(z)$ and $\theta_2(z) \mid \vartheta_3(z)\hat{\theta}_1(z)$.

Thus, with Representation (A) satisfied, we conclude

$$C = \langle \theta_0(z) + p\vartheta_1(z) + v\vartheta_2(z),\ p\theta_1(z) + v\vartheta_3(z),\ v\theta_2(z) \rangle.$$

□

If we set $n = p^s$, then $z-1$ is nilpotent in $\mathfrak{R}(R_1, p^s)$, with $(z-1)^{2p^s} = 0$. Consequently, every element of $\mathfrak{R}(R_1, p^s)$ can be expressed as a polynomial in $z-1$ with coefficients in $\mathbb{F}_{p^m}$. In particular, this applies to the polynomials $\theta_0(z)$, $\vartheta_i(z)$, $\theta_1(z)$, and $\theta_2(z)$. Therefore, we obtain specific structural results for this case.

Corollary 1. *Assume C is a cyclic code in $\mathfrak{R}(R_1, p^s)$. Then, Representation (A) has the form*

$$C = \langle (z-1)^a + p(z-1)^{t_0}\theta_0(z) + v(z-1)^{t_1}\theta_1(z), p(z-1)^b + v(z-1)^{t_2}\theta_2(z), v(z-1)^c \rangle, \tag{4.7}$$

where

$$\begin{cases} 0 \le a < p^s, \\ 0 \le b \le min\{p^{s-1}, a\}, a + b \le p^s \quad and \quad t_0 + deg(\theta_0) < b, \\ 0 \le c \le a \quad and \quad t_1 + deg(\theta_1) < c, t_2 + deg(\theta_2) < c, \\ \theta_i(z) \quad are\ either\ zeros\ or\ units. \end{cases}$$

Assume that $\chi = p$ or $\chi = v$, and that $\iota_\chi = b$ or $\iota_\chi = p^s - a$. For a polynomial

$$\gamma(z) = \chi(z-1)^t \sum_{i=0} \gamma_i (z-1)^i \in \mathfrak{R}(R_1, p^s),$$

we define its *dual* as

$$\gamma^\perp(z) = \sum_{i=0}^{\iota_\chi - 1} \left(\sum_{j=0}^{i} (-1)^{a+t+j+1} \binom{a+d-t-j}{i-j} \gamma_j \right) (z-1)^i,$$

where $d = \min\{b, c\}$.

Moreover, let

$$\delta = \begin{cases} (-1)^{p^{s-1}-d}, & \text{if } p^{s-1} - d < b, \\ 0, & \text{otherwise.} \end{cases}$$

We now describe the structure of $C^\perp$ for any cyclic code of length p^s over R_1. Note that in $\mathfrak{R}(R_1, p^s)$ we have

$$(z-1)^{p^s} = -p(z-1)^{p^{s-1}} \vartheta(z), \tag{4.8}$$

where $\vartheta(z) \in U(\mathfrak{R}(R_1, p^s))$ is a unit. This relation implies that

$$p(z-1)^{p^s} = 0 \quad \text{and} \quad v(z-1)^{p^s} = 0.$$

Theorem 5. *Suppose C is an ideal of $\mathfrak{R}(R_1, p^s)$. Then, its dual $C^\perp$ can be represented as*

$$\begin{aligned} C^\perp = \langle &(z-1)^{p^s-d} + p\delta(z-1)^{p^{s-1}-d} - p(z-1)^{p^s-a-d+t_0}\theta_0^\perp(z) \\ &- v(z-1)^{p^s-a-d+t_1}\theta_1^\perp(z), p(z-1)^b, v(z-1)^{p^s-a} \rangle, \end{aligned}$$

where $\theta_0^\perp(z)$ and $\theta_1^\perp(z)$ are the duals of the polynomials $\theta_0(z)$ and $\theta_1(z)$, respectively over $\mathbb{F}_{p^m}$.

Proof. Suppose that C is uniquely represented by the polynomial generators of the form $g_1(z) = (z-1)^a + p(z-1)^{t_0}\theta_0(z) + v(z-1)^{t_1}\theta_1(z)$, $g_2(z) = p(z-1)^b + v(z-1)^{t_2}\theta_2(z)$, and $g_3(z) = v(z-1)^c$. Then, it is easy to verify the following:

$$g_1(z)\Big[(z-1)^{p^s-d} + p\delta(z-1)^{p^{s-1}-d}\vartheta(z) - p(z-1)^{p^s-a-d+t_0}\theta_0(z) - v(z-1)^{p^s-a-d+t_1}\theta_1(z)\Big] = 0,$$

Moreover, $g_1(z)(p(z-1)^b) = 0$ and $g_1(z)(v(z-1)^{p^s-a}) = 0$. Since $\mathrm{Ann}(C)$ is an ideal of $\mathfrak{R}(R_1, p^s)$, then $I = \langle G_1(z), G_2(z), G_3(z) \rangle \subseteq \mathrm{Ann}(C)$, where

$$\begin{cases} G_1(z) = (z-1)^{p^s-d} + p\delta(z-1)^{p^{s-1}-d}\vartheta(z) \\ \qquad\qquad - p(z-1)^{p^s-a-d+t_0}\theta_0(z) - v(z-1)^{p^s-a-d+t_1}\theta_1(z), \\ G_2(z) = p(z-1)^b, \\ G_3(z) = v(z-1)^{p^s-a}. \end{cases}$$

Observe that $\eta_v(\mathrm{Ann}(C)) = \mathrm{Ann}(\eta_v(C))$, and thus $\mathrm{Ann}(C) = \langle l_1(z), l_2(z), l_3(z)\rangle$. By the nature of the map η_v, we get such that $\eta_v(l_i(z)) = \eta_v(G_i(z))$, more explicitly,

$$\begin{cases} l_1(z) = (z-1)^{p^s-d} + p\delta(z-1)^{p^{s-1}-d}\vartheta(z) - p(z-1)^{p^s-a-d+t_0}\theta_0(z) + v(z-1)^{t_1'}\theta_1'(z), \\ l_2(z) = p(z-1)^b + v(z-1)^{t_2'}\theta_2'(z), \\ l_3(z) = v(z-1)^{c'}, \end{cases}$$

where $\theta_1'(z)$ and $\theta_2'(z)$ are arbitrary elements of $\mathfrak{R}(R_1, p^s)$ with $t_i' + \deg(\theta_i') < c'$ for $i = 1, 2$. Compatibility with the generators $g_i(z)$ forces $c' = p^s - a$, $t_1' = p^s - a - d + t_1$, $\theta_1'(z) = -\theta_1(z)$, and $\theta_2'(z) = 0$. Therefore, $\mathrm{Ann}(C) = I$. Finally, since $b < p^{s-1}$ and $d = \min\{b, c\}$, then $d \leq b < p^{s-1}s$. It follows that $ip^{s-1} - d > b$ for $i > 1$. Consequently, the dual code $C^\perp$ is given by

$$\begin{aligned} C^\perp = \langle &(z-1)^{p^s-d} + p\delta(z-1)^{p^{s-1}-d} - p(z-1)^{p^s-a-d+t_0}\theta_0^\perp(z) \\ &- v(z-1)^{p^s-a-d+t_1}\theta_1^\perp(z), p(z-1)^b, v(z-1)^{p^s-c}\rangle. \end{aligned}$$

□

We now turn to the characterization of self-dual codes when $p \neq 2$. Assume that C is a self-dual code over R_1 of length p^s. In this situation, it follows that $a + c = p^s$, which further implies $b = c$ since $a + b \leq p^s$. Hence, we have $d = c = b$. Moreover, if $\delta = 0$, then we obtain

$$\left((z-1)^{p^s-d}\right)^2 = (z-1)^{2p^s-2d} = -p(z-1)^{p^s+p^{s-1}-2d}\vartheta_1(z) = 0,$$

where $\vartheta_1(z) \in U(\mathfrak{R}(R_1, p^s))$ is a unit. Therefore, we have the following result.

Theorem 6. *Let C be a cyclic code over R_1 of length p^s with $\delta = 0$. Then, C is self-dual if and only if it admits the representation*

$$C = \langle (z-1)^{p^s-b},\ p(z-1)^b,\ v(z-1)^b\rangle.$$

However, when $\delta \neq 0$, the term $(z-1)^{2p^s-2d}$ may no longer vanish. Indeed, we have

$$(z-1)^{2p^s-2d} = -p(z-1)^{p^s+p^{s-1}-2d}\vartheta_1(z).$$

Therefore, for odd primes p and $\gamma = 2^{-1}$, it follows that

$$(z-1)^{2p^s-2d} + p(z-1)^{p^s+p^{s-1}-2d} = \left((z-1)^{p^s-d} + p\gamma(z-1)^{p^{s-1}-d}\right)^2 = 0.$$

Theorem 7. *Assume that p is an odd prime and $\delta \neq 0$. A cyclic code C over R_1 is self-dual precisely when it can be represented as*

$$C = \langle (z-1)^{p^s-b} + p\gamma(z-1)^{p^{s-1}-b},\ p(z-1)^b,\ v(z-1)^b\rangle.$$

Theorem 8. *Over R_1, the only LCD cyclic code of length p^s is the trivial code $C = 0$.*

Proof. Suppose that C is a cyclic LCD code. Since $p(z-1)^b \in C \cap C^\perp$ and $v(z-1)^e \in C \cap C^\perp$, where $e = \max\{c, p^s - a\}$, it follows that $b = p^s$ and $c = p^s$. Consequently, we must also have $a = p^s$, which implies $C = 0$.

