Palestine Journal of Mathematics

Vol 13(4)(2024) , 934–947

On repeated-root constacyclic codes of arbitrary lengths over Galois ring GR(p^m, ℓ)

Youssef Ahendouz and Ismail Akharraz

Communicated by Manoj Kumar Patel

MSC 2020 Classification: Primary 11T71; Secondary 11Txx .

Keywords and phrases: Repeated-root codes, Galois rings, dual codes, discrete Fourier transform, minimum distance separable.

Abstract This article explores the properties of $(\xi_0 + p\gamma)$-constacyclic codes over GR(p^m, ℓ) of any length, where γ is a unit of GR(p^m, ℓ) and ξ_0 is a nonzero element in the Teichmüller set $\mathcal{T}$. We provide an analysis of the structure of $(\xi_0 + p\gamma)$-constacyclic codes of length p^s over GR(p^m, ℓ), and determine their b-symbol distance. Using these codes, we classify all $(\xi + p\gamma)$-constacyclic codes of length $n = p^s\eta$ (η prime to p) over GR(p^m, ℓ). We also investigate the dual of these codes and present necessary and sufficient conditions for the existence of nontrivial self-dual constacyclic codes. In addition, we calculate the b-symbol distance of these codes for length $2p^s$, where p is a prime number, and demonstrate that some of these codes are MDS (minimum distance separable).

1 Introduction

The objective of coding theory is to create codes capable of transmitting data with a high degree of precision and effectiveness. This is achieved by choosing codes with the maximum feasible minimum distance, while taking into account limitations on code length, code size, and the size of the code alphabet. This strategy guarantees that the code can rectify as many errors as feasible when transmitting data through a noisy channel. Different distances, including the Hamming distance, Lee distance, and Rosenbloom-Tsfasman distance, etc, have been developed and analyzed for their ability to detect and correct errors in various communication channels. Among these, the Hamming distance is the most widely studied and is considered to be a key distance in the field of coding theory.

The investigation of codes over finite rings has been an active field of research since the early 1970s. The introduction of nonlinear binary codes obtained from cyclic codes over $\mathbb{Z}_4$ through the utilization of the Gray map. For instance, Wolfmann conducted an analysis of negacyclic codes over $\mathbb{Z}_4$ with odd lengths, yielding significant outcomes [1, 2]. These findings were subsequently extended by Tapia-Recillas and Vega to encompass codes over $\mathbb{Z}_{2^k}$ [3]. Following this, Dinh and López-Permouth elucidated the structure of negacyclic codes of length n over a finite chain ring R, where the length n is not divisible by the characteristic p of the residue field R [4].

In case where the code length n is divisible by the characteristic p of the residue field $\bar{R}$ is known as the repeated-root codes. Over the past few years, substantial research efforts have been directed towards the examination of repeated-root constacyclic codes within the context of finite rings.

Blackford classified all negacyclic codes over $\mathbb{Z}_4$ of even length in [5] . This work extended Wolfmann's findings to encompass negacyclic codes of even length. Additionally, Dinh examined the structural characteristics of λ-constacyclic codes with a length of 2^s over $\mathbb{Z}_{2^a}$ in [6]. Here, λ represents any unit within $\mathbb{Z}_{2^a}$ following the form $4k - 1$. Dinh's study also established the Hamming, homogeneous, Lee, and Euclidean distances for all such constacyclic codes.

These studies provide further insight into the properties and structure of repeated-root constacyclic codes over finite rings and demonstrate the ongoing efforts to advance our understanding in this area.

This paper explores $(\xi_0+p\gamma)$-constacyclic codes over GR(p^m, ℓ) with arbitrary length, where

ξ_0 is a nonzero element in the Teichmüller set $\mathcal{T}$ and γ is a unit of $\mathrm{GR}(p^m, \ell)$. This class generalizes the following two cases: (i) When p equals 2, the set of constacyclic codes is identical to the set of λ-constacyclic codes over $\mathbb{Z}_{2^a}$, where λ represents any unit of $\mathbb{Z}_{2^a}$ in the form of $4k-1$, as stated in reference [6]; (ii) When $\xi_0 = 1$ and $\ell = 1$, i.e., $\mathrm{GR}(p^m, \ell) = \mathbb{Z}_{p^m}$, in this case Shixin Zhu et al. used the discrete Fourier transform to classify all $(1+\lambda p)$-constacyclic codes [7].

The following is the structure of the remaining sections in this paper. Section 2 introduces the necessary notations and findings concerning constacyclic codes and Galois rings. In Section 3, we analyze the structure of $(\xi_0 + p\gamma)$-constacyclic codes with length p^s over $GR(p^m, \ell)$, and determine the b-symbol distances of all such codes. Section 4 applies the discrete Fourier transform to classify all $(\xi_0 + p\gamma)$-constacyclic codes with length $p^s\eta$ (where η is prime to p) over $\mathrm{GR}(p^m, \ell)$. In Section 5, we deal with the self-dual $(\xi_0+p\gamma)$-constacyclic codes with length $p^s\eta$ over $\mathrm{GR}(p^m, \ell)$. Finally, section 6 investigates the MDS b-symbol distances of $(\xi_0 + p\gamma)$-constacyclic codes with length $p^s\eta$ over $\mathrm{GR}(p^m, \ell)$, and we compute the b-symbol distances for the cases $b = 1, 2$ and $\eta = 2$.

2 Preliminaries

A commutative ring with identity R is classified as a principal ideal ring if its ideals can be generated by a single element. When R has a unique maximal ideal, it is referred to as a local ring. If the ideals of R are ordered by inclusion, it is denoted as a chain ring. The subsequent proposition provides a characterization for finite chain rings.

Proposition 2.1. *[4] Consider a finite commutative chain ring R with a maximal ideal M and a residue field $\bar{R} = \frac{R}{M}$. In this context, all ideals of R exhibit the following structure:*

$$\langle 0\rangle = \langle \varrho^e\rangle \subsetneq \langle \varrho^{e-1}\rangle \subsetneq \ldots \subsetneq \langle \varrho\rangle \subsetneq R,$$

where $\varrho \in R$, and e represents the nilpotency of ϱ. Additionally,

$$\text{for all } i = 0, \ldots, e, \mid \varrho^i \mid = \mid \bar{R} \mid^{e-i}.$$

When we have a prime number p along with positive integers m and ℓ, the Galois extension of $\mathbb{Z}_{p^m}$ with characteristic p^m and cardinality $p^{m\ell}$ is defined as $\frac{\mathbb{Z}_{p^m}[x]}{\langle f(x)\rangle}$, where $f(x)$ is a basic irreducible polynomial of degree ℓ over $\mathbb{Z}_{p^m}$ and is denoted as $\mathrm{GR}(p^m, \ell)$ [8].

Within $\mathrm{GR}(p^m, \ell)$, an element ξ with an order of $p^\ell - 1$ exists. Furthermore, for any element z in $\mathrm{GR}(p^m, \ell)$, it can be uniquely expressed in the p-adic form as:

$$z = \xi_0 + p\xi_1 + \cdots + p^{m-1}\xi_{m-1}, \tag{2.1}$$

where $\xi_i \in \mathcal{T} = \left\{0, 1, \xi, \xi^2, \ldots, \xi^{p^\ell - 2}\right\}$. The set $\mathcal{T}$ is known as the Teichmüller set. Additionally, we have the following proposition.

Proposition 2.2. *[8] With the previous notations, we have*

(i) $\xi_0 + p\xi_1 + \cdots + p^{m-1}\xi_{m-1}$ ($\text{with } \xi_i \in \mathcal{T}$) is a unit of $\mathrm{GR}(p^m, a)$ if and only if $\xi_0 \neq 0$.

(ii) For any $0 \leq i \neq j \leq p^\ell - 2$, $\xi^i - \xi^j$ is unit of $\mathrm{GR}(p^m, \ell)$.

For any positive integer ℓ', the inclusion $\mathrm{GR}(p^m, \ell) \subseteq \mathrm{GR}(p^m, \ell')$ holds if and only if ℓ divides ℓ'. Moreover for any positive integer a, $\mathrm{GR}(p^m, a\ell) = \frac{\mathrm{GR}(p^m, \ell)[x]}{\langle f(x)\rangle}$, where $f(x)$ is a basic irreducible polynomial of degree a over $\mathrm{GR}(p^m, \ell)$.

In $\mathrm{GR}(p^m, \ell')$, elements can also be represented using the ξ-adic expansion as $z_0 + z_1\xi + \cdots + z_{\ell'-1}\xi^{\ell'-1}$, where $z_i \in \mathbb{Z}_{p^m}$. The Frobenius automorphism Fr of $\mathrm{GR}(p^m, \ell')$ given by

$$\mathrm{Fr}\left(\sum_{i=0}^{\ell'-1} z_i\xi^i\right) = \sum_{i=0}^{\ell'-1} z_i\xi^{ip}, \qquad (z_i \in \mathbb{Z}_{p^m}), \tag{2.2}$$

when ξ of order $p^{\ell'}-1$ in $\mathrm{GR}(p^m,\ell')$. Then Fr is an automorphism of $\mathrm{GR}(p^m,\ell')$ and

$$\mathrm{GR}(p^m,\ell)=\left\{\theta\in \mathrm{GR}(p^m,\ell');\mathrm{Fr}^{\ell}(\theta)=\theta\right\}, \tag{2.3}$$

when $\ell \mid \ell'$. For additional details, see [9].

