Ars Combinatoria, 160: 105–115
DOI:10.61091/ars-160-10
http://www.combinatorialpress.com/ars
Received 20 April 2024, Accepted 17 September 2024, Published 30 September 2024

Combinatorial Press

Article

A Note on Complete Classification of Repeated-Root σ-Constacyclic Codes of Prime Power Length over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ and their Hamming Distances

Youssef Ahendouz[1,*], **and Ismail Akharraz**[1]

[1] Mathematical and Informatics Engineering Laboratory Ibn Zohr University - Morocco

* **Correspondence:** youssef.ahendouz@edu.uiz.ac.ma

Abstract: This note presents a counterexample to Propositions 7 and 8 in the paper [1], where the authors determine the values of V and W. These values are crucial in determining the Hamming distance and MDS codes in the family of certain constacyclic codes over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$, which implies that the results found in [2] are incorrect. Furthermore, we provide corrections to the aforementioned results.

Keywords: Repeated-root codes, Chain ring, Torsion code, Constacyclic code, Minimum Distance Separable
2020 Mathematics Subject Classification: Primary 94B15, Secondary 94B05

1. Introduction

The goal of coding theory is to design codes that can transmit data with a high level of accuracy and efficiency by selecting codes with the greatest possible minimum distance, given constraints on the length of the code. This ensures that the code can correct as many errors as possible during transmission over a noisy channel.

Let R be a finite commutative ring, and let n be a positive integer. A λ-constacyclic code is a submodule C of R^n satisfying

$$(a_0, \ldots, a_{n-2}, a_{n-1}) \in C \Rightarrow (\lambda a_{n-1}, a_0, \ldots, a_{n-2}) \in C.$$

The λ-constacyclic code C is called a cyclic code when $\lambda = 1$, and C is called a negacyclic code when $\lambda = -1$. Each codeword $a = (a_0, a_1, \ldots, a_{n-1})$ is customarily identified with its polynomial representation $a(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$, and the code C is identified with the set of all polynomial representations of its codewords. Then in the ring $R[x]/\langle x^n - \lambda\rangle$, $xc(x)$ corresponds to a λ-constacyclic shift of $c(x)$. From this, the following fact is straightforward:

Proposition 1. *A submodule C of R^n is λ-constacyclic over R if and only if C is an ideal of $R[x]/\langle x^n - \lambda\rangle$.*

In the case where $R = \mathbb{F}_q$, $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$ is a principal ideal ring. Thus, λ-constacyclic codes correspond precisely to the ideals $\langle g(x)\rangle$ such that $g(x)$ divides $x^n - \lambda$. However, in general, there is no known method to determine the ideals of the ring $R[x]/\langle x^n - \lambda\rangle$. The structure of these ideals depends on the choice of the unit λ, the positive integer n, and the structure of R. If the length n is coprime with the characteristic of the ring, the structure of cyclic and negacyclic codes of length n

and their duals over a finite chain ring R is determined by Dinh and López-Permouth in [3]. Later, Kiah et al. [4] classified all repeated-root cyclic codes of length p^k over Galois rings $GR(p^2, m)$ (a special finite chain ring). The structural properties and dual codes of $(1 + w\gamma)$-constacyclic codes of arbitrary length over chain rings are given in [5], where γ is a generator of the maximal ideal and w is a unit of R.

Consider the finite commutative ring $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3\rangle = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$, where $u^3 = 0$. This ring $\mathcal{R}$ is a finite chain ring with a maximal ideal $\langle u\rangle$ and nilpotency index 3. The units of $\mathcal{R}$ are of the following form:

$$\lambda = \sigma + \beta u + \delta u^2, \text{ where } \sigma \in \mathbb{F}_{p^m}^* \text{ and } \beta, \delta \in \mathbb{F}_{p^m}.$$

The structure of constacyclic codes over $\mathcal{R}$ has been extensively examined in various publications. In the case where $\beta \neq 0$, Dinh et al. demonstrated in [6] that the ring $\mathcal{R}[x]/\langle x^{p^s} - \lambda\rangle$ is a chain ring whose ideals are

$$\langle 1\rangle \supsetneq \langle \gamma x - 1\rangle \supsetneq \cdots \supsetneq \left\langle (\gamma x - 1)^{3p^s-1}\right\rangle \supsetneq \left\langle (\gamma x - 1)^{3p^s}\right\rangle = \langle 0\rangle,$$

where $\gamma^{p^s} = \sigma$. When $\beta = 0$ and $\delta \neq 0$, Sobhani [7] determined the structure of $(\delta + \alpha u^2)$-constacyclic codes of length p^k over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$. When $\beta = \delta = 0$, Liu and Xu [8] studied the structure of constacyclic codes of length p^s over $\mathcal{R}$. However, such classification is incomplete, since there are some intersections between their types of codes. Later, Laaouine et al. [1] completely solved this problem and gave the classification of such codes, which categorizes them into 8 distinct types, but the classification is only complete by determining the values of parameters L, L_1, U, V, and W. However, the values of V and W are not well calculated, as shown in Examples 1 and 2, and this error impacts the determination of the Hamming distance of some types of these codes. Therefore, our objective in this article is to resolve these problems.

2. Cyclic Codes of Length p^s Over $\mathcal{R}$

In this section, we review some structural results presented in [1]. Consider the ring

$$\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m} = \mathbb{F}_{p^m}[u]/\langle u^3\rangle,$$

where p is a prime number and m is a positive integer. Define $\mathcal{R}'$ as the ring $\mathcal{R}[x]/\langle x^{p^s} - 1\rangle$, where s is a positive integer. According to Proposition 1, cyclic codes of length p^s over $\mathcal{R}$ are ideals of $\mathcal{R}'$. Let $\mathcal{K} = \mathbb{F}_{p^m}[x]/\langle x^{p^s} - 1\rangle$ and define $\mu : \mathcal{R}' \to \mathcal{K}$ as the map that sends $f(x)$ to $f(x) \mod u$. For an ideal C in $\mathcal{R}'$, and $0 \leq i \leq 2$, we define the i-th torsion code of a code C as

$$\mathrm{Tor}_i(C) = \mu(\{f(x) \in \mathcal{K} \mid u^i f(x) \in C\}),$$

which is an ideal of the ring $\mathcal{K}$. Clearly, we have

$$\mathrm{Tor}_0(C) \subseteq \mathrm{Tor}_1(C) \subseteq \mathrm{Tor}_2(C). \tag{1}$$

Therefore, there exist integers $T_0(C) \geq T_1(C) \geq T_2(C)$ such that

$$\mathrm{Tor}_0(C) = \left\langle (x-1)^{T_0(C)}\right\rangle, \quad \mathrm{Tor}_1(C) = \left\langle (x-1)^{T_1(C)}\right\rangle, \quad \text{and} \quad \mathrm{Tor}_2(C) = \left\langle (x-1)^{T_2(C)}\right\rangle.$$

The following Theorem is a variation of Theorem 2 and Lemma 3 in [1].