The converse is immediate, as the zero code is trivially LCD. □

Theorem 9. *Let C be a cyclic code of length p^s over R_1. Then, C is proper self-orthogonal precisely when $C = 0$.*

Proof. Suppose that C is a self-orthogonal cyclic code, so that $C \subseteq C^{\perp}$. From the general structure of cyclic codes of length p^s, we have $a + c = p^s$, which implies that $C^{\perp} = \langle G(z),\ p(z-1)^b,\ v(z-1)^c \rangle$, where $G(z) = (z-1)^{p^s-d} + p\delta(z-1)^{p^{s-1}-d}\vartheta(z) - p(z-1)^{p^s-a-d+t_0}\theta_0^{\perp}(z) - v(z-1)^{p^s-a-d+t_1}\theta_1^{\perp}(z)$. Let $g(z) = (z-1)^a + p(z-1)^{t_0}\theta_0(z) + v(z-1)^{t_1}\theta_1(z) \in C^{\perp}$. Then, there exist $\gamma_1(z), \gamma_2(z) \in \mathfrak{R}(R_1, p^s)$ such that $g(z) = G(z) + p(z-1)^b\gamma_1(z) + v(z-1)^c\gamma_2(z)$. Consequently, $G(z) = g(z) - p(z-1)^b\gamma_1(z) - v(z-1)^c\gamma_2(z) \in C$, which shows that $C^{\perp} \subseteq C$. Combining this with $C \subseteq C^{\perp}$, we conclude that $C = C^{\perp}$. Therefore, no non-trivial proper self-orthogonal cyclic code exists.

The converse is immediate since $\mathrm{Ann}(0) = \mathfrak{R}(R_1, p^s)$. □

4.2. Structures of cyclic codes over R

In this section, we investigate the algebraic description of cyclic codes of length n over R, extending the framework of cyclic codes over R_1 established in Theorem 4.

Theorem 10. *Every cyclic code of length n over R admits a representation of the form given in Representation (A).*

Proof. Define the homomorphism

$$\eta_v : \mathfrak{R}(R_1, n) \longrightarrow \mathfrak{R}(GR(p^2, m), n)$$

by setting

$$\eta_v(\gamma_0 + p\gamma_1 + v\gamma_2) = \gamma_0 + p\gamma_1,$$

for all $\gamma_0, \gamma_1, \gamma_2 \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$. For a cyclic code C over R_1, the intersection $\ker(\eta_v) \cap C$ is an $\mathfrak{R}(\mathbb{F}_{p^m}, n)$-submodule contained in $v\mathfrak{R}(\mathbb{F}_{p^m}, n)$. Hence, there exists some $\theta_2(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$ with $\theta_2(z) \mid (z^n - 1)$ such that

$$\ker(\eta_v) \cap C = \langle v\theta_2(z) \rangle.$$

Since η_v is surjective, its image $\eta_v(C)$ is an ideal of $\mathfrak{R}(GR(p^2, m), n)$, which by Theorem 4 takes the form $\langle \theta_0(z) + p\vartheta_1(z), p\theta_1(z) \rangle$ for some $\theta_0(z), \theta_1(z), \vartheta_1(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$ satisfying Representation (A). It follows that C can be expressed as

$$C = \langle \theta_0(z) + p\vartheta_1(z) + v\vartheta_2(z),\ p\theta_1(z) + v\vartheta_4(z),\ v\theta_2(z) \rangle. \tag{4.9}$$

Next, consider a cyclic code C over R of length p^s and define the map $\eta_{p^2} : \mathfrak{R}(R, n) \to \mathfrak{R}(R_1, n)$ by $\eta_{p^2}(\gamma_0 + p\gamma_1 + p^2\gamma_2 + v\gamma_3) = \gamma_0 + p\gamma_1 + v\gamma_3$ for each $\gamma_0, \gamma_1, \gamma_2, \gamma_3 \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$. Then,

$$\eta_{p^2}(C) = \langle \theta_0(z) + p\vartheta_1(z) + v\vartheta_2(z),\ p\theta_1(z) + v\vartheta_3(z),\ v\theta_2(z) \rangle,$$

and hence

$$C = \left\langle \theta_0(z) + p\vartheta_1(z) + v\vartheta_2(z) + p^2\vartheta_3(z), p\theta_1(z) + v\vartheta_4(z) + p^2\vartheta_5(z),\ v\theta_2(z) + p^2\vartheta_6(z),\ p^2\theta_3(z) \right\rangle,$$

for some $\theta_3(z), \vartheta_3(z), \vartheta_5(z), \vartheta_6(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$. Letting $\vartheta(z) = \gcd(\vartheta_6(z), \theta_3(z))$, we obtain $\eta_{p^2}(C) = \langle \theta_0(z) + p\vartheta_1(z) + v\vartheta_2(z),\ p\theta_1(z) + v\vartheta_4(z),\ v\vartheta(z) \rangle$ with $\deg(\vartheta_4) < \deg(\theta_2)$.

By Theorem 4, $\theta_1(z) \mid \theta_0(z) \mid z^n - 1$, which extends to $\theta_2(z) \mid \theta_0(z)$ and $\theta_3(z) \mid \theta_0(z)$ via the map η_{p^2}. Furthermore, $\theta_1(z) \mid \vartheta_1(z)\hat{\theta}_0(z)$. Considering the map $\eta_p : \mathfrak{R}(R,n) \to \mathfrak{R}(\mathbb{F}_{p^m} + v\mathbb{F}_{p^m}, n)$, a similar argument gives $\eta_p(C) = \langle \theta_0(z) + v\vartheta_2(z), v\vartheta_4(z), v\theta_2(z)\rangle$, which reduces to $\eta_p(C) = \langle \theta_0(z) + v\vartheta_2(z), v\vartheta(z)\rangle$ with $\vartheta(z) = \gcd(\vartheta_4(z), \theta_2(z))$, implying $\deg(\vartheta_2) < \deg(\gcd(\vartheta_4, \theta_2))$. Similarly, it can be shown that $\theta_2(z) \mid \vartheta_4(z)\hat{\theta}_1(z)$ and $\theta_2(z) \mid \vartheta_2(z)\hat{\theta}_0(z)\hat{\theta}_1(z)$. Moreover, the elements $p^2\vartheta_3(z)\hat{\theta}_0(z)\hat{\theta}_1(z)\hat{\theta}_2(z)$, $p^2\vartheta_5(z)\hat{\theta}_1(z)\hat{\theta}_2(z)$, and $p^2\vartheta_6(z)\hat{\theta}_2(z)$ all lie in $\langle p^2\theta_3(z)\rangle$, which ensures that $\theta_3(z) \mid \vartheta_3(z)\hat{\theta}_0(z)\hat{\theta}_1(z)\hat{\theta}_2(z)$, $\theta_3(z) \mid \vartheta_5(z)\hat{\theta}_1(z)\hat{\theta}_2(z)$, and $\theta_3(z) \mid \vartheta_6(z)\hat{\theta}_2(z)$. This establishes the representation of any cyclic code over R of length n as claimed. □

4.3. Cyclic codes and their dual codes over R of length n when $\gcd(n, p) = 1$.

In this subsection, we show that if $\gcd(n, p) = 1$, the set of generators of the ideal corresponding to a cyclic code C over R of length n, as given in Theorem 10, can be expressed in a simplified form. Utilizing this reduced generating set, we provide an explicit description of the dual code $C^{\perp}$, compute the cardinality of C, and determine the total number of self-orthogonal codes of length n over R.

For the remainder of this work, unless otherwise specified, the polynomials

$$\theta_0(z), \theta_1(z), \theta_2(z), \theta_3(z), \vartheta_1(z), \vartheta_2(z), \vartheta_3(z), \vartheta_4(z), \vartheta_5(z), \vartheta_6(z)$$

are assumed to lie in $\mathfrak{R}(\mathbb{F}_{p^m}, n)$ and to satisfy Representation (A). Throughout, we adopt the standing assumption that $\gcd(n, p) = 1$.