A code of length n over $\mathrm{GR}(p^m,\ell)$ is a non empty subset of $\mathrm{GR}(p^m,\ell)^n$, and it is called a linear code over $\mathrm{GR}(p^m,\ell)$ if it is an $\mathrm{GR}(p^m,\ell)$-submodule of $\mathrm{GR}(p^m,\ell)^n$. A linear code is called a λ-constacyclic code if it remains unchanged under the following shift operation:

$$\tau_\lambda(t_0,t_1,...,t_{n-1})=(\lambda t_{n-1},t_0,...,t_{n-2}),$$

where λ is a fixed unit of $\mathrm{GR}(p^m,\ell)$. If λ is equal to 1 (respectively -1), then the code is a cyclic (respectively negacyclic) code.

A codeword, represented by the tuple $(t_0,t_1,...,t_{n-1})$, can also be represented as a polynomial, $t(x)=t_0+t_1x+...+t_{n-1}x^{n-1}\in \frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^n-\lambda\rangle}$. Then $\tau_\lambda(t(x))=xt(x)$. As a result, λ-constacyclic codes of length n over $\mathrm{GR}(p^m,\ell)$ can be viewed as ideals of $\frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^n-\lambda\rangle}$.

The Euclidean inner product between two n-tuples $\mathbf{t}=(t_0,t_1,...,t_{n-1})$ and $\mathbf{t'}=(t'_0,t'_1,...,t'_{n-1})$ in $\mathrm{GR}(p^m,\ell)^n$ is defined as

$$\mathbf{t}.\mathbf{t'}=t_0t'_0+t_1t'_1+...+t_{n-1}t'_{n-1}.$$

Two n-tuples $\mathbf{t}$, $\mathbf{t'}$ are considered orthogonal when $\mathbf{t}.\mathbf{t'}=0$. The dual code $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ of length n over $\mathrm{GR}(p^m,\ell)$ is the set of n-tuples over $\mathrm{GR}(p^m,\ell)$ that are orthogonal to all codewords of $\mathcal{C}$, i.e.,

$$\mathcal{C}^\perp=\{\mathbf{t}\in \mathrm{GR}(p^m,\ell);\mathbf{t}.\mathbf{t'}=0,\ \text{for all } t'\in\mathcal{C}\}.$$

A code $\mathcal{C}$ is self-orthogonal if $\mathcal{C}\subseteq\mathcal{C}^\perp$. A code $\mathcal{C}$ is self-dual if it is equal to its dual. When m is an even number, the code $\left\langle p^{\frac{m}{2}}\right\rangle$ is a self-dual code, which is called the trivial self-dual code. The following outcome is widely recognized.

Proposition 2.3. *[10] For any linear code $\mathcal{C}$ length of n over* $\mathrm{GR}(p^m,\ell)$, $|\mathcal{C}||\mathcal{C}^\perp|=|\ \mathrm{GR}(p^m,\ell)\ |^n$.

It's important to note that the dual of a cyclic code is also a cyclic code and the dual of a negacyclic code is also a negacyclic code. In general, the dual of a λ-constacyclic code has the following properties.

Proposition 2.4. *[11] If $\mathcal{C}$ is a λ-constacyclic code of lenght n over* $\mathrm{GR}(p^m,\ell)$, *then $\mathcal{C}^\perp$ is a λ^{-1}-constacyclic code of lenght n over* $\mathrm{GR}(p^m,\ell)$.

For a polynomial $t(x)\in \mathrm{GR}(p^m,\ell)[x]$ of degree d, its reciprocal polynomial is denoted $t^*(x)$ and defined as $x^dt\left(x^{-1}\right)$. In other words, if

$$t(x)=t_0+t_1x+\cdots+t_{d-1}x^{d-1}+t_dx^d,$$

then

$$t^*(x)=t_d+t_{d-1}x+\cdots+t_1x^{d-1}+t_0x^d.$$

A polynomial $t(x)$ over $\mathrm{GR}(p^m,\ell)$ is said to be self-reciprocal if $t^*(x)=\delta t(x)$ for some unit $\delta\in\mathrm{GR}(p^m,\ell)$. We have the following result:

Proposition 2.5. [11] *Let $\mathcal{C}$ be a λ-constacyclic code of lenght n over* $\mathrm{GR}(p^m,\ell)$, *then*

$$\mathcal{C}^\perp=\{z^*(x);z(x)t(x)=0\ \ in\ \frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^n-\lambda\rangle}\ for\ all\ \ t(x)\in\mathcal{C}\}. \tag{2.4}$$

The torsion codes are defined by:

Definition 2.6. Let $\mathcal{C}$ be a λ-constacyclic code of length n over $\mathrm{GR}(p^m, \ell)$. For $i = 0, ..., m-1$, the definition of the ith torsion code of $\mathcal{C}$ is as follows:

$$\mathrm{Tor}_i(\mathcal{C}) = \left\{ \overline{t(x)}; p^i t(x) \in \mathcal{C} \right\},$$

where $- : \mathrm{GR}(p^m, \ell) \longrightarrow \mathbb{F}_{p^\ell}$ is the canonical homomorphism. In case $i = 0$, it is called the residue code of $\mathcal{C}$ and is denoted by $\mathrm{Res}(\mathcal{C})$.

It is clear, for any $i = 0, ..., m-1$, that $\mathrm{Tor}_i(\mathcal{C})$ is a $\bar{\lambda}$-constacyclic code of length n over $\mathbb{F}_{p^\ell}$.

In this paper, we consider $n = p^s\eta$ where η and s are positive integers such that $\gcd(\eta, p) = 1$. Let λ be a unit of $\mathrm{GR}(p^m, \ell)$ of the form

$$\lambda = \xi_0 + p\xi_1 + \cdots + p^{m-1}\xi_{m-1} = \xi_0 + p\gamma,$$

where $\xi_i \in \mathcal{T}$ for $i = 0, \ldots, m-1$ and $\xi_0 \neq 0$. We further assume that $\xi_1 \neq 0$, which means that γ is a unit in $\mathrm{GR}(p^m, \ell)$. Define $\alpha = \xi_0^{p^{(q+1)\ell - s}} = \xi_0^{p^{\ell - r}} \in \mathcal{T}$, where $s = q\ell + r$ and $0 \leq r \leq \ell - 1$. Then, we have $\alpha^{p^s} = \xi_0^{p^{(q+1)\ell}} = \xi_0$.

3 $(\xi_0 + p\gamma)$-constacyclic codes of length p^s over $\mathrm{GR}(p^m, \ell)$

As previously discussed in Section 2, $(\xi_0 + p\gamma)$-constacyclic codes of length p^s over $\mathrm{GR}(p^m, \ell)$ are ideals of the ring $\frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^{p^s} - (\xi_0 + p\gamma)\rangle}$.

Theorem 3.1. [12] *Suppose γ is a unit in $\mathrm{GR}(p^m, \ell)$, and ξ_0, α are nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s} = \xi_0$. Then, the following statements hold:*

(i) The quotient ring $\frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^{p^s} - (\xi_0 + p\gamma)\rangle}$ is a chain ring with maximal ideal $\langle x - \alpha\rangle$ and nilpotency index $p^s m$.

(ii) The $(\xi_0 + p\gamma)$-constacyclic codes of length p^s over $\mathrm{GR}(p^m, \ell)$ are of the form $\mathcal{C}_k = \left\langle (x - \alpha)^k \right\rangle$, where k is an integer in $\{0, ..., p^s m\}$.

(iii) For each k in $\{0, ..., p^s m\}$, we have $| \mathcal{C}_k | = p^{\ell(p^s m - k)}$.

(iv) In $\frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^{p^s} - (\xi_0 + p\gamma)\rangle}$, $\langle (x - \alpha)^{p^s} \rangle = \langle p \rangle$.

(v) The dual code of $\mathcal{C}_k = \left\langle (x - \alpha)^k \right\rangle$ is $\mathcal{C}_k^\perp = \left\langle \left(x - \alpha^{-1}\right)^{p^s m - k} \right\rangle$, and then in particular, $| \mathcal{C}_k^\perp | = p^{\ell k}$.

In [13] Ding et al. introduced the notion of the b-symbol, denoted $\pi_b(\mathbf{z})$, of a vector $\mathbf{z}$ in Δ^n, where $b \geq 1$ is an integer and Δ is an alphabet. $\pi_b(\mathbf{z})$ is defined by

$$\pi_b(\mathbf{z}) = \left[(z_0, \ldots, z_{b-1}), (z_1, \ldots, z_b), \ldots, (z_{n-1}, z_0, \ldots, z_{b-2}) \right] \in \left(\Delta^b\right)^n.$$

The b-distance between two vectors $\mathbf{z}$ and $\mathbf{y}$ is defined as

$$d_b(\mathbf{z}, \mathbf{y}) = \left| \{ 0 \leq i \leq n-1; (z_i, \ldots, z_{i+b-1}) \neq (y_i, \ldots, y_{i+b-1}) \} \right|.$$

The b-weight of a vector $\mathbf{z}$ is determined by the b-distance between $\mathbf{z}$ and the zero vector $\mathbf{0}$, as formally defined as

$$wt_b(\mathbf{z}) = \left| \{ 0 \leq i \leq n-1; (z_i, \ldots, z_{i+b-1}) \neq \mathbf{0} \} \right|,$$

where the subscripts are taken modulo n for reduction.