Theorem 1. *Cyclic codes of length p^s over $\mathcal{R}$, i.e., the ideals of $\mathcal{R}'$, are classified into 8 types as follows:*

- *Type 1. $\langle 0\rangle$, $\langle 1\rangle$. For this type, we have*

$$T_0(\langle 0\rangle) = T_1(\langle 0\rangle) = T_2(\langle 0\rangle) = p^s,$$
$$T_0(\langle 1\rangle) = T_1(\langle 1\rangle) = T_2(\langle 1\rangle) = 0.$$

- *Type 2.* $C_2 = \left\langle u^2(x-1)^\tau \right\rangle$, *where* $0 \le \tau \le p^s - 1$. *For this type,*

$$T_0(C_2) = T_1(C_2) = p^s, \quad T_2(C_2) = \tau.$$

- *Type 3.* $C_3 = \left\langle u(x-1)^\delta + u^2(x-1)^t h(x) \right\rangle$, *where* $0 \le L \le \delta \le p^s - 1$, $0 \le t < L$, *and* $h(x)$ *is either* 0 *or a unit in* $\mathcal{K}$, *and*

$$L = \min\left\{k \mid u^2(x-1)^k \in C_3\right\}. \tag{2}$$

For this type, we have

$$T_0(C_3) = p^s, \quad T_1(C_3) = \delta, \quad T_2(C_3) = L.$$

- *Type 4.*

$$C_4 = \left\langle u(x-1)^\delta + u^2(x-1)^t h(x), u^2(x-1)^\omega \right\rangle,$$

where $0 \le \omega < L \le \delta \le p^s - 1$, $0 \le t < \omega$, *either* $h(x)$ *is* 0 *or* $h(x)$ *is a unit in* $\mathcal{K}$, *and* L *is defined as in* (2). *For this type, we have*

$$T_0(C_4) = p^s, \quad T_1(C_4) = \delta, \quad T_2(C_4) = \omega.$$

- *Type 5.* $C_5 = \left\langle (x-1)^a + u(x-1)^{t_1} h_1(x) + u^2(x-1)^{t_2} h_2(x) \right\rangle$, *where* $0 < V \le U \le a \le p^s - 1$, $0 \le t_1 < U$, $0 \le t_2 < V$, *and*

$$U = \min\left\{k \mid u(x-1)^k + u^2 g(x) \in C_5\right\}, \tag{3}$$

and

$$V = \min\left\{k \mid u^2(x-1)^k \in C_5\right\}. \tag{4}$$

For this type, we have

$$T_0(C_5) = a, \quad T_1(C_5) = U, \quad T_2(C_5) = V.$$

- *Type 6.* $C_6 = \left\langle (x-1)^a + u(x-1)^{t_1} h_1(x) + u^2(x-1)^{t_2} h_2(x), u^2(x-1)^c \right\rangle$, *where* $0 \le c < V \le U \le a \le p^s - 1$, $0 \le t_1 < U$, $0 \le t_2 < c$, *and for* $i = 1, 2$, $h_i(x)$ *is either* 0 *or a unit in* $\mathcal{K}$. U *and* V *as defined in* (3) *and* (4). *For this type, we have*

$$T_0(C_6) = a, \quad T_1(C_6) = U, \quad T_2(C_6) = c.$$

- *Type 7.* $C_7 = \left\langle (x-1)^a + u(x-1)^{t_1} h_1(x) + u^2(x-1)^{t_2} h_2(x), u(x-1)^b + u^2(x-1)^{t_3} h_3(x) \right\rangle$, *where* $0 \le W \le b < U \le a \le p^s - 1$, $0 \le t_1 < b$, $0 \le t_2 < W$, $0 \le t_3 < W$, *and for* $i = 1, 2, 3$, $h_i(x)$ *is either* 0 *or a unit in* $\mathcal{K}$. U *as defined in* (3), *and*

$$W = \min\left\{k \mid u^2(x-1)^k \in C_7\right\}. \tag{5}$$

For this type, we have

$$T_0(C_7) = a, \quad T_1(C_7) = b, \quad T_2(C_7) = W.$$

- *Type 8.* $C_8 = \left\langle (x-1)^a + u(x-1)^{t_1} h_1(x) + u^2(x-1)^{t_2} h_2(x), u(x-1)^b + u^2(x-1)^{t_3} h_3(x), u^2(x-1)^c \right\rangle$, *where* $0 \le c < W \le L_1 \le b < U \le a \le p^s - 1$, $0 \le t_1 < b$, $0 \le t_2 < c$, $0 \le t_3 < c$, *and for* $i = 1, 2, 3$, $h_i(x)$ *is either* 0 *or a unit in* $\mathcal{K}$. U *and* W *as defined in* (3) *and* (5), *and*

$$L_1 = \min\left\{k \mid u^2(x-1)^k \in \langle u(x-1)^b + u^2(x-1)^{t_3} h_3(x) \rangle\right\}.$$

For this type, we have

$$T_0(C_8) = a, \quad T_1(C_8) = b, \quad T_2(C_8) = c.$$

Proposition 2. [1] *Let L, L_1 and U be as above, then we have*

$$L = \begin{cases} \delta, & \text{if } h(x) = 0, \\ \min\{\delta, p^s - \delta + t\}, & \text{if } h(x) \neq 0. \end{cases}$$

$$L_1 = \begin{cases} b, & \text{if } h_3(x) = 0, \\ \min\{b, p^s - b + t_3\}, & \text{if } h_3(x) \neq 0. \end{cases}$$

$$U = \begin{cases} a, & \text{if } h_1(x) = 0, \\ \min\{a, p^s - a + t_1\}, & \text{if } h_1(x) \neq 0. \end{cases}$$