Lemma 2. *Suppose C is a cyclic code over R.*

(i) For any $\gamma_1(z), \gamma_2(z), \gamma_3(z), \gamma_4(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$*, we have* $\gamma_1(z) \in \langle \gamma_1(z) + p\gamma_2(z) + p^2\gamma_3(z) + u\gamma_4(z)\rangle$*. Particularly, it follows that*

$$\langle \gamma_1(z), p\gamma_2(z) + p^2\gamma_3(z) + u\gamma_4(z)\rangle = \langle \gamma_1(z) + p\gamma_2(z) + p^2\gamma_3(z) + u\gamma_4(z)\rangle.$$

(ii) In $\mathfrak{R}(R, n)$*, we have*

$$\begin{aligned}&\Big\langle \theta_0(z) + p\vartheta_1(z) + v\vartheta_2(z) + p^2\vartheta_3(z),\\ &\ p\theta_1(z) + v\vartheta_4(z) + p^2\vartheta_5(z),\\ &\ v\theta_2(z) + p^2\vartheta_6(z),\\ &\ p^2\theta_3(z)\Big\rangle = \Big\langle \theta_0(z) + p\theta_1(z) + v\vartheta_4(z) + p^2\vartheta_5(z), v\theta_2(z), p^2\theta_3(z)\Big\rangle.\end{aligned}$$

Proof. For (i), let $z^n - 1 = \alpha_0(z)\cdots\alpha_m(z)$ be the prime factorization in $\mathbb{F}_{p^m}[z]$. This factorization is unique up to units, and by Hensel's lemma, each $\alpha_i(z)$ is irreducible in R. As $\gcd(n, p) = 1$, $z^n - 1$ has no repeated factors, so $\alpha_i(z) \neq \alpha_j(z)$ for $i \neq j$. By the Chinese Remainder Theorem, $\mathfrak{R}(\mathbb{F}_{p^m}, n) \cong R_1 \times \cdots \times R_m$, where $R_i = \frac{\mathbb{F}_{p^m}[z]}{\langle \alpha_i(z)\rangle}$ is a field. Hence, $\mathfrak{R}(R, n) \cong \prod_{i=1}^{m}(R_i + pR_i + p^2R_i + uR_i)$. Now, write $\gamma_i(z) = (\gamma_{i1}(z), \ldots, \gamma_{im}(z))$ with $\gamma_{ij}(z) \in R_j$. If $\gamma_{1j}(z) \neq 0$, then γ_{1j} is a unit of R_j, so

$$\gamma_{1j} = (\gamma_{1j} + p\gamma_{2j} + p^2\gamma_{3j} + v\gamma_{4j})^{p^2}\gamma_{1j}^{1-p^2} \in \langle \gamma_{1j} + p\gamma_{2j} + p^2\gamma_{3j} + v\gamma_{4j}\rangle.$$

If $\gamma_{1j} = 0$, then clearly $\gamma_{1j} \in \langle \gamma_{1j} + p\gamma_{2j} + p^2\gamma_{3j} + v\gamma_{4j}\rangle$. Therefore, $\gamma_1(z) \in \langle \gamma_1(z) + p\gamma_2(z) + p^2\gamma_3(z) + v\gamma_4(z)\rangle$, and the first statement follows. The second statement is immediate from the first.

For (ii), all conditions of Representation (A) hold. Since $z^n - 1$ factors into distinct irreducibles, $\gcd(\theta_1(z), \hat{\theta}_0(z)) = 1$, so $\theta_1(z) \mid \vartheta_1(z)$. If $\deg(\theta_1) > 0$ and $\vartheta_1(z) \neq 0$, then $\deg(\vartheta_1) < \deg(\theta_1)$ by Theorem 10, a contradiction. Hence, $\vartheta_1(z) = 0$, and similarly when $\deg(\theta_1) = 0$. By (i), we then have

$$C = \langle \theta_0(z), v\vartheta_2(z) + p^2\vartheta_3(z), p\theta_1(z) + v\vartheta_4(z) + p^2\vartheta_5(z), v\theta_2(z) + p^2\vartheta_6(z), p^2\theta_3(z) \rangle.$$

Since $v\vartheta_2(z) + p^2\vartheta_3(z) \in \ker(\eta_v) \cap C = \langle v\theta_2(z) \rangle$, it follows that $\theta_2(z) \mid \vartheta_2(z)$ and $\theta_2(z) \mid \vartheta_3(z)$. Degree constraints then force $\vartheta_2(z) = \vartheta_3(z) = 0$. Applying (i) again gives $\langle v\theta_2(z) + p^2\vartheta_6(z) \rangle = \langle v\theta_2(z), p^2\vartheta_6(z) \rangle$, which similarly implies $\vartheta_6(z) = 0$. Hence,

$$C = \langle \theta_0(z) + p\theta_1(z) + v\vartheta_4(z) + p^2\vartheta_5(z), v\theta_2(z), p^2\theta_3(z) \rangle.$$

Finally, since $\theta_3(z) \mid \theta_2(z)$ and $v^2 = p^2\alpha$ with $\alpha \neq 0$, we obtain the simplified representation

$$C = \langle \theta_0(z) + p\theta_1(z) + v\vartheta_4(z), v\theta_2(z) \rangle.$$

□

Lemma 2 implies that every non-principal ideal of $\mathfrak{R}(R, n)$ can be generated by a set of three polynomials. Specifically, these generators can be taken as $\vartheta_4(z)$, and the polynomials $\theta_i(z)$ for $i = 0, 1, 2$, all of which belong to $\mathfrak{R}(\mathbb{F}_{p^m}, n)$.

Corollary 2. *Let n be a positive integer such that $\gcd(n, p) = 1$. Then, every ideal C of $\mathfrak{R}(R, n)$ is written as*

$$C = \langle \theta_0(z) + p\theta_1(z) + v\vartheta_4(z),\ v\theta_2(z) \rangle, \tag{4.10}$$

where $\theta_0(z), \theta_1(z), \theta_2(z), \vartheta_4(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$.

In the next theorem, we describe the structure of the duals of cyclic codes under $\gcd(n, p) = 1$.

Theorem 11. *Let C be a cyclic code over R of length n corresponding to an ideal $C = \langle \theta_0(z) + p\theta_1(z) + v\vartheta_4(z), v\theta_2(z) \rangle$ of $\mathfrak{R}(R, n)$. Then,*

$$Ann(C) = \left\langle \frac{z^n - 1}{\gcd(\theta_2(z), \theta_1(z))} + p\hat{\theta}_0(z), v\hat{\theta}_0(z) \right\rangle.$$

Moreover, the ideal

$$\left\langle \frac{z^n - 1}{\gcd(\theta_2(z), \theta_1(z))^*} + p\hat{\theta}_0^*(z), v\hat{\theta}_0^*(z) \right\rangle$$

corresponds to the dual code $C^\perp$ of C.

Proof. First, note that both $\theta_2(z)$ and $\theta_1(z)$ divide $z^n - 1$ since $z^n - 1$ is a product of distinct irreducible polynomials in $\mathbb{F}_{p^m}[z]$. By Lemma 2, we have

$$\mathrm{Ann}(C) = \langle \theta_0'(z) + p\theta_1'(z) + v\vartheta_4'(z), v\theta_2'(z) \rangle = \langle \theta_0'(z), p\theta_1'(z), v\theta_2'(z) \rangle$$

for some $\theta_0'(z), \theta_1'(z), \theta_2'(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$ satisfying Representation (A). Then, $(\theta_0'(z) + p\theta_1'(z) + v\vartheta_4'(z))v\theta_2(z) = 0$, so $z^n - 1 \mid \theta_0'(z)\theta_2(z)$, and thus $\frac{z^n-1}{\theta_2(z)} \mid \theta_0'(z)$. Similarly, by Lemma 2 (i), $v\theta_2(z) + v\vartheta_2(z) \in C$ and $\theta_0'(z) \in \mathrm{Ann}(C)$, which gives $\frac{z^n-1}{\theta_1(z)} \mid \theta_0'(z)$ and $\frac{z^n-1}{\vartheta_4(z)} \mid \theta_0'(z)$. Hence,

$\theta_0'(z) = \frac{z^n-1}{\gcd(\theta_1(z),\vartheta_4(z))}\, l(z)$ for some $l(z) \in \frac{\mathbb{F}_p[z]}{\langle z^n-1\rangle}$. Taking into account that $\theta_2(z)$ also divides $\theta_0'(z)$, we conclude $\theta_0'(z) = \frac{z^n-1}{\gcd(\theta_2(z),\theta_1(z))}\, l(z)$. Analogously, $\theta_1'(z) = \frac{z^n-1}{\theta_0(z)} l'(z)$ and $\vartheta_4'(z) = \frac{z^n-1}{\theta_0(z)} l''(z)$ for some $l'(z), l''(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$. Finally, $v\theta_2'(z)\theta_0(z) = 0$, thus $\theta_2'(z) = \hat{\theta}_0(z) l_2(z)$ for some $l_2(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$. Therefore, by Lemma 2, we obtain

$$\mathrm{Ann}(C) \subseteq \left\langle \frac{z^n-1}{\gcd(\theta_2(z),\theta_1(z))} + p\hat{\theta}_0(z), v\hat{\theta}_0(z) \right\rangle.$$

The reverse inclusion is straightforward to check, so the equality follows.