The b-distance of a code $\mathcal{C}$ is established as the smallest b-distance between any pair of distinct codewords $\mathbf{z}_1$ and $\mathbf{z}_2$ within $\mathcal{C}$. In other words:

$$d_b(\mathcal{C}) = \min\{ d_b(\mathbf{z}_1, \mathbf{z}_2); \mathbf{z}_1, \mathbf{z}_2 \in \mathcal{C}, \mathbf{z}_1 \neq \mathbf{z}_2 \}.$$

According to this definition of b-distance, when $b = 1$, then the b-distance is equivalent to the Hamming distance. If $b = 2$, then the b-distance is known as the symbol-pair distance.

In [7] Shixin Zhu et al. determined the Hamming distances of all $(1+p\gamma)$-constacyclic codes of length p^s over $\mathrm{GR}(p^m,\ell)$, where γ is a unit in $\mathrm{GR}(p^m,\ell)$. In the following, we use the same technics to calculate the b-symbol distance of $(\xi_0+p\gamma)$-constacyclic codes of length of p^s over $\mathrm{GR}(p^m,\ell)$, where γ is a unit in $\mathrm{GR}(p^m,\ell)$, ξ_0,α are nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s}=\xi_0$, and $1\leq b\leq \lfloor\frac{p}{2}\rfloor$.

Let $\mathcal{C}_k=\langle(x-\alpha)^k\rangle$, be a nonzero $(\xi_0+p\gamma)$-constacyclic code of length p^s over $\mathrm{GR}(p^m,\ell)$, where k is an element of the set $\{0,...,p^sm-1\}$. We distinguish two cases

- Case $0\leq k\leq p^s(m-1)$: As $\langle 0\rangle\neq\mathcal{C}_{p^s(m-1)}\subset\cdots\subset\mathcal{C}_1\subset\mathcal{C}_0=\langle 1\rangle$. Therefore
$$d_b(\mathcal{C}_{p^s(m-1)})\geq\cdots\geq d_b(\mathcal{C}_1)\geq d_b(\mathcal{C}_0)=d_b(\langle 1\rangle)=b.$$
According to Theorem 3.1, $\mathcal{C}_{p^s(m-1)}=\langle(x-\alpha)^{p^s(m-1)}\rangle=\langle p^{m-1}\rangle$. So $d_b(\mathcal{C}_{p^s(m-1)})=b$, and therefore, $d_b(\mathcal{C}_k)=b$.
- Case $p^s(m-1)+1\leqslant k\leqslant p^sm-1$: we can write $k=p^s(m-1)+i$ where $1\leqslant i\leqslant p^s-1$. Hence, $\mathcal{C}_k=\langle(x-\alpha)^{p^s(m-1)+i}\rangle=\langle p^{m-1}(x-\alpha)^i\rangle$. Thus, each code $\mathcal{C}_k$ is the code $\langle(x-\overline{\alpha})^i\rangle$ of length p^s over $\mathbb{F}_{p^\ell}$ multiplied by p^{m-1}. And so, $d_b(\mathcal{C}_k)=d_b(\langle(x-\overline{\alpha})^i\rangle)$.

Then the b-symbol distance of $(\xi_0+p\gamma)$-constacyclic codes of length p^s over GR (p^m,ℓ) can be determined through the combination of the results in two previous cases and the Theorem 9 in[14] as follows:

Theorem 3.2. *Suppose γ is a unit in $\mathrm{GR}(p^m,\ell)$, ξ_0,α are nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s}=\xi_0$, and $1\leq b\leq\lfloor\frac{p}{2}\rfloor$. Then the b-distance of the nonzero $(\xi_0+p\gamma)$-constacyclic code $\mathcal{C}_k=\langle(x-\alpha)^k\rangle$ of length p^s over $\mathrm{GR}(p^m,\ell)$, where $k\in\{0,1,...,p^sm-1\}$, is specified as follows:*

$$d_b(\mathcal{C}_k)=\begin{cases}b, & \text{if } 0\leq k\leq p^s(m-1),\\ (\tau+b)(\pi+1)p^\omega, & \text{if } k=p^sm-p^{s-\omega}+\pi p^{s-\omega-1}+\tau,\\ & \quad \text{where } 0\leq\omega\leq s-2, 0\leq\pi\leq p-2 \text{ and } b>\tau(\pi+1),\\ b(\pi+2)p^\omega, & \text{if } p^sm-p^{s-\omega}+\pi p^{s-\omega-1}+\tau\leq k\leq p^sm-p^{s-\omega}+(\pi+1)p^{s-\omega-1},\\ & \text{where } 0\leq\omega\leq s-2, 0\leq\pi\leq p-2 \text{ and } b\leq\tau(\pi+1),\\ (\pi+b)p^{s-1}, & \text{if } k=p^sm-p+\pi, \quad \text{where } 0\leq\pi\leq p-b,\\ p^s, & \text{if } k\geq p^sm-b+1.\end{cases}$$

4 $(\xi_0+p\gamma)$-constacyclic codes of length $p^s\eta$ over $\mathrm{GR}(p^m,\ell)$

Lemma 4.1 (Hensel's lemma). *[8] Let $f(x)$ be a monic polynomial in $\mathrm{GR}(p^m,\ell)[x]$. If $\overline{f(x)}$ can be factored as $\overline{f(x)}=g_1(x)g_2(x)...g_t(x)$ in $\mathbb{F}_{p^\ell}[x]$, where $g_1(x),g_2(x),...,g_t(x)$ are pairwise coprime polynomials over $\mathbb{F}_{p^\ell}$, then there exist $f_1(x),f_2(x),...,f_t(x)$ in $\mathrm{GR}(p^m,\ell)[x]$ such that $f(x)=f_1(x)f_2(x)...f_t(x)$, with $\overline{f_k(x)}=g_k(x)$ for all $k=1,...,t$.*

Hensel's lemma is a crucial tool in the analysis of finite Galois rings, which ensures the lifting of factorizations of coprime polynomials in $\mathrm{GR}(p^m,\ell)[x]$. Since η and p are coprime, $x^\eta-\alpha$ can be uniquely factored into monic basic irreducible (then irreducible) polynomials in $\mathrm{GR}(p^m,\ell)[x]$ as
$$x^\eta-\alpha=f_1(x)f_2(x)...f_t(x).$$

Now, let a' be the order of p^ℓ mudulo η, in particular $\frac{p^{a'\ell}-1}{\eta}$ is positive integer , and let ξ be an element of order $p^{a'\ell}-1$ in $\mathrm{GR}(p^m,a'\ell)$. If we note $\zeta=\xi^{\frac{p^{a'\ell}-1}{\eta}}$, then ζ is of order η in $\mathrm{GR}(p^m,a'\ell)$.

Next, let $\mathrm{GR}(p^m,a\ell)$ be an extension of $\mathrm{GR}(p^m,a'\ell)$ containing a root ε of $x^\eta-\alpha$. It's clear that $\varepsilon,\varepsilon\zeta,...,\varepsilon\zeta^{\eta-1}$ are in $\mathrm{GR}(p^m,a\ell)$, and are the distinct roots of $x^\eta-\alpha$, then for all $k=0,...,\eta-1$, then there exists a unique j_k in $\{1,...,t\}$ such that $f_{j_k}(\varepsilon\zeta^k)=0$, i.e., $f_{j_k}(x)$ is the minimal polynomial of $\varepsilon\zeta^k$ over $\mathrm{GR}(p^m,\ell)$.

We define the following equivalence relation $\sim$ on the set $\{0,1,2,...,\eta-1\}$ as follows:

$k \sim k'$ if and only if $\varepsilon\zeta^k$ and $\varepsilon\zeta^{k'}$ have the same minimal polynomial.

Let Γ be the set of complete representatives of all equivalence classes. For each $k \in \Gamma$, we define Γ_k as the class containing k, $a_k = |\Gamma_k|$, and $g_k(x) = f_{j_k}(x)$. It is important to note that $a_k = \deg g_k(x)$.

Proposition 4.2. *For each* $k \in \Gamma, \varepsilon\zeta^k \in \mathrm{GR}(p^m, a_k\ell)$, *and*

$$\{\varepsilon\zeta^j; j \in \Gamma_k\} = \{\phi^i(\varepsilon\zeta^k); i = 0, ..., a_k - 1\}, \tag{4.1}$$

where $\phi = \mathrm{Fr}^\ell$, *and* Fr *is the Frobenius automorphism of* $\mathrm{GR}(p^m, \ell.a!)$.

Proof. The homorphism $\Upsilon : \frac{\mathrm{GR}(p^m,\ell)[x]}{\langle g_k(x)\rangle} \longrightarrow \mathrm{GR}(p^m, \ell)[\varepsilon\zeta^k]$, such that for every $c(x) \in \frac{\mathrm{GR}(p^m,\ell)[x]}{\langle g_k(x)\rangle}$, $\Upsilon(c(x)) = c(\varepsilon\zeta^k)$ is an isomorphism, whence $\mathrm{GR}(p^m, \ell)[\varepsilon\zeta^k]$ is a Galois ring of characteristic p^m and cardinality $p^{ma_k\ell}$, then $\varepsilon\zeta^k \in \mathrm{GR}(p^m, a_k\ell)$. On the other hand, it is clear from (2.3) that for any θ in $\mathrm{GR}(p^m, a_k\ell)$, $g_k(\phi(\theta)) = \phi(g_k(\theta))$, then $\varepsilon\zeta^k, \phi(\varepsilon\zeta^k), ..., \phi^{a_k-1}(\varepsilon\zeta^k)$ are also roots of $g_k(x)$, so it suffices to show that these roots are pairwise distinct. Assume that $\phi^r(\varepsilon\zeta^k) = \varepsilon\zeta^k$, for $r = 1, ..., a_k - 1$, i.e., $\mathrm{Fr}^{r\ell}(\varepsilon\zeta^k) = \varepsilon\zeta^k$, by (2.3) again $\varepsilon\zeta^k \in \mathrm{GR}(p^m, r\ell)$, also $\mathrm{GR}(p^m, a_k\ell) \subseteq \mathrm{GR}(p^m, r\ell)$, which is impossible.