Remark 1. *In Propositions 7 and 8 of* [1] *it is claimed that*

$$V = \begin{cases} a, & \text{if } h_1(x) = h_2(x) = 0, \\ \min\{a, p^s - a + t_2\}, & \text{if } h_1(x) = 0 \text{ and } h_2(x) \neq 0, \\ \min\{a, p^s - a + t_1\}, & \text{if } h_1(x) \neq 0. \end{cases} \tag{6}$$

$$W = \begin{cases} b, & \text{if } h_1(x) = h_2(x) = h_3(x) = 0, \\ & \text{or } h_1(x) \neq 0 \text{ and } h_3(x) = 0, \\ \min\{b, p^s - a + t_2\}, & \text{if } h_1(x) = h_3(x) = 0, h_2(x) \neq 0, \\ \min\{b, p^s - b + t_3\}, & \text{if } h_1(x) = h_2(x) = 0, h_3(x) \neq 0 \\ & \text{or } h_1(x) \neq 0 \text{ and } h_3(x) \neq 0, \\ \min\{b, p^s - a + t_2, p^s - b + t_3\}, & \text{if } h_1(x) = 0, h_2(x) \neq 0, h_3(x) \neq 0. \end{cases} \tag{7}$$

This claim is not true in general. To be more precise, in the following, we present a counter-example.

Example 1. *Let $\mathcal{R} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. Consider the cyclic code $C_5 = \langle (x-1) + u \rangle$ of length 2 over $\mathcal{R}$. Here, $a = 1$, $t_1 = 0$, $h_1(x) = 1$, and $h_2(x) = 0$. Since $u^2 = [(x-1) + u][(x-1) + u]$, we have $u^2 \in C_5$. This implies that $V = 0$. By* (6)*, we see that* $\min\{a, p^s - a + t_1\} = 1$. *Hence $V \neq \min\{a, p^s - a + t_1\}$.*

Example 2. *Let $\mathcal{R} = \mathbb{F}_3 + u\mathbb{F}_3 + u^3\mathbb{F}_3$. Consider the cyclic code $C_7 = \langle (x-1)^2 + u, u(x-1) \rangle$ of length 3 over $\mathcal{R}$. Here, $a = 2$, $b = 1$, $t_1 = 0$, $h_1(x) = 1$, and $h_2(x) = h_3(x) = 0$. We have*

$$u^2 = u\left[(x-1)^2 + u\right] - (x-1)\left[u(x-1)\right] \in C_7.$$

This implies that $W = 0$. By (7)*, we see that $W = b = 1$, which is not true.*

In the following Theorem we provide a correction of Propositions 7 and 8 of [1].

Theorem 2. *Let V be as defined in* (4)*, then we have*

$$V = \begin{cases} a, & \text{if } h_1(x) = h_2(x) = 0, \\ \min\{a, p^s - a + t_2\}, & \text{if } h_1(x) = 0 \text{ and } h_2(x) \neq 0, \\ \min\{a, p^s - 2a + 2t_1\}, & \text{if } h_1(x) \neq 0, h_2(x) = 0 \text{ and } a \leq p^s - a + t_1, \\ \min\{a, p^s - a + t_2, p^s - 2a + 2t_1\}, & \text{if } h_1(x) \neq 0, h_2(x) \neq 0, a \leq p^s - a + t_1 \text{ and } 2t_1 \neq a + t_2, \\ \min\{a, p^s - a + t_2 + \alpha_1\}, & \text{if } h_1(x) \neq 0, h_2(x) \neq 0, a \leq p^s - a + t_1 \text{ and } 2t_1 = a + t_2, \\ t_1, & \text{if } h_1(x) \neq 0, h_2(x) = 0 \text{ and } a \geq p^s - a + t_1, \\ \min\{t_1, a + t_2 - t_1\}, & \text{if } h_1(x) \neq 0, h_2(x) \neq 0, a \geq p^s - a + t_1 \text{ and } 2t_1 \neq a + t_2, \\ \min\{p^s + t_1 - a, t_1 + \alpha_1\}, & \text{if } h_1(x) \neq 0, h_2(x) \neq 0, a \geq p^s - a + t_1 \text{ and } 2t_1 = a + t_2, \end{cases} \tag{8}$$

where

$$\alpha_1 = \max\left\{0 \leq k \leq p^s \mid (x-1)^k \text{ divides } h_1(x) - h_2(x)h_1(x)^{-1}\right\}.$$

Proof. Since $u^2(x-1)^V \in C_5$, there exists $F(x) = g_0(x)+ug_1(x)+u^2g_2(x)$, where $g_0(x), g_1(x), g_2(x) \in \mathcal{K}$ such that

$$\begin{aligned} u^2(x-1)^V =& F(x)\left((x-1)^a + u(x-1)^{t_1}h_1(x) + u^2(x-1)^{t_2}h_2(x)\right) \\ =& (x-1)^a g_0(x) + u\left((x-1)^{t_1}h_1(x)g_0(x) + (x-1)^a g_1(x)\right) \\ &+ u^2\left((x-1)^{t_2}h_2(x)g_0(x) + (x-1)^a g_2(x) + (x-1)^{t_1}h_1(x)g_1(x)\right). \end{aligned}$$

This equation can be represented as a system of equations:

$$(x-1)^a g_0(x) = 0, \tag{9a}$$
$$(x-1)^{t_1}h_1(x)g_0(x) + (x-1)^a g_1(x) = 0, \tag{9b}$$
$$(x-1)^V = (x-1)^{t_2}h_2(x)g_0(x) + (x-1)^a g_2(x) + (x-1)^{t_1}h_1(x)g_1(x). \tag{9c}$$

Equation (9a) can be rewritten as $g_0(x) = (x-1)^{p^s-a}g_0'(x)$, where $g_0'(x) \in \mathcal{K}$. Substituting this into the system (9), we obtain:

$$(x-1)^{p^s-a+t_1}h_1(x)g_0'(x) + (x-1)^a g_1(x) = 0, \tag{10a}$$
$$(x-1)^V = (x-1)^{p^s-a+t_2}h_2(x)g_0'(x) + (x-1)^a g_2(x) + (x-1)^{t_1}h_1(x)g_1(x). \tag{10b}$$