The statement for the dual code $C^\perp$ is an immediate consequence of the above and the discussion preceding Lemma 2. □

Lemma 3. *Let C and C' be cyclic codes over R of length n such that $C \subseteq C'$, with $\gcd(n,p) = 1$. Assume that $\theta_0(z), \theta_1(z), \theta_2(z), \theta_0'(z), \theta_1'(z), \theta_2'(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$ satisfy Representation (A), and that*

$$C = \langle \theta_0(z) + p\theta_1(z) + v\vartheta_4(z), v\theta_2(z)\rangle,$$
$$C' = \langle \theta_0'(z) + p\theta_1'(z) + v\vartheta_4'(z), v\theta_2'(z)\rangle.$$

Then, the following divisibility relations hold:

$$\theta_0'(z) \mid \theta_0(z), \quad \theta_1'(z) \mid \theta_1(z), \quad \textit{and} \quad \gcd(\theta_2'(z), \vartheta_4'(z)) \mid \gcd(\theta_2(z), \vartheta_4(z)).$$

Proof. Since C is contained in C', we can express $\theta_0(z)$ as

$$\begin{aligned}\theta_0(z) = {} & (\theta_0'(z) + p\theta_1'(z) + v\vartheta_4'(z))(a_1(z) + p\theta_2(z) + p^2 a_3(z) + v a_4(z)) \\ & + v\theta_2'(z)(b_1(z) + v b_2(z)).\end{aligned}$$

for some $a_1(z), \theta_2(z), a_3(z), a_4(z), g_1(z), g_2(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$. From this decomposition, it follows immediately that $\theta_0(z) = \theta_0'(z)a_1(z)$. Similarly, for the p-component, we have

$$\begin{aligned}p\theta_1(z) = {} & (\theta_0'(z) + p\theta_1'(z) + v\vartheta_4'(z))(\gamma_1(z) + p\gamma_2(z) + p^2\gamma_3(z) + v\gamma_4(z)) \\ & + v\theta_2'(z)(\gamma_5(z) + p\gamma_6(z) + p^2\gamma_7(z) + v\gamma_8(z))\end{aligned}$$

for some $\gamma_i(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$. Comparing the coefficients of p gives $\theta_1(z) = \theta_1'(z)\gamma_1(z) + \theta_0'(z)\gamma_2(z)$. Since $\theta_1'(z)$ divides $\theta_0'(z)$, we conclude that $\theta_1'(z) \mid \theta_1(z)$. For the v-component, we find

$$\vartheta_4(z) = \vartheta_4'(z)\gamma_1(z) + \theta_0'(z)\gamma_3(z) + \theta_2'(z)\gamma_5(z).$$

Using the fact that $\theta_2'(z) \mid \theta_0'(z)$ (by part (4) of Theorem 4), it follows that $\gcd(\theta_2'(z), \vartheta_4'(z)) \mid \vartheta_4(z)$. Finally, considering the v-term $v\theta_2(z)$, we can write

$$\begin{aligned}v\theta_2(z) = {} & (\theta_0'(z) + p\theta_1'(z) + v\vartheta_4'(z))(\gamma_1(z) + p\gamma_2(z) + p^2\gamma_3(z) + v\gamma_4(z)) \\ & + v\theta_2'(z)(\alpha_1(z) + p\alpha_2(z) + p^2\alpha_3(z) + v\alpha_4(z)).\end{aligned}$$

for some $\gamma_i(z), \alpha_i(z) \in \mathfrak{R}(\mathbb{F}_{p^m}, n)$. Comparing the coefficients of v yields $\theta_2(z) = \theta_0'(z)\gamma_3(z) + \vartheta_4'(z)\gamma_1(z) + \theta_2'(z)\alpha_1(z)$. By an argument similar to the previous cases, we deduce that $\gcd(\vartheta_4'(z), \theta_2'(z)) \mid \theta_2(z)$. Hence, we conclude $\theta_0'(z) \mid \theta_0(z), \theta_1'(z) \mid \theta_1(z)$, and $\gcd(\theta_2'(z), \vartheta_4'(z)) \mid \gcd(\theta_2(z), \vartheta_4(z))$. □

As a consequence of the earlier results, the generator polynomials for the ideals of $\mathfrak{R}(\mathbb{F}_{p^m}, n)$ corresponding to self-orthogonal and self-dual codes over R can be explicitly described.

Theorem 12. *Suppose C is a cyclic code given by $C = \langle \theta_0(z) + p\theta_1(z) + v\vartheta_4(z), v\theta_2(z)\rangle$. Then,*

(*i*) *C is self-orthogonal if and only if*

$$\frac{z^n - 1}{\gcd(\theta_2(z), \theta_1(z))^*} \mid \theta_0(z).$$

(*ii*) *There do not exist any self-dual cyclic codes over R.*

Proof. (*i*) Assume C is self-orthogonal. Hence, Theorem 11 and Lemma 3 imply $\frac{z^n-1}{\gcd(\theta_2(z),\theta_1(z))} \mid \theta_0(z)$. Conversely, if $\frac{z^n-1}{\gcd(\theta_2(z),\theta_1(z))} \mid \theta_0(z)$, then it follows that $z^n - 1 = -(z^n - 1)^* \mid (\theta_0(z)\gcd(\theta_2(z), \theta_1(z))^*)^*$. Hence, $z^n - 1 \mid \theta_0^*(z)\gcd(\theta_2(z), \theta_1(z))$, and consequently $\frac{z^n-1}{\theta_0^*(z)} \mid \gcd(\theta_2(z), \theta_1(z))$. Furthermore, from the first paragraph of the proof of Theorem 11, we also have $\gcd(\theta_2(z), \theta_1(z)) \mid \vartheta_4(z)$, leading to $\frac{z^n-1}{\theta_0^*(z)} \mid \vartheta_4(z)$. Therefore, by Lemma 3, C is self-orthogonal.
(ii) By contradiction, we assume C is self-dual, and let $q(z) = \gcd(\theta_2(z), \theta_1(z))$. Then, by Lemma 2 and Theorems 10 and 11, we can write

$$\theta_0(z) = \left(\frac{z^n - 1}{q^*(z)}\right)\gamma_1(z), \theta_1(z) = \left(\frac{z^n - 1}{\theta_0^*(z)}\right)\gamma_2(z), \vartheta_4(z) = 0, \theta_2(z) = \left(\frac{z^n - 1}{\theta_0^*(z)}\right)\gamma_3(z),$$

for some units $\gamma_1(z), \gamma_2(z), \gamma_3(z)$ in $\mathfrak{R}(\mathbb{F}_{p^m}, n)$. It follows that

$$q(z) = \gcd(\theta_2(z), \theta_1(z)) = \frac{z^n - 1}{\theta_0^*(z)} \quad \text{and} \quad \theta_0(z) = \left(\frac{z^n - 1}{q^*(z)}\right)\gamma_1(z) = \theta_0^*(z)\gamma_1(z).$$

Since $\theta_1(z) \mid \theta_0(z)$ by Theorem 10, we must have $\frac{z^n-1}{\theta_0(z)} \mid \theta_0(z)$. Given that $z^n - 1$ factors into distinct irreducible polynomials, this forces $\theta_0(z) = z^n - 1$, yielding $C = \langle p, v\rangle$, which is impossible because $pC \neq 0$ and $vC \neq 0$. Therefore, we have the result. □

We conclude this section by providing a characterization (Proposition 1) and a mass formula (Theorem 13) for cyclic LCD codes with $\gcd(n, p) = 1$.

4.4. Mass identity of cyclic LCD and self-orthogonal codes over R.

In this section, we let $\gcd(n, p) = 1$. For elements $x, y \in R$, we write $y \sim x$ if $x = uy$ for some unit $u \in R$.