□

Remark 4.3. Let a be any positive integer. We denote $\mathcal{R}(a) = \frac{\mathrm{GR}(p^m,a\ell)[y]}{\langle y^{p^s}-\lambda\rangle}$. As $y^{p^s} = \lambda$ in $\mathcal{R}(a)$, it follows that $(\alpha^{-1}y)^{p^{s+m-1}} = 1$. Thus, we have:

$$(\alpha^{-1}y)^{\eta\eta'} = \alpha^{-1}y, \qquad \text{where } \eta\eta' = 1 \mod (p^{s+m-1}). \tag{4.2}$$

4.1 Discrete Fourier transform

The discrete Fourier transform (DFT) is utilized for codes of arbitrary length n, which may not necessarily be a power of prime numbers, i.e., in the case of $n = p^s\eta$ where $\gcd(p, \eta) = 1$. It's a widely used tool in analyzing linear codes over finite rings [7]. We use DFT as a crucial component in describing the structure of constacyclic codes over $\mathrm{GR}(p^m, \ell)$.

Definition 4.4. Let $\mathbf{z} = (z_{0,0}, \ldots, z_{\eta-1,0}, z_{0,1}, \ldots, z_{\eta-1,1}, \ldots, z_{0,p^s-1}, \ldots, z_{\eta-1,p^s-1}) \in \mathrm{GR}(p^m, \ell)^n$, and $z(x) = \sum_{i=0}^{\eta-1}\sum_{j=0}^{p^s-1} z_{i,j}x^{i+j\eta} \in \frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^n-\lambda\rangle}$ the corresponding polynomial of $\mathbf{z}$. We define the discrete Fourier transform of $\mathbf{z}$ by

$$(\widehat{z}_0, \widehat{z}_1, \ldots, \widehat{z}_{\eta-1}) \in \mathcal{R}(a)^\eta,$$

where $\widehat{z}_k = z\left((\alpha^{-1}y)^{\eta'}\varepsilon\zeta^k\right) = \sum_{i=0}^{\eta-1}\sum_{j=0}^{p^s-1} z_{i,j}y^{\eta' i+j}(\alpha^{-\eta'}\varepsilon\zeta^k)^i$. We thus define the Mattson-Solomon polynomial of $\mathbf{z}$ by

$$\widehat{\mathbf{z}}(x) = \sum_{k=0}^{\eta-1} \widehat{z}_k x^{\eta-k}.$$

The following lemma show that $\mathbf{z}$ can be recovered if its Mattson–Solomon polynomial is known.

Lemma 4.5. *Let* $\boldsymbol{z} \in \mathrm{GR}(p^m, \ell)^n$ *with* $\widehat{\boldsymbol{z}}(x)$ *its Mattson-Solomon polynomial. Then for all* $0 \leqslant d \leqslant \eta - 1$:

$$\sum_{j=0}^{p^s-1} z_{d,j}y^j = ((\alpha^{-1}y)^{\eta'}\varepsilon)^{-d}\frac{1}{\eta}\widehat{\boldsymbol{z}}\left(\zeta^d\right).$$

Proof. Let $0 \leqslant d \leqslant \eta - 1$,

$$\begin{aligned}\widehat{\mathbf{z}}\left(\zeta^d\right) &= \sum_{k=0}^{\eta-1} \widehat{z}_k \zeta^{-dk} = \sum_{k=0}^{\eta-1} \left(\sum_{i=0}^{\eta-1} \sum_{j=0}^{p^s-1} z_{i,j} y^{\eta' i+j} (\alpha^{-\eta'} \varepsilon \zeta^k)^i \right) \zeta^{-kd} \\ &= \sum_{i=0}^{\eta-1} \sum_{j=0}^{p^s-1} z_{i,j} y^{\eta' i+j} (\alpha^{-\eta'} \varepsilon)^i \sum_{k=0}^{\eta-1} \zeta^{k(i-d)} \\ &= \eta((\alpha^{-1}y)^{\eta'} \varepsilon)^d \sum_{j=0}^{p^s-1} z_{d,j} y^j.\end{aligned}$$

Note that if $i \neq d$, $\sum\limits_{k=0}^{\eta-1} \zeta^{k(i-d)} = 0$, and if $i = d$, $\sum\limits_{k=0}^{\eta-1} \zeta^{k(i-d)} = \eta$. □

In the following we define the following two operations on $\mathcal{R}(a)^\eta$:

$$(z_0, ..., z_{\eta-1}) + (z'_0, ..., z'_{\eta-1}) = (z'_0 + z_0, ..., z_{\eta-1} + z'_{\eta-1}),$$
$$(z_0, ..., z_{\eta-1}) * (z'_0, ..., z'_{\eta-1}) = (z_0 z'_0, ..., z_{\eta-1} z'_{\eta-1}).$$

Proposition 4.6. *With the previous notations the map*

$$\begin{array}{rccc} \psi : & \frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^n-\lambda\rangle} & \longrightarrow & \mathcal{R}(a)^\eta \\ & z(x) & \longmapsto & (\widehat{z}_0, \widehat{z}_1, \ldots, \widehat{z}_{\eta-1}) \end{array},$$

is a ring homomorphism.

Proof. Let $z_1(x), z_2(x)$ be two polynomails in $\frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^n-\lambda\rangle}$. It is clear that $\psi(z_1(x) + z_2(x)) = \psi(z_1(x)) + \psi(z_2(x))$. By Euclid's division theorem $z_1(x)z_2(x) = q(x)(x^n - \lambda) + r(x)$, where $\deg(r(x)) \leq n - 1$.

As for all $k = 0, ..., \eta-1$, $\left((\alpha^{-1}y)^{\eta'} \varepsilon \zeta^k\right)^n - \lambda = 0$, then $z_1\left((\alpha^{-1}y)^{\eta'} \varepsilon \zeta^k\right) z_2\left((\alpha^{-1}y)^{\eta'} \varepsilon \zeta^k\right) = r\left((\alpha^{-1}y)^{\eta'} \varepsilon \zeta^k\right)$ i.e.,

$$\psi(z_1(x)z_2(x)) = \psi(z_1(x)) * \psi(z_2(x)).$$

□

Let ϕ be as defined in Proposition 4.2. We extend ϕ to $\mathcal{R}(a)$ by defining $\hat{\phi}(y) = y$. According to Proposition 4.2, $(\widehat{z}_0, \widehat{z}_1, \ldots, \widehat{z}_{\eta-1})$ is determined by $(\widehat{z}_k)_{k\in\Gamma}$, and $\widehat{z}_k \in \mathcal{R}(a_k)$. Then by Lemma 4.5,

$$\begin{array}{rccc} \psi : & \frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^n-\lambda\rangle} & \longrightarrow & \oplus_{k\in\Gamma}\mathcal{R}(a_k) \\ & z(x) & \longmapsto & (\widehat{z}_k)_{k\in\Gamma} \end{array},$$

is an injection homomorphism. Moreover we have

$$|\oplus_{k\in\Gamma}\mathcal{R}(a_k)| = \prod_{k\in\Gamma} |\mathcal{R}(a_k)| = \prod_{k\in\Gamma} p^{m\ell a_k p^s} = p^{m\ell n} = \left|\frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^n-\lambda\rangle}\right|.$$

This shows that ψ is an isomorphism. We summarize our results as follows:

Theorem 4.7. *Let γ be a unit in $\mathrm{GR}(p^m, \ell)$, ξ_0 and α be nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s} = \xi_0$. Let $\mathcal{C}$ be a $(\xi_0 + p\gamma)$-constacyclic code of length $p^s\eta$ (η prime to p) over $\mathrm{GR}(p^m, \ell)$. Then*

$$\mathcal{C} \cong \oplus_{k\in\Gamma}\mathcal{C}_k, \tag{4.3}$$

where $\mathcal{C}_k = \left\{ z\left((\alpha^{-1}y)^{\eta'} \varepsilon \zeta^k\right); z(x) \in \mathcal{C} \right\}$ is an ideal of $\mathcal{R}(a_k)$.

The combination of Theorem 3.1 and Theorem 4.7 leads to the following corollary.

Corollary 4.8. *Let γ be a unit in $\mathrm{GR}(p^m, \ell)$, ξ_0 and α be nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s} = \xi_0$. Then the number of distinct $(\xi_0 + p\gamma)$-constacyclic codes of length $p^s\eta$ over $\mathrm{GR}(p^m, \ell)$, with $\gcd(p, \eta) = 1$, is $(p^s m + 1)^{|\Gamma|}$.*

4.2 Generator polynomials

The following lemma will prove valuable in determining generator polynomials.

Lemma 4.9. *For each $k, k' \in \Gamma$,*

(i) if $k' \neq k$, then $g_k\left(\left(\alpha^{-1}y\right)^{\eta'}\varepsilon\zeta^{k'}\right)$ is a unit in $\mathcal{R}\left(b_{k'}\right)$;

(ii) $g_k\left(\left(\alpha^{-1}y\right)^{\eta'}\varepsilon\zeta^{k}\right) \in \langle y-\alpha\rangle$ and $g_k\left(\left(\alpha^{-1}y\right)^{\eta'}\varepsilon\zeta^{k}\right) \notin \left\langle (y-\alpha)^2\right\rangle$,

where $g_k(x)$ is the minimal polynomial of $\varepsilon\zeta^k$ over $\mathrm{GR}(p^m,\ell)$.