We will now consider the four possible cases:

- If $h_1(x) = h_2(x) = 0$, we have that $C_5 = \langle (x-1)^a \rangle$, and $V = a$.
- If $h_1(x) = 0$ and $h_2(x) \neq 0$, then equation (10b) can be simplified to:

  $$(x-1)^V = (x-1)^{p^s-a+t_2}h_2(x)g_0'(x) + (x-1)^a g_2(x).$$

  Therefore, it follows that $V \geq \min\{a, p^s - a + t_2\}$. Conversely, when we consider

  $$g_1(x) = g_0'(x) = 0, g_2(x) = 1, \text{ and } g_0'(x) = h_2(x)^{-1}, g_1(x) = g_2(x) = 0,$$

  we can deduce that $u^2(x-1)^a, u^2(x-1)^{p^s-a+t_2} \in C_5$. This implies that $V = \min\{a, p^s - a + t_2\}$.
- If $h_1(x) \neq 0$ and $a \leq p^s - a + t_1$. Then from (10a) we have,

  $$(x-1)^{p^s-2a+t_1}h_1(x)g_0'(x) + g_1(x) = (x-1)^{p^s-a}g_4(x),$$

  for some $g_4(x) \in \mathcal{K}$. Then from (10*b*),

  $$\begin{aligned} (x-1)^V =& (x-1)^{p^s-a+t_2}h_2(x)g_0'(x) + (x-1)^a g_2(x) + (x-1)^{t_1}h_1(x)g_1(x) \\ =& (x-1)^{p^s-a+t_2}h_2(x)g_0'(x) + (x-1)^a g_2(x) \\ &+ (x-1)^{t_1}h_1(x)\left((x-1)^{p^s-a}g_4(x) - (x-1)^{p^s-2a+t_1}h_1(x)g_0'(x)\right) \\ =& (x-1)^a g_2(x) + \left((x-1)^{p^s-a+t_2}h_2(x) - (x-1)^{p^s-2a+2t_1}h_1(x)^2\right)g_0'(x) \\ &+ (x-1)^{p^s-a+t_1}h_1(x)g_4(x) \\ =& (x-1)^a g_2(x) + (x-1)^{\beta_1}f_1(x)g_0'(x) + (x-1)^{p^s-a+t_1}h_1(x)g_4(x), \end{aligned}$$

  where

  $$\begin{aligned} \beta_1 &= \max\{k \mid (x-1)^k \text{ divides } (x-1)^{p^s-a+t_2}h_2(x) - (x-1)^{p^s-2a+2t_1}h_1(x)^2\} \\ &= \begin{cases} p^s - 2a + 2t_1, & \text{if } h_2(x) = 0, \\ \min\{p^s - a + t_2, p^s - 2a + 2t_1\}, & \text{if } h_2(x) \neq 0 \text{ and } 2t_1 \neq a + t_2, \\ p^s - a + t_2 + \alpha_1, & \text{if } h_2(x) \neq 0 \text{ and } 2t_1 = a + t_2, \end{cases} \end{aligned}$$

  and $f_1(x)$ a unit of $\mathcal{K}$ such that

  $$(x-1)^{p^s-a+t_2}h_2(x) - (x-1)^{p^s-2a+2t_1}h_1(x) = (x-1)^{\beta_1}f_1(x).$$

  Then $V \geq \min\{a, \beta_1, p^s - a + t_1\} = \min\{a, \beta_1\}$. Conversely if we take

$$g_4(x) = g_0'(x) = 0, g_2(x) = 1, \text{ and } g_0'(x) = f_1(x)^{-1}, g_4(x) = g_2(x) = 0,$$

we obtain respectively $u^2(x-1)^a, u^2(x-1)^{\beta_1} \in C_5$. So

$$V = \min\{a,\beta_1\} = \begin{cases} \min\{a, p^s - 2a + 2t_1\}, & \text{if } h_2(x) = 0, \\ \min\{a, p^s - a + t_2, p^s - 2a + 2t_1\}, & \text{if } h_2(x) \neq 0 \text{ and } 2t_1 \neq a + t_2, \\ \min\{a, p^s - a + t_2 + \alpha_1\}, & \text{if } h_2(x) \neq 0 \text{ and } 2t_1 = a + t_2. \end{cases} \quad (11)$$

- If $h_1(x) \neq 0$ and $a \geq p^s - a + t_1$. Then from (10a), we have,

$$h_1(x)g_0'(x) + (x-1)^{2a-p^s-t_1}g_1(x) = (x-1)^{a-t_1}g_5(x),$$

for some $g_5(x) \in \mathcal{K}$. This implies that, from (10b),

$$\begin{aligned}(x-1)^V =& (x-1)^a g_2(x) + (x-1)^{p^s-a+t_2}h_2(x)g_0'(x) + (x-1)^{t_1}h_1(x)g_1(x) \\ =& (x-1)^a g_2(x) + (x-1)^{p^s-a+t_2}\left((x-1)^{a-t_1}g_5(x) - (x-1)^{2a-p^s-t_1}g_1(x)\right)h_2(x)h_1(x)^{-1} \\ &+ (x-1)^{t_1}h_1(x)g_1(x) \\ =& (x-1)^a g_2(x) + (x-1)^{p^s+t_2-t_1}h_2(x)h_1(x)^{-1}g_5(x) \\ &+ \left((x-1)^{t_1}h_1(x) - (x-1)^{a+t_2-t_1}h_2(x)h_1(x)^{-1}\right)g_1(x) \\ =& (x-1)^a g_2(x) + (x-1)^{p^s+t_2-t_1}h_2(x)h_1(x)^{-1}g_5(x) + (x-1)^{\beta_2}f_2(x)g_1(x),\end{aligned}$$

where

$$\begin{aligned}\beta_2 &= \max\left\{0 \leq k \leq p^s \mid (x-1)^k \text{ divides } (x-1)^{t_1}h_1(x) - (x-1)^{a+t_2-t_1}h_2(x)h_1(x)^{-1}\right\} \\ &= \begin{cases} t_1, & \text{if } h_2(x) = 0, \\ \min\{t_1, a + t_2 - t_1\}, & \text{if } h_2(x) \neq 0 \text{ and } 2t_1 \neq a + t_2, \\ t_1 + \alpha_1, & \text{if } h_2(x) \neq 0 \text{ and } 2t_1 = a + t_2, \end{cases}\end{aligned}$$

and $f_2(x)$ a unit of $\mathcal{K}$ such that

$$(x-1)^{t_1}h_1(x) - (x-1)^{a+t_2-t_1}h_2(x)h_1(x)^{-1} = (x-1)^{\beta_2}f_2(x).$$