Theorem 13. *Let $\alpha_1(z), \ldots, \alpha_t(z)$ be the irreducible factors of $z^n - 1$ in $\mathbb{F}_{p^m}[z]$, where $\alpha_{2i-1}(z) \sim \alpha_{2i}^*(z)$ for $1 \leq i \leq k$, and $\alpha_j(z)$ are self-reciprocal for $2k + 1 \leq j \leq t$. Define the set $\mathcal{Q}$ of polynomials $\theta_0(z) \in \mathbb{F}_{p^k}[z]$ such that*

$$\alpha_{2k+1}(z)\cdots\alpha_t(z) \mid \theta_0(z) \mid z^n - 1,$$

and for each $1 \leq i \leq k$, at least one of $\alpha_{2i-1}(z)$ or $\alpha_{2i}(z)$ divides $\theta_0(z)$. Then, the total number of cyclic self-orthogonal codes is given by

$$N_{\text{self-orth}} = \sum_{\theta_0(z)\in\mathcal{Q}} \left(\sum_{\frac{z^n-1}{\theta_0^*(z)} \mid \theta_2(z)\theta_0(z)} \aleph_0 \right), \tag{4.11}$$

where

$$\aleph_0 = \sum_{\frac{z^n-1}{\theta_0^*(z)} | \theta_1(z)\theta_0(z)} (p^k)^{\deg(\theta_2)-\deg\left(\gcd(\theta_2(z),\theta_1(z))\right)}.$$

Proof. For a fixed $\theta_0(z) \in \mathcal{Q}$, it holds that at least one of $\alpha_i(z)$ or $\alpha_i^*(z)$ divides $\theta_0(z)$ for each $1 \le i \le t$. Equivalently, $\alpha_i(z) \mid \theta_0(z)$ for $i > 2k$, and for each $1 \le i \le k$, at least one of $\alpha_{2i-1}(z)$ or $\alpha_{2i}(z)$ divides $\theta_0(z)$. Consider the polynomials $\theta_2(z), \theta_1(z) \in \mathfrak{R}(R, n)$ such that $\frac{z^n-1}{\theta_0^*(z)} \mid \theta_2(z) \mid \theta_0(z)$, $\frac{z^n-1}{\theta_0^*(z)} \mid \theta_1(z) \mid \theta_0(z)$. Using the polynomials $\theta_0(z), \theta_1(z)$ and $\theta_2(z)$, define the ideal $I = \langle \theta_0(z) + p\theta_1(z) + v\vartheta_4(z), v\theta_2(z)\rangle$. The total number of such distinct ideals is then given by

$$\sum_{\theta_0(z)\in\mathcal{Q}} \left(\sum_{\frac{z^n-1}{\theta_0^*(z)} | \theta_2(z)\theta_0(z)} \aleph_0 \right).$$

By Theorem 12, each of these ideals corresponds to a self-orthogonal code. □

Proposition 1. *Let* $\gcd(n, p) = 1$, *and let C be a cyclic code over R of length n with corresponding ideal* $\langle \theta_0(z) + p\theta_1(z) + v\vartheta_4(z),\ v\theta_2(z)\rangle$. *Then, C is an LCD code if and only if* $\deg(\theta_0) = \deg(\theta_2) = \deg(\theta_1)$ *and* $\theta_0^*(z) \mid \theta_0(z)$.

Proof. Observe that

$$\left\langle \frac{z^n-1}{\gcd(\theta_2(z),\theta_1(z))},\ p\frac{z^n-1}{\theta_0^*(z)},\ v\frac{z^n-1}{\theta_0^*(z)} \right\rangle$$

is the ideal corresponding to $C^\perp$ by Theorem 10. Suppose $C \cap C^\perp = \{0\}$. Since $p\frac{z^n-1}{\theta_0^*(z)}\theta_0(z) \in C \cap C^\perp$, it follows that $\frac{z^n-1}{\theta_0^*(z)}\theta_0(z) = 0$, so $\theta_0^*(z) \mid \theta_0(z)$. Hence, if $g(z)$ is an irreducible factor of $z^n - 1$ over $\mathbb{F}_{p^m}$ dividing $\theta_0(z)$, then $g^*(z)$ also divides $\theta_0(z)$, giving $\theta_0(z) = \beta\theta_0^*(z)$ for some nonzero $\beta \in \mathbb{F}_{p^m}$. On the other hand, $(p\theta_1(z) + v\vartheta_4(z))\frac{z^n-1}{\theta_0^*(z)} \in C \cap C^\perp$, so $\theta_1(z)\frac{z^n-1}{\theta_0^*(z)} = 0$ and $\theta_0^* \mid \theta_1(z)$. Since $\theta_0(z) \mid \theta_0^*(z)$ and $\theta_1(z) \mid \theta_0(z)$ by Representation (A), we deduce $\deg(\theta_1) = \deg(\theta_0)$. Moreover, because $\gcd(\theta_2(z), \theta_1(z)) \mid \vartheta_4(z)$ (see proof of Theorem 11), we must have $\vartheta_4(z) = 0$ by Representation (A). Conversely, assume $\deg(\theta_0(z)) = \deg(\theta_2(z)) = \deg(\theta_1(z)), \vartheta_4(z) = 0$, and $\theta_0^*(z) \mid \theta_0(z)$. Then, $v\frac{z^n-1}{\theta_0^*(z)}\theta_2(z) \in C \cap C^\perp$, so $\frac{z^n-1}{\theta_0^*(z)}\theta_2(z) = 0$, which implies $\deg(\theta_2) = \deg(\theta_0)$ by the same argument as for $\theta_1(z)$. Hence, the ideals corresponding to C and $C^\perp$ are

$$\langle \theta_0(z),\ p\theta_0(z),\ v\theta_0(z)\rangle \quad \text{and} \quad \left\langle \frac{z^n-1}{\theta_0^*(z)},\ p\frac{z^n-1}{\theta_0^*(z)},\ v\frac{z^n-1}{\theta_0^*(z)} \right\rangle,$$

respectively. Suppose $l(z) \in C \cap C^\perp$. Then, there exist $\gamma_i(z), \alpha_i(z) \in \mathfrak{R}(R, n)$ for $i = 1, 2, 3$ such that

$$\theta_0(z)\gamma_1(z) + p\theta_0(z)\gamma_2(z) + v\theta_0(z)\gamma_3(z) = \frac{z^n-1}{\theta_0^*(z)}\alpha_1(z) + p\frac{z^n-1}{\theta_0^*(z)}\alpha_2(z) + v\frac{z^n-1}{\theta_0^*(z)}\alpha_3(z).$$

This implies $\theta_0(z)\gamma_i(z) = \frac{z^n-1}{\theta_0^*(z)}\alpha_i(z)$, for each $i = 1, 2, 3$. Since $\theta_0(z) = \beta\theta_0^*(z)$ for some $\beta \in \mathbb{F}_{p^m}$, it follows that $\theta_0(z) \mid \alpha_i(z)$, and therefore all terms vanish; $\theta_0(z)\gamma_1(z) + p\theta_0(z)\gamma_2(z) + v\theta_0(z)\gamma_3(z) = 0$. Thus, $C \cap C^\perp = \{0\}$, so C is an LCD code. □

Corollary 3. *Suppose* $\gcd(n, p) = 1$. *Let* e_1 *(resp.* e_2*) denote the number of irreducible factors* $\theta(z)$ *of* $z^n - 1$ *over* $\mathbb{F}_{p^m}$ *satisfying* $\theta(z) = \pm\theta^*(z)$ *(resp.* $\theta(z) \neq \pm\theta^*(z)$*). Then, the total number of cyclic LCD codes of length n over R is given by*

$$2^{e_1+\frac{e_2}{2}}.$$

Proof. According to Proposition 1, a cyclic LCD code of length n over R is uniquely determined by a choice of polynomial $\theta_0(z) \in \mathfrak{R}(R, n)$ with the condition that whenever an irreducible divisor of $z^n - 1$ over $\mathbb{F}_{p^m}$ divides $\theta_0(z)$, its reciprocal polynomial must also divide $\theta_0(z)$. Counting the possible selections of such factors yields the formula $2^{e_1+e_2/2}$. □

Using Theorem 5, we can explicitly compute the number of cyclic LCD codes over R of length n with $\gcd(n, p) = 1$ in the following example.

5. Numerics

This section presents examples that illustrate our findings.

Example 1. *We illustrate Representation (A) given in Theorem 4. Let us consider the ideals in* $\mathfrak{R}(R_1, 4)$, *where* $R_1 = \frac{GR(4,m)[v]}{\langle v^2, pv\rangle}$.

(1) Let C_1 *be the ideal generated by* $(z-1)^2$. *Theorem 4 gives the representation as*

$$C_1 = \langle (z-1)^2, 2(z-1)^2, v(z-1)^2\rangle, \quad \textit{where} \quad \theta_0(z) = \theta_1(z) = \theta_2(z) = (z-1)^2.$$

However, as an ideal, C yields the following as possible constructions:

$$\langle (z-1)^2, 0\rangle, \quad \langle (z-1)^2 + 2(z-1)^2, 0\rangle, \quad \langle (z-1)^2 + 2(z-1)^3, 0\rangle,$$

$$\textit{and} \quad \langle (z-1)^2 + 2(z-1)^3 + 2(z-1)^2, 0\rangle.$$

Thus, the construction obtained above is not unique in general.

(2) Let C_2 *be the ideal generated by* $(z-1)^3$. *Theorem 4 gives the representation as*

$$C_2 = \langle\langle (z-1)^3, \quad 2(z-1)^2, \quad v(z-1)^3\rangle\rangle,$$
$$\theta_0(z) = (z-1)^3 = \theta_2(z), \theta_1(z) = (z-1)^2,$$

while the ordinary representation will be $\langle (z-1)^3\rangle$. *From the last representation, we see that the ideal is generated by one element. However, we cannot immediately know all the* $deg(\theta_0)$, $deg(\theta_1)$, *and* $deg(\theta_2)$ *of the ideal from its algebraic structure, whereas in the Representation (A), we know all the degrees of* θ_0, θ_1, *and* θ_2.