Proof. (i) We know that $g_k(x) = \prod\limits_{j\in\Gamma_k}\left(x-\varepsilon\zeta^j\right)$. Then,

$$\begin{aligned} g_k\left(\left(\alpha^{-1}y\right)^{\eta'}\varepsilon\zeta^{k'}\right) &= \prod_{j\in\Gamma_k}\left(\left(\alpha^{-1}y\right)^{\eta'}\varepsilon\zeta^{k'}-\varepsilon\zeta^j\right) \\ &= \prod_{j\in\Gamma_k}\left[\left(\left(\alpha^{-1}y\right)^{\eta'}-1\right)\varepsilon\zeta^{k'}+\left(\varepsilon\zeta^{k'}-\varepsilon\zeta^j\right)\right]. \end{aligned}$$

It's clear that $\left(\left(\alpha^{-1}y\right)^{\eta'}-1\right) = \alpha^{-1}(y-\alpha)\left(\left(\alpha^{-1}y\right)^{\eta'-1}+\ldots+1\right)$, since $(y-\alpha)$ is a nilpotent element in $\mathcal{R}(b_{k'})$, then $\left(\left(\alpha^{-1}y\right)^{\eta'}-1\right)\varepsilon\zeta^{k'}$ is also a nilpotent element in $\mathcal{R}(b_{k'})$.

As for each $j\in\Gamma_k, j\neq k'$, then $\varepsilon\zeta^{k'}-\varepsilon\zeta^j$ is a unit (cf Proposition 2.2). So, the conclusion is obtained.

(ii) Since $x^\eta-\alpha = \prod\limits_{j\in\Gamma} g_j(x)$, then $\prod\limits_{j\in\Gamma} g_j\left(\left(\alpha^{-1}y\right)^{\eta'}\varepsilon\xi^k\right) = \left(\left(\alpha^{-1}y\right)^{\eta'}\varepsilon\xi^k\right)^\eta-\alpha = y-\alpha$.

from (i) we have $\kappa = \prod\limits_{j\in\Gamma\setminus\{k\}} g_j\left(\left(\alpha^{-1}y\right)^{\eta'}\varepsilon\xi^k\right)$ is a unit. Hence, $g_k\left(\left(\alpha^{-1}y\right)^{\eta'}\varepsilon\zeta^k\right) = \kappa^{-1}(y-\alpha)$.

□

Theorem 4.10. *Let γ be a unit in $\mathrm{GR}(p^m,\ell)$, ξ_0 and α be nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s}=\xi_0$. Let $\mathcal{C}$ be a $(\xi_0+p\gamma)$-constacyclic code of length $p^s\eta$ (η is prime to p) over $\mathrm{GR}(p^m,\ell)$. Then*

$$\mathcal{C} = \left\langle \prod_{k\in\Gamma}\left[g_k(x)\right]^{i_k}\right\rangle, \qquad (0\leq i_k\leq p^s m),$$

where $x^\eta-\alpha = \prod\limits_{k\in\Gamma} g_k(x)$ is the unique factorization of $x^\eta-\alpha$ into a product of monic basic irreducible pairwise coprime polynomials in $\mathrm{GR}\left(p^m,\ell\right)[x]$. Moreover $|\,\mathcal{C}\,| = \prod\limits_{i=1}^{t} p^{\ell\deg(g_k(x))(p^s m-i_k)}$.

Proof. By Theorem 4.7, we have that $\mathcal{C}$ is isomorphic to $\bigoplus_{k\in\Gamma}\mathcal{C}_k$, where $\mathcal{C}_k$ is an ideal of $\mathcal{R}(a_k)$ given by $\mathcal{C}_k = \left\{c\left(\left(\alpha^{-1}y\right)^{\eta'}\varepsilon\zeta^k\right); c(x)\in\mathcal{C}\right\}$. From Theorem 3.1, we know that $\mathcal{C}_k$ is generated by $(y-\alpha)^{i_k}$, where $i_k\in\{0,1,\ldots,p^s m\}$. Using Lemma 4.9, we can show that $\mathcal{C}$ is generated by the product $\prod\limits_{k\in\Gamma}[g_k(x)]^{i_k}$, where $i_k\in\{0,1,\ldots,p^s m\}$, and $|\,\mathcal{C}\,| = \prod\limits_{k\in\Gamma}|\,\langle(y-\alpha)^{i_k}\rangle\,| = \prod\limits_{k\in\Gamma} p^{\ell a_k(p^s m-i_k)}$. □

5 Dual codes of constacyclic codes

In this section, our objective is to determine the dual of a $(\xi_0+p\gamma)$-constacyclic code of length $p^s\eta$ over $\mathrm{GR}(p^m,\ell)$, where $\gcd(p,\eta)=1$, γ is a unit in $\mathrm{GR}(p^m,\ell)$, and ξ_0,α are nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s}=\xi_0$. We express the code $\mathcal{C}$ as a direct sum of its component codes, i.e., $\mathcal{C}\cong\oplus_{k\in\Gamma}\mathcal{C}_k$.

We begin by recalling that $\mathcal{C}^{\perp}$ is a $(\xi_0+p\gamma)^{-1}$-constacyclic code of length $p^s\eta$ over $\mathrm{GR}(p^m,\ell)$, and that

$$x^{\eta}-\alpha=\prod_{k\in\Gamma}g_k(x),$$

where $g_k(x)$ is the minimal polynomial of $\varepsilon\zeta^k$, as defined earlier. Note that $(\xi_0+p\gamma)^{-1}=\xi_0^{-1}+p\gamma'$, for some unit γ' of $\mathrm{GR}(p^m,\ell)$ [15, Theorem 3.20]. We then define, for all $k\in\Gamma$, the polynomial $\widetilde{g}_k(x)$ by

$$\widetilde{g}_k(x)=g_k(0)^{-1}g_k^*(x),$$

where $\widetilde{g}_k(x)$ is a monic irreducible polynomial. Moreover, we have

$$x^{\eta}-\alpha^{-1}=\prod_{k\in\Gamma}\widetilde{g}_k(x).$$

The distinct roots of $x^{\eta}-\alpha^{-1}$ are given by $\varepsilon^{-1},\varepsilon^{-1}\zeta^{-1},...,\varepsilon^{-1}\zeta^{-(\eta-1)}$, and for all $k\in\Gamma$, $\widetilde{g}_k(\varepsilon^{-1}\zeta^{-k})=0$. Hence, $\widetilde{g}_k(x)$ is the minimal polynomial of $\varepsilon^{-1}\zeta^{-k}$. We denote for all $k\in\Gamma,\mathcal{C}_k^*$ as follows:

$$\mathcal{C}_k^*=\left\{z\left((\alpha y)^{\eta'}\varepsilon^{-1}\zeta^{-k}\right);z(x)\in\mathcal{C}^{\perp}\right\}\subseteq\frac{\mathrm{GR}(p^m,\ell a_k)[y]}{\langle y^{p^s}-(\xi_0+p\gamma)^{-1}\rangle}. \tag{5.1}$$

Lemma 5.1. *With the previous notations, for all k in Γ, $\mathcal{C}_k^{\perp}=\mathcal{C}_k^*$.*

Proof. Let k be an element of Γ, and let $u\left((\alpha y)^{\eta'}\varepsilon^{-1}\zeta^{-k}\right)\in\mathcal{C}_k^*$, where $u(x)\in\mathcal{C}^{\perp}$. By Proposition 2.5, for any $c(x)$ in $\mathcal{C}$, we have that $u^*(x)c(x)=0$ in $\frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^n-(\xi_0+p\gamma)\rangle}$. Furthermore, Proposition 4.6 gives us:

$$\widehat{u^*}_k\widehat{c}_k=0,\text{i.e.}\left((\alpha^{-1}y)^{\eta'}\varepsilon\zeta^k\right)^{\deg(u(x))}u\left((\alpha^{-1}y)^{-\eta'}\varepsilon^{-1}\zeta^{-k}\right)\hat{c}_k=0\quad\text{in}\quad\mathcal{R}(a_k).$$

Since $\left((\alpha^{-1}y)^{\eta'}\varepsilon\zeta^k\right)^{\deg(u(x))}$ is a unit in $\mathcal{R}(a_k)$, we obtain $u\left((\alpha^{-1}y)^{-\eta'}\varepsilon^{-1}\zeta^{-k}\right)\hat{c}_k=0$. By Euclid's division theorem, there exists $q(y)$ and $r(y)$ such that:

$$u\left((\alpha^{-1}y)^{-\eta'}\varepsilon^{-1}\zeta^{-k}\right)=q(y)+r(y)(y^{p^s}-(\xi_0+p\gamma)),$$

where $q(y)=0$ or $\deg q(y)<p^s$. Thus, in $\mathcal{R}(a_k)$, we have $q(y)\hat{c}_k=0$ for all $\hat{c}_k$ in $\mathcal{C}_k$. Using Proposition 2.5, we obtain $q^*(y)\in\mathcal{C}_k^{\perp}$. Moreover, we have

$$q^*(y)=y^{\deg(q(y))}q\left(\frac{1}{y}\right)=y^{\deg(q(y))}\left[u\left((\alpha y)^{\eta'}\varepsilon^{-1}\zeta^{-k}\right)-r\left(\frac{1}{y}\right)\left(\frac{1}{y^{p^s}}-(\xi_0+p\gamma)\right)\right].$$