Similarly to the previous case, we have:

- If $h_2(x) = 0$, then $V = \min\{a,\beta_2\} = t_1$.
- If $h_2(x) \neq 0$, then

$$V = \min\{a, p^s + t_2 - t_1, \beta_2\} = \begin{cases} \min\{t_1, a + t_2 - t_1\}, & \text{if } 2t_1 \neq a + t_2, \\ \min\{p^s + t_1 - a, t_1 + \alpha_1\}, & \text{if } 2t_1 = a + t_2. \end{cases}$$

□

Theorem 3. *Let W be defined as in* (5)*. Then we have:*

$$W = \begin{cases} b, & \text{if } h_1(x) = h_2(x) = h_3(x) = 0, \\ \min\{b, a - b + t_3\}, & \text{if } h_1(x) = h_2(x) = 0 \text{ and } h_3(x) \neq 0, \\ \min\{p^s - a + t_2, b\}, & \text{if } h_2(x) \neq 0 \text{ and } h_1(x) = h_3(x) = 0, \\ \min\{p^s - a + t_2, b, a - b + t_3\}, & \text{if } h_1(x) = 0, h_2(x) \neq 0 \text{ and } h_3(x) \neq 0, \\ t_1, & \text{if } h_1(x) \neq 0 \text{ and } h_2(x) = h_3(x) = 0, \\ \min\{p^s - a + t_2, t_1\}, & \text{if } h_1(x) \neq 0, h_2(x) \neq 0 \text{ and } h_3(x) = 0, \\ \min\{\beta_3, \beta_4, b, p^s - b + t_3\}, & \text{if } h_1(x) \neq 0 \text{ and } h_3(x) \neq 0, \end{cases}$$

where

$$\begin{aligned}
\beta_3 &= \begin{cases} p^s - a + t_1 - b + t_3, & \text{if } h_2(x) = 0, \\ \min\{p^s - a + t_2, p^s - a + t_1 - b + t_3\}, & \text{if } h_2(x) \neq 0 \text{ and } t_2 \neq t_1 - b + t_3, \\ p^s - a + t_1 - b + t_3 + \alpha_3, & \text{if } h_2(x) \neq 0 \text{ and } t_2 = t_1 - b + t_3, \end{cases} \\
\beta_4 &= \begin{cases} \min\{t_1, a - b + t_3\}, & \text{if } t_1 \neq a - b + t_3, \\ t_1 + \alpha_4, & \text{if } t_1 = a - b + t_3, \end{cases} \\
\alpha_3 &= \max\left\{0 \leq k \leq p^s \mid (x-1)^k \text{ divides } h_2(x) - h_1(x)h_3(x)\right\}, \\
\alpha_4 &= \max\left\{0 \leq k \leq p^s \mid (x-1)^k \text{ divides } h_1(x) - h_3(x)\right\}.
\end{aligned}$$

Proof. Since $u^2(x-1)^W \in C_7$, then there exist $F_1(x)$ and $F_2(x)$ in $\mathcal{R}'$ such that

$$u^2(x-1)^W = F_1(x)\left((x-1)^a + u(x-1)^{t_1}h_1(x) + u^2(x-1)^{t_2}h_2(x)\right) + F_2(x)\left(u(x-1)^b + u^2(x-1)^{t_3}h_3(x)\right).$$

Write $F_1(x)$ and $F_2(x)$ as:

$$F_1(x) = (x-1)^{p^s-a}g_0(x) + ug_1(x) + u^2g_2(x),$$

and

$$F_2(x) = g_4(x) + ug_5(x),$$

where, $g_0(x), ..., g_5(x) \in \mathcal{K}$. Then

$$\begin{aligned}
u^2(x-1)^W &= u\left((x-1)^{p^s-a+t_1}h_1(x)g_0(x) + (x-1)^a g_1(x) + (x-1)^b g_4(x)\right) \\
&= u^2((x-1)^{p^s-a+t_2}h_2(x)g_0(x) + (x-1)^a g_2(x) + (x-1)^{t_1}h_1(x)g_1(x) \\
&\quad + (x-1)^b g_5(x) + (x-1)^{t_3}h_3(x)g_4(x)).
\end{aligned}$$

We must have,

$$(x-1)^{p^s-a+t_1}h_1(x)g_0(x) + (x-1)^a g_1(x) + (x-1)^b g_4(x) = 0. \tag{12}$$

- If $h_1(x) = 0$, then

$$(x-1)^{a-b}g_1(x) + g_4(x) = (x-1)^{p^s-b}g_6(x),$$

for some $g_6(x) \in \mathcal{K}$. Hence

$$\begin{aligned}
(x-1)^W &= (x-1)^{p^s-a+t_2}h_2(x)g_0(x) + (x-1)^a g_2(x) + (x-1)^b g_5(x) \\
&\quad + (x-1)^{t_3}h_3(x)g_4(x) \\
&= (x-1)^{p^s-a+t_2}h_2(x)g_0(x) + (x-1)^a g_2(x) + (x-1)^b g_5(x) \\
&\quad + (x-1)^{p^s-b+t_3}h_3(x)g_6(x) - (x-1)^{a-b+t_3}h_3(x)g_1(x).
\end{aligned}$$

  - If $h_2(x) = h_3(x) = 0$. Then $W = \min\{a, b\} = b$.
  - If $h_2(x) = 0$ and $h_3(x) \neq 0$. Then $W = \min\{a, b, p^s - b + t_3, a - b + t_3\} = \min\{b, a - b + t_3\}$.
  - If $h_2(x) \neq 0$ and $h_3(x) = 0$. Then $W = \min\{p^s - a + t_2, a, b\} = \min\{p^s - a + t_2, b\}$.
  - If $h_2(x) \neq 0$ and $h_3(x) \neq 0$. Then $W = \min\{p^s - a + t_2, a, b, p^s - b + t_3, a - b + t_3\} = \min\{p^s - a + t_2, b, a - b + t_3\}$.