Now, we find the duals of C_1 *and* C_2 :

$$C_1^{\perp} = \langle (z-1)^2, 2(z-1)^2, v(z-1)^2\rangle, \quad C_2^{\perp} = \langle (z-1)^2, 2(z-1), v(z-1)\rangle.$$

We note that C_1 *is a self-dual code over* $GR(4, m)[v]$.

Example 2. *After calculations, the polynomials $\theta_0^{\perp}$ and $\theta_1^{\perp}$ in representation of $C^{\perp}$ in Theorem 5 take the forms in some cases where $b = 0, 1$ and $a = p^s, p^s - 1, p^s - 2, p^s - 3$ (Table 2),*

$$\theta_0^{\perp}(z) = \begin{cases} 0, & \text{if } b = 0, \\ (-1)^{a+1}\theta_{0,0}, & \text{if } b = 1, \end{cases}$$

$$\theta_1^{\perp}(z) = \begin{cases} 0, & \text{if } a = p^s, \\ (-1)^{3+t_1}\theta_{1,0}, & \text{if } a = p^s - 1, \\ (-1)^{2+t_1}\theta_{1,0} + \left((-1)^{2+t_1}(1+d-t_1)\theta_{1,0} + (-1)^{3+t_1}\theta_{1,1}\right)(z-1), & \text{if } a = p^s - 2, \\ (-1)^{1+t_1}\theta_{1,0} + \left((-1)^{1+t_1}(1+d-t_1)\theta_{1,0} + (-1)^{2+t_1}\theta_{1,1}\right)(z-1), & \\ +\left((-1)^{1+t_1}\frac{(d-t_1)(d-t_1-1)}{2}\theta_{1,0} + (-1)^{2+t_1}(d-t_1-1)\theta_{1,1}, & \text{if } a = p^s - 3, \\ +(-1)^{3+t_1}\theta_{1,2}\right)(z-1)^2. & \end{cases}$$

Table 2. Cyclic codes and their dual codes over R.

Cyclic Code C	**Dual Code** $C^{\perp}$
$\langle 1, 3, v\rangle$	$\langle (z-1)^3, 3, v(z-1)^3\rangle$
$\langle (z-1), 3, v\rangle$	$\langle (z-1)^3, 3, v(z-1)^2\rangle$
$\langle (z-1) + v\theta_{1,0}, 3 + v\theta_{2,0}v(z-1)\rangle$	$\langle (z-1)^3 + v\theta_{1,0}, 3, v(z-1)^2\rangle$
$\langle (z-1) + 3\theta_{0,0}, 3(z-1), v\rangle$	$\langle (z-1)^3 - 3\theta_{0,0}, 3, v(z-1)^2\rangle$
$\langle (z-1) + 3\theta_{0,0} + v\theta_{1,0}, 3(z-1) + v\theta_{2,0}, v(z-1)\rangle$	$\langle (z-1)^2 - 3\theta_{0,0} + v\theta_{1,0}, 3(z-1), v(z-1)^2\rangle$
$\langle (z-1)^2, 3, v\rangle$	$\langle (z-1)^3, 3, v(z-1)\rangle$
$\langle (z-1)^2 + v\theta_{1,0}, 3 + v\theta_{2,0}, v(z-1)\rangle$	$\langle (z-1)^3 + v\theta_{1,0}, 3, v(z-1)\rangle$
$\langle (z-1)^2 + v(\theta_{1,0} + \theta_{1,1}(z-1)), 3 + v(\theta_{2,0} + \theta_{2,1}(z-1)), v(z-1)^2\rangle$	$\langle (z-1)^3 + v\theta_{1,0}, 3(z-1), v(z-1)\rangle$
$\langle (z-1)^2 + 3\theta_{0,0}, 3(z-1), v\rangle$	$\langle (z-1)^3 - 3\theta_{1,0}, 3(z-1), v(z-1)\rangle$
$\langle (z-1)^2 + 3\theta_{0,0} + v\theta_{1,0}, 3(z-1) + v\theta_{2,0}, v(z-1)\rangle$	$\langle (z-1)^2 - 3\theta_{1,0} + v\theta_{1,0}, 3(z-1), v(z-1)\rangle$
$\langle (z-1)^2 + 3\theta_{0,0} + v(\theta_{1,0} + \theta_{1,1}(z-1)), 3(z-1) + v(\theta_{2,0} + \theta_{2,1}(z-1)), v(z-1)^2\rangle$	$\langle (z-1)^2 - 3\theta_{1,0} + v\theta_{1,0}, 3(z-1), v(z-1)\rangle$
$\langle (z-1)^3, 3(z-1)^b + v(z-1)^{t_2}\theta_2(z), v(z-1)^c\rangle$	$\langle (z-1)^{3-d}, 3(z-1), v\rangle$

Example 3. *Let $R_1 = GR(3^2, 1)[v]$ and $v^2 = 3v = 0$. We investigate cyclic codes of length 3 over R_1. In particular, we list all cyclic codes and their duals.*

Example 4. *We illustrate the application of Theorem 13 by computing the number of cyclic self-orthogonal codes over $R = \mathrm{GR}(3^3, 3)[v]/\langle v^2 - 3^2\alpha,\ 3v\rangle$ for parameters $(n, p, m) = (2, 3, 3)$.*

(1) ***Factorization.*** *Over $\mathbb{F}_{27}$, the polynomial $z^2 - 1$ decomposes as*

$$z^2 - 1 = (z-1)(z+1).$$

Both factors are irreducible and self-reciprocal up to a unit, since $(z-1)^*(z) = -z+1 \sim z-1$ *and* $(z+1)^*(z) = z+1$. *Hence,* $e_1 = 2$, $e_2 = 0$, *and* $k = 0$.

(2) ***Construction of Q.*** *As all irreducible factors are self-reciprocal, the defining condition in Theorem 13 reduces to*

$$z^2 - 1 \mid \theta_0(z) \mid z^2 - 1,$$

so that $\mathcal{Q} = \{ z^2 - 1 \}$.

(3) ***Computation of L.*** *For* $\theta_0(z) = z^2 - 1$, *we have* $\theta_0^*(z) = z^2 - 1$, *and* $L = \frac{z^2-1}{\theta_0^*(z)} = 1$. *Consequently, the formula in Theorem 13 simplifies to*

$$N_{\text{self-orth}} = \sum_{\frac{z^2-1}{\theta_0^*(z)} \mid \theta_2(z)\theta_0(z)} \aleph_0,$$

where

$$\aleph_0 = \sum_{\frac{z^2-1}{\theta_0^*(z)} \mid \theta_1(z)\theta_0(z)} (3^3)^{\deg(\theta_2(z)) - \deg\left(\gcd(\theta_2(z),\theta_1(z))\right)}.$$

Because the divisibility conditions are automatically satisfied, the summations extend over all divisors of $z^2 - 1$.

(4) ***Evaluation of the summation.*** *The divisors of* $z^2 - 1$ *are* 1, $z-1$, $z+1$, *and* $z^2 - 1$. *For each ordered pair* $(\theta_1(z), \theta_2(z))$, *we compute*

$$(3^3)^{\deg(\theta_2) - \deg(\gcd(\theta_2(z),\theta_1(z)))} = 27^{\deg(\theta_2(z)) - \deg(\gcd(\theta_2(z),\theta_1(z)))}.$$

The resulting values are summarized as follows:

$$\begin{aligned}
&\theta_2(z) = 1: && \textstyle\sum_{\theta_1(z)} 27^0 = 4,\\
&\theta_2(z) = z-1: && 27 + 1 + 27 + 1 = 56,\\
&\theta_2(z) = z+1: && 56,\\
&\theta_2(z) = z^2 - 1: && 27^2 + 27 + 27 + 1 = 784.
\end{aligned}$$

Thus, $N_{\text{self-orth}} = 4 + 56 + 56 + 784 = 900$.