Thus, in $\frac{\mathrm{GR}(p^m,\ell a_k)[y]}{\langle y^{p^s}-(\xi_0+p\gamma)^{-1}\rangle}$, there exists a unit ρ such that $u\left((\alpha y)^{\eta'}\varepsilon^{-1}\zeta^{-k}\right)=\rho q^*(y)\in\mathcal{C}_k^{\perp}$. Therefore, we conclude that $\mathcal{C}_k^*\subseteq\mathcal{C}_k^{\perp}$. On the other hand, according to Proposition 2.3, we have

$$|\,\mathcal{C}^{\perp}\,|=\prod_{k\in\Gamma}|\,\mathcal{C}_k^*\,|\leq\prod_{k\in\Gamma}|\,\mathcal{C}_k^{\perp}\,|=\prod_{k\in\Gamma}\frac{p^{ma_k\ell p^s}}{|\,\mathcal{C}_k\,|}=\frac{p^{mn\ell}}{|\,\mathcal{C}\,|}=|\,\mathcal{C}^{\perp}\,|\,.$$

Therefore, it is necessary that for every k in Γ, $\mathcal{C}_k^{\perp}=\mathcal{C}_k^*$. □

Now, let $\mathcal{C}=\left\langle\prod_{k\in\Gamma}[g_k(x)]^{i_k}\right\rangle$ be a $(\xi_0+p\gamma)$-constacyclic code of length $p^s\eta$ $(\gcd(p,\eta)=1)$ over $\mathrm{GR}(p^m,\ell)$, where $0\leq i_k\leq p^sm$. Then for any $k\in\Gamma,\mathcal{C}_k=\left\langle(y-\alpha)^{i_k}\right\rangle$, i.e. by Lemma 5.1, $\mathcal{C}_k^*=\mathcal{C}_k^{\perp}=\left\langle(y-\alpha^{-1})^{p^sm-i_k}\right\rangle$. As $\widetilde{g}_k(x)$ is the minimal polynomial of $\varepsilon\zeta^{-k}$. So, by Theorem 4.10,

$$\mathcal{C}^{\perp}=\left\langle\prod_{k\in\Gamma}[\widetilde{g}_i(x)]^{p^sm-i_k}\right\rangle=\left\langle\prod_{k\in\Gamma}[g_i^*(x)]^{p^sm-i_k}\right\rangle.$$

Therefore, it can be inferred that the following theorem holds.

Theorem 5.2. *Let γ be a unit in $\mathrm{GR}(p^m,\ell)$, ξ_0 and α be nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s}=\xi_0$. Let $\mathcal{C}=\left\langle \prod_{k\in\Gamma}[g_k(x)]^{i_k}\right\rangle$ be a $(\xi_0+p\gamma)$-constacyclic code of length $p^s\eta$ $(\gcd(p,\eta)=1)$ over $\mathrm{GR}(p^m,\ell)$, where $0\le i_k\le p^s m$. Then*

$$\mathcal{C}^{\perp}=\left\langle \prod_{k\in\Gamma}[g_k^*(x)]^{p^s m-i_k}\right\rangle.$$

Let us proceed to determine self-dual $(\xi_0+p\gamma)$-constacyclic codes of length $n=p^s\eta$ over $\mathrm{GR}(p^m,\ell)$, where $\gcd(p,\eta)=1$. We begin by considering the following lemma.

Lemma 5.3. *[15] Suppose R is a chain ring with a maximal ideal $\langle\varrho\rangle$, and its nilpotency is denoted by e. Let λ be a unit of R such that $\lambda-\lambda^{-1}$ is also a unit. In such cases, a self-dual λ-constacyclic code C of length n over R can only exist when e is an even number. Furthermore, if e is indeed an even number, then the only self-dual λ-constacyclic code of length n over R is $C=\langle\varrho^{\frac{e}{2}}\rangle$.*

Remark 5.4. Assume that γ is a unit in $\mathrm{GR}(p^m,\ell)$, and let ξ_0 be a nonzero element in the Teichmüller set $\mathcal{T}$ such that $\alpha^{p^s}=\xi_0$. By applying Proposition 2.2, $\lambda-\lambda^{-1}$ is a unit if and only if $\xi_0^2\neq 1$.

We can therefore deduce the following theorem.

Theorem 5.5. *Let γ be a unit in $\mathrm{GR}(p^m,\ell)$, ξ_0 and α be nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s}=\xi_0$ and $\xi_0^2\neq 1$. Then a self-dual $(\xi_0+p\gamma)$-constacyclic code $\mathcal{C}$ of length $p^s\eta$ $(\gcd(p,\eta)=1)$ over $\mathrm{GR}(p^m,\ell)$ can only exist if m is an even number. Moreover if m is an even number, then the only self-dual $(\xi_0+p\gamma)$-constacyclic code of length $p^s\eta$ over $\mathrm{GR}(p^m,\ell)$ is $\mathcal{C}=\langle p^{\frac{m}{2}}\rangle$.*

We now consider the case where $\xi_0^2=1$, and begin by introducing the following lemma.

Lemma 5.6. *Let γ be a unit in $\mathrm{GR}(p^m,\ell)$, and suppose ξ_0 and α are nonzero elements in the Teichmüller set $\mathcal{T}$ satisfying $\alpha^{p^s}=\xi_0$ and $\xi_0^2=1$. Let $\mathcal{C}_k=\langle(x-\alpha)^k\rangle$ be an ideal of $\frac{\mathrm{GR}(p^m,\ell)}{\langle x^{p^s}-\xi_0+p\gamma\rangle}$ for some $k=0,\ldots,p^s m$. Then, it follows that in $\frac{\mathrm{GR}(p^m,\ell)}{\langle x^{p^s}-(\xi_0+p\gamma)^{-1}\rangle}$, we have $\mathcal{C}_k=\langle(x-\alpha)^k\rangle$.*

Proof. The lemma is straightforward for $k=0,\ldots,p^s-1$. However, for $k\ge p^s$, i.e., $k=tp^s+i$, where $i=0,\ldots,p^s-1$ and $t=0,\ldots,m-1$, we can observe from Theorem 3.1 that $\mathcal{C}_k=\langle p^t(x-\alpha)^k\rangle$. □

Consider a $(\xi_0+p\gamma)$-constacyclic code $\mathcal{C}$ over $\mathrm{GR}(p^m,\ell)$ of length $n=p^s\eta$ (η prime to p), given by $\mathcal{C}=\left\langle\prod_{k\in\Gamma}g_k(x)^{i_k}\right\rangle$, where ξ_0 and α are nonzero elements in the Teichmüller set $\mathcal{T}$ satisfying $\alpha^{p^s}=\xi_0$ and $\xi_0^2=1$, and γ is a unit of $\mathrm{GR}(p^m,\ell)$. Since $\widetilde{x^\eta-\alpha}=x^\eta-\alpha$, it follows that for any factor monic basic irreducible polynomial $g(x)$ of $x^\eta-\alpha$, $\widetilde{g}(x)$ is also a factor monic basic irreducible polynomial of $x^\eta-\alpha$. Therefore, without loss of generality, we can assume $\Gamma=\{1,\ldots,t\}$, and we can express the generator polynomial of $\mathcal{C}$ as

$$g_1(x)^{i_1}\cdots g_\sigma(x)^{i_\sigma}g_{\sigma+1}(x)^{i_{\sigma+1}}\cdots g_{\sigma+\rho}(x)^{i_{\sigma+\rho}}\tilde{g}_{\sigma+1}(x)^{i_{\sigma+\rho+1}}\cdots\tilde{g}_{\sigma+\rho}(x)^{i_{\sigma+2\rho}},\tag{5.2}$$

where σ and ρ are integers such that $t=\sigma+2\rho$, and for all $k=1,\ldots,\sigma$, $g_k(x)$ is self-reciprocal polynomial.

Now let's write $\mathcal{C}=\oplus_{k\in\Gamma}\mathcal{C}_k$ and $\mathcal{C}^{\perp}=\oplus_{k\in\Gamma}\mathcal{D}_k$, where $\mathcal{C}_k$ and $\mathcal{D}_k$ are ideals of $\mathcal{R}(a_k)$. According to Theorem 4.10, for any $k\in\Gamma$, $\mathcal{C}_k=\langle(y-\alpha)^{i_k}\rangle$. On the other hand, by Lemma 5.1, $\mathcal{D}_k=\mathcal{C}_{j_k}^{\perp}=\langle(y-\alpha)^{p^s m-i_{j_k}}\rangle$ in $\frac{\mathrm{GR}(p^m,\ell a_k)[y]}{\langle y^{p^s}-(\xi_0+p\gamma)^{-1}\rangle}$, where $j_k\in\Gamma$ such that $-k\in\Gamma_{j_k}$. Thus, by Lemma 5.6 , $\mathcal{D}_k=\langle(y-\alpha)^{p^s m-i_{j_k}}\rangle$ in $\mathcal{R}(a_k)$. Thus, $\mathcal{C}$ is self-dual if and only if for all $k\in\Gamma$, $i_k=p^s m-i_{j_k}$. Since $\tilde{g}_k(x)$ is the minimal polynomial of $\varepsilon\zeta^{j_k}$, then $g_{j_k}(x)=\tilde{g}_k(x)$. Then $\mathcal{C}$ is self-dual if and only if for all $k=1,..,\sigma, i_k=p^s m-i_k$ and for all $k=\sigma+1,..,\sigma+\rho, i_k=p^s m-i_{k+\rho}$. We have therefore established the following theorem.