- If $h_1(x) \neq 0$, since $b \leq U$ then by Proposition 2, $p^s - a + t_1 \geq b$. From (12),

$$(x-1)^{p^s-a+t_1-b}h_1(x)g_0(x) + (x-1)^{a-b}g_1(x) + g_4(x) = (x-1)^{p^s-b}g_7(x),$$

for some $g_7(x) \in \mathcal{K}$. Hence

$$\begin{aligned}(x-1)^W &= (x-1)^{p^s-a+t_2}h_2(x)g_0(x) + (x-1)^a g_2(x) + (x-1)^{t_1}h_1(x)g_1(x) + (x-1)^b g_5(x)\\ &\quad + (x-1)^{t_3}h_3(x)g_4(x)\\ &= (x-1)^{p^s-a+t_2}h_2(x)g_0(x) + (x-1)^a g_2(x) + (x-1)^{t_1}h_1(x)g_1(x) + (x-1)^b g_5(x)\\ &\quad + (x-1)^{t_3}\left((x-1)^{p^s-b}g_7(x) - (x-1)^{p^s-a+t_1-b}h_1(x)g_0(x) - (x-1)^{a-b}g_1(x)\right)h_3(x)\\ &= \left((x-1)^{p^s-a+t_2}h_2(x) - (x-1)^{p^s-a+t_1-b+t_3}h_1(x)h_3(x)\right)g_0(x)\\ &\quad + (x-1)^a g_2(x) + \left((x-1)^{t_1}h_1(x) - (x-1)^{a-b+t_3}h_3(x)\right)g_1(x)\\ &\quad + (x-1)^b g_5(x) + (x-1)^{p^s-b+t_3}h_3(x)g_7(x).\end{aligned}$$

– If $h_3(x) = 0$, then

$$(x-1)^W = (x-1)^{p^s-a+t_2}h_2(x)g_0(x) + (x-1)^a g_2(x) + (x-1)^{t_1}h_1(x)g_1(x) + (x-1)^b g_5(x).$$

Then $W = \begin{cases}\min\{a, t_1, b\} = t_1, & \text{if } h_2(x) = 0,\\ \min\{p^s - a + t_2, a, t_1, b\} = \min\{p^s - a + t_2, t_1\}, & \text{if } h_2(x) \neq 0.\end{cases}$

– If $h_3(x) \neq 0$. Let

$$\begin{aligned}\beta_3 &= \max\left\{0 \leq k \leq p^s \mid (x-1)^k \text{ divides } (x-1)^{p^s-a+t_2}h_2(x) - (x-1)^{p^s-a+t_1-b+t_3}h_1(x)h_3(x)\right\}\\ &= \begin{cases}p^s - a + t_1 - b + t_3, & \text{if } h_2(x) = 0,\\ \min\{p^s - a + t_2, p^s - a + t_1 - b + t_3\}, & \text{if } h_2(x) \neq 0 \text{ and } t_2 \neq t_1 - b + t_3,\\ p^s - a + t_1 - b + t_3 + \alpha_3, & \text{if } h_2(x) \neq 0 \text{ and } t_2 = t_1 - b + t_3.\end{cases}\end{aligned}$$

$$\begin{aligned}\beta_4 &= \max\left\{0 \leq k \leq p^s \mid (x-1)^k \text{ divides } (x-1)^{t_1}h_1(x) - (x-1)^{a-b+t_3}h_3(x)\right\}\\ &= \begin{cases}\min\{t_1, a - b + t_3\}, & \text{if } t_1 \neq a - b + t_3,\\ t_1 + \alpha_4, & \text{if } t_1 = a - b + t_3.\end{cases}\end{aligned}$$

And $f_3(x)$ a unit of $\mathcal{K}$ such that

$$(x-1)^{p^s-a+t_2}h_2(x) - (x-1)^{p^s-a+t_1-b+t_3}h_1(x)h_3(x) = (x-1)^{\beta_3}f_3(x).$$

And $f_4(x)$ a unit of $\mathcal{K}$ such that

$$(x-1)^{t_1}h_1(x) - (x-1)^{a-b+t_3}h_3(x) = (x-1)^{\beta_4}f_4(x).$$

Which means that

$$\begin{aligned}(x-1)^W =&(x-1)^{\beta_3}f_3(x)g_0(x) + (x-1)^a g_2(x) + (x-1)^{\beta_4}f_4(x)g_1(x)\\ &+ (x-1)^b g_5(x) + (x-1)^{p^s-b+t_3}h_3(x)g_7(x).\end{aligned}$$

Then $W = \min\{\beta_3, \beta_4, b, p^s - b + t_3\}$.

□

3. Hamming Distance and MDS Codes

The Hamming weight of a codeword w is represented as $wt_H(w)$ and is calculated as the cardinality of the set $\{i \mid w_i \neq 0\}$. The Hamming distance of a code C is denoted by $d_H(C)$ and is defined as the minimum value of $wt_H(w)$ for $w \neq 0$, where $w \in C$.

In 1998, Norton et al. [9] introduced the Singleton bound for a linear code C of length n over a finite chain ring R with respect to the Hamming distance $d_H(C)$. This bound is expressed as $|C| \leq |R|^{n-d_H(C)+1}$.

Definition 1. *Let C be a linear code of length n over a finite commutative ring R. C is said to be a Maximum Distance Separable (MDS) code with respect to the Hamming distance if $|C| = |R|^{n-d_H(C)+1}$.*

In [2], the Hamming distances and MDS codes in the family of cyclic codes of length p^s over $\mathcal{R}$ have been established. However, for certain types of these codes, both the Hamming distances and MDS codes depend on the values of V and W. This indicates that the Hamming distances and MDS codes provided by [2] are not correct. In the following, we will present the necessary corrections. We begin with a key theorem.