(5) ***Result.*** *Since* $|\mathcal{Q}| = 1$, *the total number of cyclic self-orthogonal codes over R for* $(n, p, m) = (2, 3, 3)$ *is* $N_{\text{self-orth}} = 900$. *This computation verifies the consistency of Theorem 13 and demonstrates how the mass formula systematically enumerates cyclic self-orthogonal codes via the factorization of* $z^n - 1$ *and the interplay of divisor degrees in* $\mathbb{F}_{p^m}[z]$ *(Figure 2 (a)).*

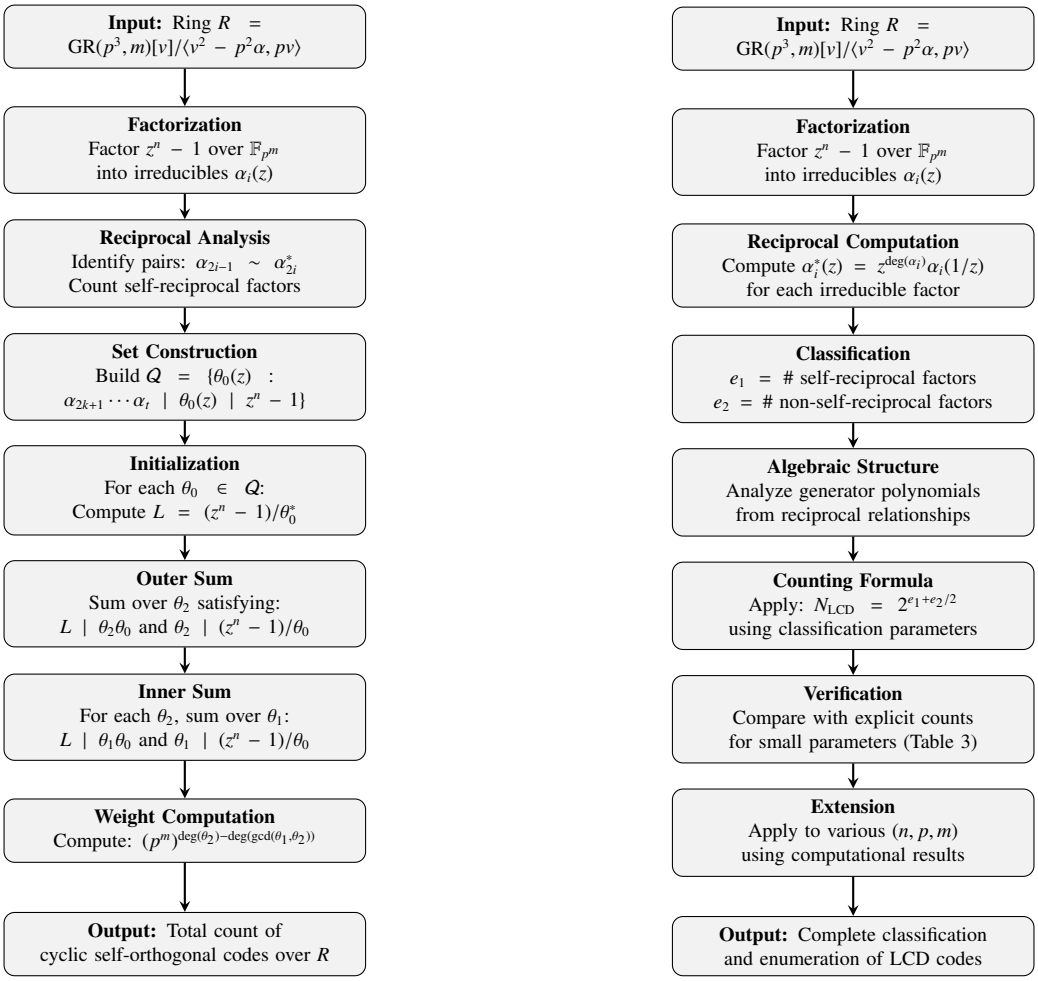
Example 5. *Tables 3 and 4 list the total number of LCD codes over R for various lengths* $n = 9, 15, 10, 14, 13, 8, 12, 6, 21, 24, 18$ *with primes* $p = 3, 7, 13,$ *and* 11.

Table 3. Number of cyclic LCD codes over R for various parameters (n, p, m).

Parameters (n, p, m)	Factorization of $z^n - 1$	e_1	e_2	Number of LCD codes
(14, 3, 1)	$(z-1)(z+1)(z^6+z^5+z^4+z^3+z^2+z+1)$ $(z^6+2z^5+z^4+2z^3+z^2+2z+1)$	4	0	16
(11, 5, 2)	$(z+4)(z^5+2z^4+4z^3+z^2+z+4)$ $(z^5+4z^4+4z^3+z^2+3z+4)$	1	2	4
(10, 3, 1)	$(z-1)(z+1)(z^4+z^3+z^2+z+1)$ $(z^4+2z^3+z^2+2z+1)$	4	0	16

Table 4. Number of cyclic LCD codes over R for various parameters (n, p, m) (continued).

Parameters (n, p, m)	Factorization of $z^n - 1$	e_1	e_2	Number of LCD codes
(24, 11, 3)	$(z+1)(z+10)(z^2+1)(z^2+z+1)(z^2+2z+10)$ $(z^2+8z+10)(z^2+5z+1)(z^2+5z+10)(z^2+10z+1)$ $(z^2+9z+10)(z^2+3z+10)(z^2+6z+1)(z^2+6z+10)$	7	6	1024
(13, 5, 1)	$(z+4)(z^4+z^3+4z^2+z+1)$ $(z^4+2z^3+z^2+2z+1)$ (z^4+3z^3+3z+1)	4	0	16
(12, 13, 2)	$(z+1)(z+2)(z+4)(z+8)(z+3)(z+6)$ $(z+12)(z+11)(z+9)(z+5)(z+10)(z+7)$	2	10	128
(8, 5, 1)	$(z-1)(z+1)(z-2)(z+2)(z^2+2)(z^2+3)$	2	4	16
(21, 13, 3)	$(z+4)(z+12)(z+10)(z^2+z+3)(z^2+2z+3)$ $(z^2+2z+9)(z^2+3z+1)(z^2+6z+1)(z^2+6z+3)$ $(z^2+9z+9)(z^2+5z+1)(z^2+5z+9)$	4	8	256
(12, 7, 1)	$(z-1)(z+1)(z-3)(z+3)(z-2)(z+2)(z^2+1)$ $(z^2+2)(z^2+4)$	3	6	64
(18, 7, 2)	$(z+1)(z+3)(z+2)(z+6)(z+4)(z+5)$ $(z^3+3)(z^3+2)(z^3+4)(z^3+5)$	2	8	64
(9, 7, 1)	$(z-1)(z-3)(z-5)(z^3+3)(z^3+5)$	1	4	8
(6, 11, 1)	$(z-1)(z+1)(z^2+z+1)(z^2+10z+1)$	4	0	16
(15, 11, 1)	$(z-2)(z-6)(z-7)(z-8)(z-10)(z^2+z+1)$ $(z^2+3z+9)(z^2+4z+5)(z^2+5z+3)(z^2+9z+4)$	2	8	64
(12, 13, 3)	$(z+1)(z+2)(z+4)(z+8)(z+3)(z+6)$ $(z+12)(z+11)(z+9)(z+5)(z+10)(z+7)$	2	10	128



(a) Self-orthogonal codes enumeration (b) LCD codes enumeration

Figure 2. Enumeration procedures for (a) cyclic self-orthogonal codes using the mass formula (Theorem 13) and (b) cyclic LCD codes using the classification formula (Corollary 3), over the ring R.

Remark 1. *The computation in Appendix A provides a symbolic verification of the factorization patterns that underpin our enumeration formula for cyclic LCD codes. This exercise highlights a key conceptual distinction from earlier works, particularly that of [25]. While their analysis relies on polynomial factorizations over the base field $\mathbb{F}_p$, our investigation is conducted within the more structurally intricate setting of the Galois ring $\mathrm{GR}(p^3, m)$.*

This shift in the algebraic framework is significant. By working over the extension field $\mathbb{F}_{p^m}$ as the residue field, our approach captures a richer and more refined factorization of $z^n - 1$, which directly determines the structure and enumeration of the corresponding cyclic codes. Moreover, by formulating our results over a local Frobenius non-chain ring of higher characteristic p^3 endowed with a specific nilpotent structure, we demonstrate that the principles of code enumeration can be systematically extended beyond simpler, non-Frobenius or chain-ring contexts.

Consequently, the enumeration formulas derived in this work are not merely analogous to those in [25]; they constitute a substantive generalization to a broader and more algebraically complex

class of rings. This advancement broadens the scope of enumerative coding theory and deepens our understanding of code structures over mixed-characteristic, non-chain rings.

6. Conclusions

In this work, we have investigated cyclic, self-dual, and linear complementary dual (LCD) codes of length n over the local Frobenius non-chain ring

$$R = \mathrm{GR}(p^3, m)[v], \quad v^2 = p^2\alpha,\ \alpha \in \mathbb{F}_{p^m}^*,\ pv = 0. \tag{6.1}$$

We first established a complete algebraic framework describing the structure of cyclic codes of arbitrary length over R. For the case $\gcd(n, p) = 1$, we derived explicit forms of generator polynomials and characterized the corresponding ideals in $\frac{R[z]}{\langle z^n-1\rangle}$. Building on this foundation, we constructed and enumerated both self-dual and LCD cyclic codes, providing necessary and sufficient conditions for their existence. The resulting mass formulas and enumeration theorems extend known results for chain and Galois rings to a broader class of non-chain Frobenius rings.

Additionally, we verified the enumeration formulas through explicit examples and computational cases for small parameters, confirming the validity of Theorem 13. These examples also highlight the combinatorial growth of self-orthogonal code families, emphasizing the structural richness of cyclic codes over R.