Theorem 5.7. *Suppose we are given a unit γ in $\mathrm{GR}(p^m,\ell)$, and two nonzero elements ξ_0 and α in the Teichmüller set $\mathcal{T}$ such that $\alpha^{p^s}=\xi_0$ and $\xi_0^2=1$. Let $\mathcal{C}$ be a $(\xi_0+p\gamma)$-constacyclic code of length $p^s\eta$ (with $\gcd(p,\eta)=1$) over $\mathrm{GR}(p^m,\ell)$ with a generator polynomial as defined in (5.2).*

(i) If $x^\eta-\alpha$ has a factor monic basic irreducible self-reciprocal polynomial, then $\mathcal{C}$ is a self-dual if and only if p^sm is an even number and the generator polynomial of $\mathcal{C}$ is in the form

$$g_1(x)^{\frac{p^sm}{2}}\cdots g_\sigma(x)^{\frac{p^sm}{2}}g_{\sigma+1}(x)^{i_{\sigma+1}}\cdots g_{\sigma+\rho}(x)^{i_{\sigma+\rho}}\tilde{g}_{\sigma+1}(x)^{p^sm-i_{\sigma+1}}\cdots\tilde{g}_{\sigma+\rho}(x)^{p^sm-i_{\sigma+\rho}}.$$

(ii) If $x^\eta-\alpha$ has not a factor monic basic irreducible self-reciprocal polynomial, then $\mathcal{C}$ is a self-dual if and only if the generator polynomial of $\mathcal{C}$ has the form

$$g_1(x)^{i_1}\cdots g_\rho(x)^{i_\rho}\tilde{g}_1(x)^{p^sm-i_1}\cdots\tilde{g}_\rho(x)^{p^sm-i_\rho}.$$

Corollary 5.8. *Let γ be a unit in $\mathrm{GR}(p^m,\ell)$, and suppose ξ_0 and α are nonzero elements in the Teichmüller set $\mathcal{T}$ satisfying $\alpha^{p^s}=\xi_0$ and $\xi_0^2=1$. Then, the number of distinct self-dual $(\xi_0+p\gamma)$-constacyclic codes of length $p^s\eta$ ($\gcd(p,\eta)=1$) over $\mathrm{GR}(p^m,\ell)$ is $(p^sm+1)^\rho$, where ρ is defined as in (5.2).*

Lemma 5.9. *Let γ be a unit in $\mathrm{GR}(p^m,\ell)$, ξ_0 and α be nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s}=\xi_0$. Then in $\frac{\mathrm{GR}(p^m,\ell)[x]}{\langle x^n-(\xi_0+p\gamma)\rangle}$, $\langle(x^\eta-\alpha)^{p^s}\rangle=\langle p\rangle$, where $n=p^s\eta$ and $\gcd(p,\eta)=1$.*

Proof. Using the unique factorization of $x^\eta-\alpha$ into a product of monic basic irreducible pairwise coprime polynomials in $\mathrm{GR}(p^m,\ell)[x]$, we can express $(x^\eta-\alpha)^{p^s}$ as $\prod_{k\in\Gamma}g_k(x)^{p^s}$. By applying Lemma 4.9, we can conclude that for all $k\in\Gamma$, $\langle(x^\eta-\alpha)^{p^s}\rangle=\langle(y-\alpha)^{p^s}\rangle$ in $\mathcal{R}(a_k)$. Then, from Theorem 3.1, it follows that $\langle(x^\eta-\alpha)^{p^s}\rangle=\langle p\rangle$. Hence, we have $\langle(x^\eta-\alpha)^{p^s}\rangle\cong\oplus_{k\in\Gamma}\langle p\rangle=\langle p\rangle$. □

Corollary 5.10. *Let γ be a unit in $\mathrm{GR}(p^m,\ell)$, and suppose ξ_0 and α are nonzero elements in the Teichmüller set $\mathcal{T}$ satisfying $\alpha^{p^s}=\xi_0$ and $\xi_0^2=1$. Then the nontrivial self-dual $(\xi_0+p\gamma)$-constacyclic code of length $p^s\eta$ ($\gcd(p,\eta)=1$) over $\mathrm{GR}(p^m,\ell)$ exists if and only if there exists a basic irreducible polynomial factor $g(x)$ of $x^\eta-\alpha$ such that $g(x)$ is not a self-reciprocal polynomial.*

Proof. If there exists a basic irreducible polynomial factor $g(x)$ of $x^\eta-\alpha$ such that $g(x)$ is not a self-reciprocal polynomial, then the code $\langle g(x)g^*(x)^{p^sm-1}\rangle$ is a nontrivial self-dual $(\xi_0+p\gamma)$-constacyclic code of length $p^s\eta$ over $\mathrm{GR}(p^m,\ell)$. If any factor $g(x)$, a basic irreducible polynomial factor of $x^\eta-\alpha$, is a self-reciprocal polynomial, then any $(\xi_0+p\gamma)$-constacyclic code of length $p^s\eta$ over $\mathrm{GR}(p^m,\ell)$ is given by $\mathcal{C}=\langle\prod_{k\in\Gamma}g_k(x)^{i_k}\rangle$, where for any $k\in\Gamma$, $g_k(x)$ is a self-reciprocal polynomial. In this case, $\mathcal{C}$ is self-dual if and only if for any $k\in\Gamma$, $i_k=p^sm-i_k$, which is possible only when p^sm is even. Furthermore, according to the previous lemma, $\mathcal{C}=\langle p\rangle$, and thus, $\mathcal{C}$ is trivial. □

Example 5.11. Consider the polynomial factorization $x^7-1=g_1(x)g_2(x)g_3(x)$ in $\mathbb{Z}_4[x]$,

$$g_1(x)=x-1,\quad g_2(x)=x^3+2x^2+x-1,\quad g_3(x)=x^3-x^2+2x-1.$$

Then the self-dual 3-constacyclic code of length 28 over $\mathbb{Z}_4$ is of the form

$$\left\langle g_1(x)^8g_2(x)^ig_3(x)^{16-i}\right\rangle,$$

where $i\in\{0,\dots,16\}$.

Example 5.12. Consider the polynomial factorization $x^4-1=g_1(x)g_2(x)g_3(x)$ in $\mathbb{Z}_9[x]$, where

$$g_1(x)=x-1,\quad g_2(x)=x+1,\quad g_3(x)=x^2+1.$$

Since each $g_i(x)$ for $i=1,2,3$ is a self-reciprocal polynomial, the trivial code $\langle 3\rangle$ is the unique self-dual 4-constacyclic code of length $4\cdot 9$ over $\mathbb{Z}_9$.

6 MDS b-symbol distance

Recently, the construction of Maximum Distance Separable (MDS) b-symbol codes has become a key area in error-correcting code research. MDS b-symbol codes are considered optimal as they possess the highest possible error-correction capability among b-symbol codes. It is a commonly known that the parameters of an $[n; k; d_b]$ code over R must comply with the Singleton bound [13], which states that $\mid C \mid \leq R^{(n-d_b(C)+1)}$. A code C is considered an MDS b-symbol if $\mid C \mid = R^{(n-d_b(C)+1)}$. This section aims to identify all MDS b-symbol $(\xi_0 + p\gamma)$-constacyclic codes of length $2p^s$ over $\mathrm{GR}(p^m, \ell)$, when $b = 1$ and $b = 2$. We'll begin with a key lemma.

Lemma 6.1. *[16] Let γ be a unit in $\mathrm{GR}(p^m, \ell)$, ξ_0 and α be nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s} = \xi_0$. Let $\mathcal{C}$ be a $(\xi_0 + p\gamma)$-constacyclic code of length $p^s\eta$ (with $\gcd(p, \eta) = 1$) over $\mathrm{GR}(p^m, \ell)$. Then, the following are true:*

(i) $d_b(\mathcal{C}) = d_b(\mathrm{Tor}_{m-1}(\mathcal{C}))$.

(ii) The code $\mathcal{C}$ is an MDS b-symbol code if and only if $\mathrm{Res}(\mathcal{C}) = \mathrm{Tor}_{m-1}(\mathcal{C})$ and $\mathrm{Tor}_{m-1}(\mathcal{C})$ is an MDS b-symbol code of length $p^s\eta$ over $\mathbb{F}_{p^\ell}$.

This prompts us to compute $\mathrm{Res}(\mathcal{C})$ and $\mathrm{Tor}_{m-1}(\mathcal{C})$, but before that, we present the following lemma.