Theorem 4. [10, Theorem V.1.] *Let C be a cyclic codes of length p^s over $\mathcal{R}$. Then the following hold.*

1. $d_h(C) = d_h(\mathrm{Tor}_2(C))$.
2. *The code C is an MDS code if and only if* $\mathrm{Tor}_0(C) = \mathrm{Tor}_2(C)$ *and* $\mathrm{Tor}_2(C)$ *is an MDS code of length p^s over $\mathbb{F}_{p^m}$.*

As for any cyclic code C of length p^s over $\mathcal{R}$, $\mathrm{Tor}_2(C)$ is a cyclic code of length p^s over $\mathbb{F}_{p^m}$, its Hamming distance is completely determined by the following theorem.

Theorem 5. [11, Theorem 4.11.] *Let C be a cyclic codes of length p^s, then $C = \left\langle (x-1)^i \right\rangle \subseteq \mathbb{F}_{p^m}[x]/\langle p^s - 1\rangle$, for $i \in \{0, 1, \ldots, p^s\}$. The Hamming distance d_i of C is determined by*

$$d_i = \begin{cases} 1, & \text{if } i = 0, \\ \beta + 2, & \text{if } \beta p^{s-1} + 1 \leqslant i \leqslant (\beta+1)p^{s-1} \text{ where } 0 \leqslant \beta \leqslant p-2, \\ (t+1)p^k, & \text{if } p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \leqslant i \leqslant p^s - p^{s-k} + tp^{s-k-1} \\ & \text{where } 1 \leqslant t \leqslant p-1, \text{ and } 1 \leqslant k \leqslant s-1, \\ 0, & \text{if } i = p^s. \end{cases}$$

Next, we will identify all MDS cyclic codes of length p^s over $\mathcal{R}$. It is clear that $\mathrm{Tor}_0(C) = \mathrm{Tor}_2(C)$ if and only if $C = \langle 1\rangle$ or C is of type 5 with $V = a$. Additionally, it is evident that $C = \langle 1\rangle$ is an MDS code. Subsequently, our focus will be on the determination of all MDS cyclic codes of length p^s over $\mathcal{R}$ of type type 5.

Lemma 1. [12, Theorem 3.2] *Let $C = \langle (x-1)^a \rangle$ be a cyclic code of length p^s over $\mathbb{F}_{p^m}$, for $a \in \{1, \ldots, p^s - 1\}$. Then C is an MDS cyclic code if and only if one of the following conditions holds:*

- *If $s = 1$, then $1 \leq a \leq p-1$. In this case, $d_h(C) = a + 1$.*
- *If $s \geq 2$, and $a = 1$, In this case, $d_h(C) = 2$.*
- *If $s \geq 2$, and $a = p^s - 1$. In this case, $d_h(C) = p^s$.*

Theorem 6. *Let $C_5 = \langle (x-1)^a \rangle$ be a cyclic code of length p^s over $\mathcal{R}$, for $a \in \{1, \ldots, p^s - 1\}$. Then C_5 is an MDS cyclic code if and only if one of the following conditions holds:*

- *If $s = 1$, then $1 \leq a \leq p-1$. In this case, $d_h(C_5) = a + 1$.*
- *If $s \geq 2$, and $a = 1$, In this case, $d_h(C_5) = 2$.*
- *If $s \geq 2$, and $a = p^s - 1$. In this case, $d_h(C_5) = p^s$.*

Proof. Just notice that $\mathrm{Tor}_0(C) = \mathrm{Tor}_2(C) = a$ and we apply the previous lemma. □

Theorem 7. *Let $C_5 = \left\langle (x-1)^a + u^2(x-1)^{t_2}h_2(x) \right\rangle$ be a cyclic code of length p^s over $\mathcal{R}$, of type 5 (as defined in Theorem 1), where $h_2(x) \neq 0$. Then C_5 is an MDS cyclic code if and only if one of the following conditions holds:*

- *If $s = 1$, then $\max\{2a - p^s, 0\} \leq t_2 < a \leq p-1$, in such case, $d_h(C_5) = a + 1$.*
- *If $s \geq 2$, then*

– $C_5 = \langle (x-1) + uh_2 \rangle$ *where* $h_2 \in \mathbb{F}_{p^m}^*$, *in such case,* $d_h(C_5) = 2$.
– $a = p^s - 1$, $t_2 = p^s - 2$, *in such case,* $d_h(C_5) = p^s$.

Proof. According to equation (8), it is required that $a = \min\{a, p^s - a + t_2\}$, which can be expressed as $2a - p^s \leq t_2$. Consequently, by Lemma 1, C_5 is an MDS cyclic code if and only if one of the following conditions holds:

- If $s = 1$, then $\max\{2a - p^s, 0\} \leq t_2 < a \leq p - 1$.
- If $s \geq 2$, there are two possibilities:
  – When $a = 1$, then $t_2 = 0$, resulting in $C_5 = \langle (x-1) + uh_2 \rangle$, where $h_2 \in \mathbb{F}_{p^m}^*$.
  – When $a = p^s - 1$, then $t_2 < a \leq p^s - a + t_2$. It follows that $t_2 = a - 1 = p^s - 2$.

□

In the following, we examine the case where $h_1(x)$ is a unit. Since $\mathrm{Tor}_0(C) = \mathrm{Tor}_2(C)$, it follows from (1) that $a = U$. This implies $a \leq p^s - a + t_1$ according to Proposition 2. Then, from (11), we have that $V = a$ if and only if:

$$\begin{cases} a \leq p^s - 2a + 2t_1, & \text{if } h_2(x) = 0, \\ a \leq p^s - a + t_2 \text{ and } a \leq p^s - 2a + 2t_1, & \text{if } h_2(x) \neq 0 \text{ and } 2t_1 \neq a + t_2, \\ a \leq p^s - a + t_2 + \alpha_1, & \text{if } h_2(x) \neq 0 \text{ and } 2t_1 = a + t_2. \end{cases}$$

This is equivalent to:

$$\begin{cases} \max\left\{\frac{3a-p^s}{2}, 0\right\} \leq t_1, & \text{if } h_2(x) = 0, \\ \max\{2a - p^s, 0\} \leq t_2 \text{ and } \max\left\{\frac{3a-p^s}{2}, 0\right\} \leq t_1, & \text{if } h_2(x) \neq 0 \text{ and } 2t_1 \neq a + t_2, \\ 2a \leq p^s + t_2 + \alpha_1, & \text{if } h_2(x) \neq 0 \text{ and } 2t_1 = a + t_2. \end{cases} \tag{13}$$

Therefore, we have the following Theorems.