Our findings contribute to a deeper understanding of the algebraic structure and enumeration of codes over non-chain local rings, bridging the gap between theoretical ring properties and their coding-theoretic applications. Future research may extend these results to analyze the Gray images and minimum distance properties of the constructed codes, explore new classes of double circulant and quasi-cyclic codes over R, and develop algorithmic constructions for optimal and quantum codes derived from this framework.

Author contributions

Sami Alabiad: Conceptualization, Methodology, Formal analysis, Investigation, Writing-review and editing, Writing-original draft; Alhanouf Ali Alhomaidhi: Conceptualization, Methodology, Validation, Project administration, Writing-review and editing. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

The authors declare that they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors would like to thank the Ongoing Research Funding program, (ORF-2025-1112), King Saud University, Riyadh, Saudi Arabia.

Conflict of interests

The authors declare no conflict of interest.

References

1. I. F. Blake, Codes over certain rings, *Inf. Contr.*, **20** (1972), 396–404. http://doi.org/10.1016/S0019-9958(72)90223-9
2. A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inf. Theory*, **40** (1994), 301–319. http://doi.org/10.1109/18.312154
3. A. R. Calderbank, N. J. A. Sloane, Modular and p-adic codes, *Des. Codes Cryptogr.*, **6** (1995), 21–35. http://doi.org/10.1007/BF01390768
4. P. Kanwar, S. R. López-Permouth, Cyclic codes over the integers modulo p^m, *Finite Fields Appl.*, **3** (1997), 334–352. http://doi.org/10.1006/ffta.1997.0189
5. A. Bonnecaze, P. Udaya, Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inf. Theory*, **45** (1999), 1250–1255. http://doi.org/10.1109/18.761278
6. H. Q. Dinh, S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inf. Theory*, **50** (2004), 1728–1744. http://doi.org/10.1109/TIT.2004.831789
7. B. Yildiz, S. Karadeniz, Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, *Des. Codes Cryptogr.*, **58** (2011), 221–234. http://doi.org/10.1007/s10623-010-9399-3
8. A. K. Singh, P. K. Kewat, On cyclic codes over the ring $\mathbb{Z}_p[u]/\langle u^k\rangle$, *Des. Codes Cryptogr.*, **74** (2015), 1–13. http://doi.org/10.1007/s10623-013-9843-2
9. B. Kim, Y. Lee, Classification of self-dual cyclic codes over the chain ring $\mathbb{Z}_p[u]/\langle u^3\rangle$, *Des. Codes Cryptogr.*, **88** (2020), 2247–2273. http://doi.org/10.1007/s10623-020-00776-1
10. E. M. Rains, N. J. A. Sloane, Self-dual codes, in V. S. Pless, W. C. Huffman (Eds.), *Handbook of Coding Theory*, Amsterdam: North-Holland, 1998. https://doi.org/10.48550/arXiv.math/0208001
11. T. A. Gulliver, V. K. Bhargava, Some best rate $\frac{1}{p}$ and rate $\frac{p-1}{p}$ systematic quasi-cyclic codes, *IEEE Trans. Inf. Theory*, **37** (1991), 552–555. http://doi.org/10.1109/18.79911
12. M. Shi, D. Huang, L. Sok, P. Solé, Double circulant self-dual and LCD codes over Galois rings, *Adv. Math. Commun.*, **13** (2019), 171–183. http://doi.org/10.3934/amc.2019011
13. M. Shi, H. Zhu, L. Sok, P. Solé, On self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q$, *Cryptogr. Commun.*, **12** (2020), 53–70. https://doi.org/10.1007/s12095-019-00363-9
14. J. L. Massey, Linear codes with complementary duals, *Discrete Math.*, **106/107** (1992), 337–342. http://doi.org/10.1016/0012-365X(92)90563-U
15. M. Shi, Y. Zhang, Quasi-twisted codes with constacyclic constituent codes, *Finite Fields Appl.*, **39** (2016), 159–178. https://doi.org/10.1016/j.ffa.2016.01.010
16. M. Shi, H. Zhu, L. Qian, P. Solé, On self-dual four circulant codes, *Int. J. Found. Comput. Sci.*, **29** (2018), 1143–1150. https://doi.org/10.1142/S0129054118500259

17. M. Alshuhail, A. Betty, A. Galvez, Duality of codes over non-unital rings of order six, *AIMS Math.*, **10** (2025), 4934–4951. http://doi.org/10.3934/math.2025839
18. D. Xie, S. Zhu, Two families of self-orthogonal codes with applications in LCD codes and optimally extendable codes, *Finite Fields Appl.*, **108** (2025), 102659. https://doi.org/10.1016/j.ffa.2025.102659
19. H. Islam, O. Prakash, Construction of LCD and new quantum codes from cyclic codes over a finite non-chain ring, *Cryptogr. Commun.*, **14** (2022), 59–73. https://doi.org/10.1007/s12095-021-00516-9
20. S. Li, M. Shi, H. Liu, Several constructions of optimal LCD codes over small finite fields, *Cryptogr. Commun.*, **16** (2024), 779–800. https://doi.org/10.1007/s12095-024-00699
21. L. Sok, M. Shi, P. Solé, Construction of optimal LCD codes over large finite fields, *Finite Fields Appl.*, **50** (2018), 138–153. https://doi.org/10.1016/j.ffa.2017.11.007
22. N. Aydin, Y. Cengellenmis, A. Dertli, On some constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$, their $\mathbb{Z}_4$ images, and new codes, *Des. Codes Cryptogr.*, **86** (2018), 1249–1255. http://doi.org/10.1007/s10623-017-0392-y
23. M. Shi, F. Özbudak, L. Xu, P. Solé, LCD codes from tridiagonal Toeplitz matrices, *Finite Fields Appl.*, **75** (2021), 101892. http://doi.org/10.1016/j.ffa.2021.101892
24. C. A. Castillo-Guillén, C. Rentería-Márquez, H. Tapia-Recillas, Constacyclic codes over finite local Frobenius non-chain rings with nilpotency index 3, *Finite Fields Appl.*, **43** (2017), 1–21. https://doi.org/10.1016/j.ffa.2016.08.004
25. H. S. Choi, B. Kim, Various structures of cyclic codes over the non-Frobenius ring $\mathbb{F}_p[u,v]/\langle u^2, v^2, uv, vu\rangle$, *Adv. Math. Commun.*, **18** (2024), 304–327. http://doi.org/10.3934/amc.2023030
26. S. T. Dougherty, E. Saltürk, S. Szabo, On codes over Frobenius rings: Generating characters, MacWilliams identities and generator matrices, *Appl. Algebra Eng. Commun. Comput.*, **30** (2019), 193–206. https://doi.org/10.1007/s00200-019-00384-0
27. S. H. Saif, Constructions and enumerations of self-dual and LCD double circulant codes over a local ring, *Mathematics*, **13** (2025), 3527. https://doi.org/10.3390/math13213527
28. S. H. Saif, Structures, ranks and minimal distances of cyclic codes over $\mathbb{Z}_{p^2} + u\mathbb{Z}_{p^2}$, *Mathematics*, **13** (2025), 3354. https://doi.org/10.3390/math13203354
29. S. Alabiad, A. A. Alhomaidhi, N. A. Alsarori, On linear codes over local rings of order p^4, *Mathematics*, **12** (2024), 3069. http://doi.org/10.3390/math12193069
30. S. Alabiad, A. A. Alhomaidhi, Cyclic, LCD, and self-dual codes over the non-Frobenius ring $\mathrm{GR}(p^2, m)[u]/\langle u^2, pu\rangle$, *Mathematics*, **13** (2025), 3193. https://doi.org/10.3390/math13193193

A. Verification of polynomial factorizations

This appendix provides computational verification of the polynomial factorizations reported in Table 3 using Magma. We illustrate the procedure with one representative example; the remaining cases were confirmed analogously. All computations were carried out in Magma on a standard finite-field environment.

Example: Verification for $(n, p, m) = (14, 3, 1)$

The factorization of $z^{14} - 1$ over $\mathbb{F}_3$ in Table 3 is

$$z^{14} - 1 = (z-1)(z+1)(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1)(z^6 - z^5 + z^4 - z^3 + z^2 - z + 1). \tag{A.1}$$

The following MAGMA code verifies this result:

```
> p := 3; n := 14;
> F := GF(p);
> P<z> := PolynomialRing(F);
> Factorization(z^n - 1);
```

The computation returns:

```
[
<z + 1, 1>,
<z + 2, 1>,
<z^6 + z^5 + z^4 + z^3 + z^2 + z + 1, 1>,
<z^6 + 2*z^5 + z^4 + 2*z^3 + z^2 + 2*z + 1, 1>
]
```

This is algebraically equivalent to the factorization shown in Table 3, since, $(z + 2) = (z - 1)$ in $\mathbb{F}_3$. Hence, we obtain $e_1 = 4$ and $e_2 = 0$, giving $2^{e_1 + \frac{e_2}{2}} = 16$ cyclic LCD codes, as reported in Table 3.

All remaining factorizations in Tables 3 and 4 were verified in the same way using Figure 2 (b).