Lemma 6.2. *Let $f(x)$ be a divisor of $x^\eta - \overline{\alpha}$ in $\mathbb{F}_{p^\ell}[x]$. Then, for any positive integer j, $\left\langle f(x)^{p^s+j} \right\rangle = \left\langle f(x)^{p^s} \right\rangle$ in $\frac{\mathbb{F}_{p^\ell}[x]}{\langle x^{p^s\eta} - \overline{\xi_0} \rangle}$.*

Proof. Let $\widehat{f}(x) = \frac{x^\eta - \overline{\alpha}}{f(x)}$. As $f(x)^j$ and $\widehat{f}(x)^{p^s}$ are coprime in $\mathbb{F}_{p^\ell}[x]$, the there exist $\phi(x), \varphi(x) \in \mathbb{F}_{p^\ell}[x]$ such that $\phi(x)f(x)^j + \varphi(x)\hat{f}(x)^{p^s} = 1$ in $\mathbb{F}_{p^\ell}[x]$. We have also

$$\phi(x)f(x)^{p^s+j} = \left(1 - \varphi(x)\hat{f}(x)^{p^s}\right) f(x)^{p^s} = f(x)^{p^s} - \varphi(x)\left(x^\eta - \overline{\alpha}\right)^{p^s}.$$

Then in $\frac{\mathbb{F}_{p^\ell}[x]}{\langle x^{p^s\eta} - \overline{\xi_0} \rangle}$, $\phi(x)f(x)^{p^s+j} = f(x)^{p^s}$. Concretely $\left\langle f(x)^{p^s} \right\rangle \subseteq \left\langle f(x)^{p^s+j} \right\rangle$. The other inclusion is obvious. □

Theorem 6.3. *Let $\mathcal{C}$ be a $(\xi_0 + p\gamma)$-constacyclic code of lenght n over $\mathrm{GR}(p^m, \ell)$, with generator polynomial $\prod_{k\in\Gamma} [g_k(x)]^{i_k}$, where $0 \leq i_k \leq p^s m$ and $x^\eta - \alpha = \prod_{k\in\Gamma} [g_k(x)]^{i_k}$ be the unique factorization of $x^\eta - \alpha$ into a product of monic basic irreducible pairwise coprime polynomials in $\mathrm{GR}(p^m, \ell)[x]$. Then*

(i) $\mathrm{Res}(\mathcal{C}) = \left\langle \prod_{k\in\Gamma} \left[\overline{g_k(x)}\right]^{R_i} \right\rangle$,

(ii) $\mathrm{Tor}_{m-1}(\mathcal{C}) = \left\langle \prod_{k\in\Gamma} \left[\overline{g_k(x)}\right]^{T_i} \right\rangle$,

where for any $k \in \Gamma$, $T_k = \begin{cases} 0, & \text{if } i_k \leq (m-1)p^s, \\ i_k - (m-1)p^s, & \text{if } i_k \geq (m-1)p^s, \end{cases}$ and $R_k = \begin{cases} i_k, & \text{if } i_k \leq p^s, \\ p^s, & \text{if } i_k \geq p^s. \end{cases}$

Proof. (i) It is evident that $\mathrm{Res}(\mathcal{C}) = \left\langle \prod_{k\in\Gamma} \left[\overline{g_k(x)}\right]^{i_k} \right\rangle$. By utilizing Lemma 6.2, we see that $\mathrm{Res}(\mathcal{C}) = \left\langle \prod_{k\in\Gamma} \left[\overline{g_k(x)}\right]^{R_k} \right\rangle$.

(ii) Note that $\overline{\mathbf{c}} \in \mathrm{Tor}_{m-1}(\mathcal{C})$, if and only if $p^{m-1}\mathbf{c} \in \mathcal{C} \cap \left\langle p^{m-1} \right\rangle$. On the other hand from Lemma 5.9,

$$\left\langle p^{m-1} \right\rangle = \left\langle (x^m - \alpha)^{(m-1)p^s} \right\rangle = \left\langle \prod_{k\in\Gamma} [g_k(x)]^{(m-1)p^s} \right\rangle.$$

Then

$$\mathcal{C} \cap \langle p^{m-1} \rangle = \left\langle \prod_{k\in\Gamma} [g_k(x)]^{\max((m-1)p^s, i_k)} \right\rangle = \left\langle p^{m-1} \prod_{k\in\Gamma} [g_k(x)]^{T_k} \right\rangle.$$

We therefore obtain $\bar{\mathbf{c}} \in \mathrm{Tor}_{m-1}(\mathcal{C})$, if and only if $p^{m-1}\mathbf{c} \in \left\langle p^{m-1} \prod_{k\in\Gamma} [g_k(x)]^{T_k} \right\rangle$, i.e., $\bar{\mathbf{c}} \in \left\langle \prod_{k\in\Gamma} \left[\overline{g_k(x)}\right]^{T_k} \right\rangle$.

□

Corollary 6.4. *Let γ be a unit in $\mathrm{GR}(p^m, \ell)$, ξ_0 and α be nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s} = \xi_0$. Let $\mathcal{C}$ be a $(\xi_0 + p\gamma)$-constacyclic code of length $p^s\eta$ (η is prime to p) over $\mathrm{GR}(p^m, \ell)$. Then $\mathrm{Res}(\mathcal{C}) = \mathrm{Tor}_{m-1}(\mathcal{C})$ if and only if $\mathcal{C} = \langle 1 \rangle$. In particular $\langle 1 \rangle$ is the only MDS b-symbol.*

Proof. It is a direct consequence of Theorem 6.3 and Lemma 6.1. □

The following result is a direct consequence of Theorem 4.10.

Theorem 6.5. *Let γ be a unit in $\mathrm{GR}(p^m, \ell)$, ξ_0 and α be nonzero elements in the Teichmüller set $\mathcal{T}$ with $\alpha^{p^s} = \xi_0$. Let $\mathcal{C}$ be a $(\xi_0 + p\gamma)$-constacyclic code of length $2p^s$ (is an odd prime number) over $\mathrm{GR}(p^m, \ell)$. Then*

(i) If α is not a square, then $\mathcal{C} = \langle (x^2 - \alpha)^i \rangle$, for $i = 0, ..., p^s m$.

(ii) If α is a square, i.e, $\alpha = \delta^2$, then $\mathcal{C} = \langle (x - \delta)^i (x + \delta)^j \rangle$, for $i, j = 0, ..., p^s m$.

The Hamming and symbol-pair distances of any $(\xi_0 + p\gamma)$-constacyclic code of lenght $2p^s$ over $\mathrm{GR}(p^m, \ell)$, (with $\gcd(p, 2) = 1$) are fully established and determined by the Theorem 2 [17] and Theorem 3.17 [18].

7 Conclusion

In this work, we have established the structure of $(\xi_0 + p\gamma)$-constacyclic codes with a length of ηp^s over the ring $\mathrm{GR}(p^m, \ell)$. Here, ξ_0 is nonzero elements in the Teichmüller set $\mathcal{T}$, and γ is a unit in $\mathrm{GR}(p^m, \ell)$. This structural insight has enabled us to characterize self-dual $(\xi_0 + p\gamma)$-constacyclic codes. We provide a necessary and sufficient condition for the existence of nontrivial self-dual $(\xi_0 + p\gamma)$-constacyclic codes. Additionally, a method has been devised to determine the b-symbol distance of $(\xi_0 + p\gamma)$-constacyclic codes with a length of $2p^s$ for both $b = 1$ and $b = 2$. It has also been shown that $\langle 1 \rangle$ is the unique Maximum Distance Separable (MDS) $(\xi_0 + p\gamma)$-constacyclic codes with a length of ηp^s over $\mathrm{GR}(p^m, \ell)$.

References

[1] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 45 (7) (1999) 2527–2532.

[2] J. Wolfmann, Binary image of cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 47 (5) (2001) 1773–1779.

[3] H. Tapia-Recillas, G. Vega, A Generalization of Negacyclic Codes, Electronic Notes in Discrete Mathematics, Volume 6, 2001, Pages 251-261,

[4] H.Q. Dinh, S.R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory 50 (2004) 1728–1744.

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

[6] H.Q. Dinh, Complete distances of all negacyclic codes of length 2^s Over $\mathbb{Z}_a$, IEEE Trans. Inform. Theory 53 (1) (2007) 147–161.

[7] S. Zhu, X. Kai, A class of constacyclic codes over $\mathbb{Z}_{p^m}$, Finite Fields Appl. 16 (2010) 243–254.

[8] Z.X. Wan, Lectures on Finite Fields and Galois Rings, World Scientific Publishing, 2003.

[9] S.T. Dougherty, Y.H. Park, On modular cyclic codes, Finite Fields Appl. 13 (2007) 31–57.

[10] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2010.

[11] H.Q. Dinh, Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, J. Algebra 324 (2010) 940–950.

[12] H. Liu, Y. Maouche, Some Repeated-Root Constacyclic Codes over Galois Rings, IEEE Trans. Inf. Theory, 63 (10) (2017) 6247-6255.

[13] B. Ding, T. Zhang and G. Ge, Maximum distance separable codes for b-symbol read channels, Finite Fields Appl., 49 (2018), pp. 180–197.

[14] H. Q. Dinh, X. Wang, H. Liu, and S. Sriboonchitta, On the b-distance of repeated-root constacyclic codes of prime power lengths, Discrete Mathematics, vol. 343, no. 4, Apr. 2020, Art. no. 111780.

[15] H. Q. Dinh, H. D. T. Nguyen, S. Sriboonchitta, and T. M. Vo, Repeatedroot constacyclic codes of prime power lengths over finite chain rings, Finite Fields Their Appl., vol. 43, pp. 22–41, Jan. 2017.

[16] A. Sharma and T. Sidana, On b-symbol distances of repeated-root consta- cyclic codes, IEEE Trans. Inform. Theory, vol. 6, no. 12, pp. 7848–7867, 2019

[17] H. Ozadam and F. Ozbudak, The minimum Hamming distance of cyclic codes of length $2p^s$, in Proc. Int. Symp. Appl. Algebra, Algebr. Algorithms, Error-Correcting Codes, Jun. 2009, pp. 92–100.

[18] H. Q. Dinh, X. Wang, H. Liu, and S. Sriboonchitta, On the symbolpair distances of repeated-root constacyclic codes of length $2p^s$, Discrete Math., vol. 342, no. 11, pp. 3062–3078, Nov. 2019.

Author information

Youssef Ahendouz and Ismail Akharraz, Mathematical and Informatics Engineering Laboratory , Ibn Zohr University, Morocco.
E-mail: youssef.ahendouz@gmail.com, i.akharraz@uiz.ac.ma

Received: 2023-09-05
Accepted: 2023-11-21