Theorem 8. *Let* $C_5 = \left\langle (x-1)^a + u(x-1)^{t_1} h_1(x) + u^2(x-1)^{t_2} h_2(x) \right\rangle$ *be a cyclic code of length* p *over* $\mathcal{R}$, *of type* 5 *(as defined in Theorem* 1), *where* $h_1(x) \neq 0$. *Then* C_5 *is an MDS cyclic code if and only if one of the following conditions holds:*

- *If* $h_2(x) = 0$, *then* $\max\left\{\frac{3a-p}{2}, 0\right\} \leq t_1$.
- *If* $h_2(x) \neq 0$ *and* $2t_1 \neq a + t_2$, *then* $\max\{2a - p, 0\} \leq t_2$ *and* $\max\left\{\frac{3a-p}{2}, 0\right\} \leq t_1$.
- *If* $h_2(x) \neq 0$ *and* $2t_1 = a + t_2$, *then* $2a \leq p + t_2 + \alpha_1$.

In all cases, $d_h(C_5) = a + 1$.

Theorem 9. *Let* $C_5 = \left\langle (x-1)^a + u(x-1)^{t_1} h_1(x) + u^2(x-1)^{t_2} h_2(x) \right\rangle$ *be a cyclic code of length* p^s *over* $\mathcal{R}$, *of type 5 (as defined in Theorem 1), where* $h_1(x) \neq 0$ *and* $s \geq 2$. *Then* C_5 *is an MDS cyclic code if and only if one of the following conditions holds:*

- $C_5 = \left\langle (x-1) + uh_1 + u^2 h_2 \right\rangle$ *where* $h_1, h_2 \in \mathbb{F}_{p^m}$ *and* $h_1 \neq 0$. *In this case,* $d_h(C_5) = 2$.
- $a = p^s - 1$, $h_2(x) \neq 0$, $2t_1 = a + t_2$, *and* $2a \leq p^s + t_2 + \alpha_1$. *In this case,* $d_h(C_5) = p^s$.

Proof. According to Lemma 1, $a = 1$ or $a = p^s - 1$. In the case where $a = 1$, (13) is always satisfied. In the case where $a = p^s - 1$, (13) is satisfied if and only if $h_2(x) \neq 0$, $2t_1 = a + t_2$, and $2a \leq p^s + t_2 + \alpha_1$. □

Remark 2. *Consider* $\sigma \in \mathbb{F}_{p^m}^*$. *It follows that* $\sigma^{p^m} = \sigma$. *By utilizing the Division Algorithm, we can find nonnegative integers* σ_q *and* σ_r *such that* $s = \sigma_q m + \sigma_r$, *where* $0 \leq \sigma_r \leq m - 1$. *Let* $\sigma_0 = \sigma^{-p^{(\sigma_q+1)m-s}} = \sigma^{-p^{m-\sigma_r}}$. *Consequently,* $\sigma_0^{p^s} = \sigma^{-p^{(\sigma_q+1)m}} = \sigma^{-1}$.

Let Δ be the map $\Delta : \mathcal{R}[x]/\langle x^{p^s} - 1\rangle \to \mathcal{R}[x]/\langle x^{p^s} - \sigma\rangle$, given by $f(x) \mapsto f(\sigma_0 x)$. It is easy to verify that Δ is a ring isomorphism and it preserves the Hamming weight.

Specifically, A is a cyclic code of length p^s over $\mathcal{R}$ if and only if $B = \Delta(A)$ is a σ-constacyclic code of length p^s over $\mathcal{R}$, and furthermore $d_h(B) = d_h(A)$. Moreover, B is an MDS code if and only if A is an MDS code. Thus, our results about the Hamming distance of cyclic codes of length p^s over $\mathcal{R}$ can be correspondingly carried over to σ-constacyclic codes of length p^s over $\mathcal{R}$ via the isomorphism Δ.

Declaration of competing interest

There is no conflict of interest related to this work.

References

1. Laaouine, J., Charkani, M. E. and Wang, L., 2021. Complete classification of repeated-root σ-constacyclic codes of prime power length over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$. *Discrete Mathematics*, 344(6), p.112325.
2. Dinh, H. Q., Laaouine, J., Charkani, M. E. and Chinnakum, W., 2021. Hamming distance of constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$. *IEEE Access*, 9, pp.141064–141078.
3. Dinh, H. Q. and López-Permouth, S. R., 2004. Cyclic and negacyclic codes over finite chain rings. *IEEE Transactions on Information Theory*, 50(8), pp.1728–1744.
4. Kiah, H. M., Leung, K. H. and Ling, S., 2008. Cyclic codes over GR(p^2, m) of length p^k. *Finite Fields and Their Applications*, 14(3), pp.834–846.
5. Cao, Y., 2013. On constacyclic codes over finite chain rings. *Finite Fields and Their Applications*, 24, pp.124–135.
6. Dinh, H. Q., Dhompongsa, S. and Sriboonchitta, S., 2016. Repeated-root constacyclic codes of prime power length over $\mathbb{F}_{p^m}$ and their duals. *Discrete Mathematics*, 339(6), pp.1706–1715.
7. Sobhani, R., 2015. Complete classification of $(\delta + \alpha u^2)$-constacyclic codes of length p^k over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$. *Finite Fields and Their Applications*, 34, pp.123–138.
8. Liu, X. and Xu, X., 2014. Some classes of repeated-root constacyclic codes over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$. *Journal of the Korean Mathematical Society*, 51(4), pp.853–866.
9. Norton, G. H. and Salagean, A., 2000. On the Hamming distance of linear codes over a finite chain ring. *IEEE Transactions on Information Theory*, 46(3), pp.1060–1067.
10. Sharma, A. and Sidana, T., 2019. On b-symbol distances of repeated-root constacyclic codes. *IEEE Transactions on Information Theory*, 65(12), pp.7848–7867.
11. Dinh, H. Q., 2008. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. *Finite Fields and Their Applications*, 14(1), pp.22–40.
12. Dinh, H.Q., ElDin, R.T., Nguyen, B.T. and Tansuchat, R., 2020. MDS constacyclic codes of prime power lengths over finite fields and construction of quantum MDS codes. *International Journal of Theoretical Physics, 59*, pp.3043-3078.