Thai Journal of **Math**ematics
Special Issue (2022): Annual Meeting in Mathematics 2021
Pages 1 – 14
http://thaijmath.in.cmu.ac.th

ISSN 1686-0209

Hamming Distances of Constacyclic Codes of Length $6p^s$ over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$

Jirayu Phuto and Chakkrid Klin-eam*

Department of Mathematics, Faculty of Science
Naresuan University, Phitsanulok 65000, Thailand
e-mail : jirayup60@email.nu.ac.th (J. Phuto); chakkridk@nu.ac.th (C. Klin-eam)

Abstract Let $p \geq 5$ be a prime and $\alpha + u\beta$ be a non-square and non-cube unit of the finite commutative chain ring $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$. In this paper, we study the Hamming distances of all constacyclic codes of length $6p^s$ over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$ which are separated into 2 types, i.e., β is a unit and $\beta = 0$. For each case, we show that there exists only one maximum distance separable constacyclic code of length $6p^s$ over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$.

MSC: 94B05; 13A99
Keywords: chain rings; hamming distances; singleton bound; repeated-root codes.

1. Introduction

A linear code C over a finite field can detect and correct $\lfloor \frac{d-1}{2} \rfloor$ or fewer errors where d is the minimum Hamming distance of C in [1]. Therefore, the value d is a significant value in coding theory. Many researchers are interested in Hamming distances of those codes (see [2–4]). Normally, we first determine the algebraic structures of codes. After that, we compute the Hamming distances of codes. After the facts [5] that some good non-linear codes over $\mathbb{Z}_2$ are obtained from cyclic codes over $\mathbb{Z}_4$ (Kerdock and Preparata codes) via the Gray map, it makes that codes over finite rings are famous. One of good subclasses of linear codes of length n over a finite commutative ring R is a subclass of γ-constacyclic codes where γ is a unit of R. Moreover, those γ-constacyclic codes can be viewed to ideals of the ring $\frac{R[x]}{\langle x^n-\gamma\rangle}$. If the length of a code and the characteristic of R are not relatively prime, that code is said to be *a repeated-root code*. Otherwise, it is called *a simple-root code*. The repeated-root codes were first studied by Berman [6] in 1967. Subsequently, the fact that repeated-root codes are optimal in a few cases is provided in [7, 8]. The optimal code could have two great values of dimension and distance of code. In this paper, optimal codes are obtained when the maximum distance of codes meet the

*Corresponding author.

Singleton bound. Maximum distance separable (MDS) code is optimal in the sense that it has the highest possible detection and correction for given a length and a code.

In [9–11], the algebraic structures of constacyclic codes of lengths $p^s, 2p^s$ and $3p^s$ over the finite commutative chain ring $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$ were studied. Furthermore, for each $\alpha, \beta \in \mathbb{F}_{p^m} \setminus \{0\}$, the Hamming distance of $(\alpha + u\beta)$-constacyclic codes of length p^s over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$ was computed in [10]. In general, the structures of constacyclic codes of length np^s were also studied in [12, 13]. In 2018, Dinh et. al. [14] gave Hamming distance of the remaining constacyclic codes of length p^s over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$ and introduced Symbol-Pair distance for those codes. In addition, the Hamming distances of all constacyclic codes of length $2p^s$ over the same ring were also given by Dinh et. al [15]. Moreover, the singleton bound for linear codes over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$ is determined to compute MDS constacyclic codes of length $2p^s$.

Let $p \geq 5$ be a prime and $\alpha + u\beta$ be a non-square and non-cube unit of the finite commutative chain ring $\mathcal{R} := \frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$. In this paper, we determine the Hamming distances of $(\alpha + u\beta)$-constacyclic codes of length $6p^s$ over $\mathcal{R}$. We separate those results into 2 cases, i.e., $\beta \neq 0$ and $\beta = 0$. Furthermore, MDS constacyclic code of length $6p^s$ is only the ideal $\langle 1\rangle$ of the quotient ring $\frac{\mathcal{R}[x]}{\langle x^{6p^s} - (\alpha + u\beta)\rangle}$. The paper is sorted as follows. In Section 2, we give some results leading to the main results. In Section 3, we study Hamming distances of $(\alpha + u\beta)$-constacyclic codes of length $6p^s$ over $\mathcal{R}$ when $\beta \neq 0$. Next, we compute Hamming distances of the remaining constacyclic codes in Section 4. The last section is conclusion.

2. Preliminaries

In this section, $\mathtt{R}$ will denote a finite commutative ring with identity. The *local ring* has the unique maximal ideal. For an ideal I of $\mathtt{R}$, it is *principal* if there exists an element $r \in \mathtt{R}$ such that $I = \langle r\rangle$. The *principal ideal ring* is a ring which each ideal is principal. The ring $\mathtt{R}$ is said to be *a chain ring* if the set of all ideals is linearly ordered under set inclusion. Next, the following three statements are equivalent where $\mathtt{R}$ is a finite commutative ring with identity as follows.

Theorem 2.1. [16] *The following conditions are equivalent:*

(1) $\mathtt{R}$ *is a local ring and the maximal ideal* M *is principal of* $\mathtt{R}$*, i.e.,* $M = \langle r\rangle$ *for some* $r \in \mathtt{R}$*,*
(2) $\mathtt{R}$ *is a local principal ideal ring,*
(3) $\mathtt{R}$ *is a chain ring with ideals* $\langle r^i\rangle$*,* $0 \leq i \leq N(r)$*, where* $N(r)$ *is the nilpotency of* r*, i.e.,* $N(r)$ *is the smallest positive integer such that* $r^{N(r)} = 0$*.*

Let $\mathbb{F}_{p^m}$ be a finite field with characteristic p and carnality p^m where $p \geq 5$ is a prime and m is a positive integer. Let ξ be a primitive element of $\mathbb{F}_{p^m}$. Then

$$\mathbb{F}_{p^m} = \{0, \xi, \xi^2, \ldots, \xi^{p^m-1} = 1\}.$$

It is obvious to see that $2|(p^m - 1)$ because p is an odd prime which implies $\xi^{\frac{p^m-1}{2}} = -1$. Furthermore, the following important property holds.

Theorem 2.2. *The following conditions are equivalent:*

(1) $p^m \equiv 1 \pmod 3$.

(2) The polynomial $x^2+\gamma x+\gamma^2$ is reducible over $\mathbb{F}_{p^m}$ where γ is a unit of $\mathbb{F}_{p^m}$. (The polynomial $x^2-\gamma x+\gamma^2$ is reducible over $\mathbb{F}_{p^m}$ where γ is a unit of $\mathbb{F}_{p^m}$.)
(3) -3 is a square element of $\mathbb{F}_{p^m}$, i.e., there exists $\delta\in\mathbb{F}_{p^m}$ such that $\delta^2=-3$.

Proof. (1.) $\Rightarrow$ (2.) Suppose that $p^m\equiv 1 \pmod 3$. So, $3|(p^m-1)$. We now consider that

$$\begin{aligned}x^3-\gamma^3&=(x-\gamma)(x^2+\gamma x+\gamma^2)\\&=(x-\xi^{\frac{(p^m-1)}{3}}\gamma)(x-\xi^{\frac{2(p^m-1)}{3}}\gamma)(x-\xi^{\frac{3(p^m-1)}{3}}\gamma)\\&=(x-\gamma)(x-\xi^{\frac{(p^m-1)}{3}}\gamma)(x-\xi^{\frac{2(p^m-1)}{3}}\gamma).\end{aligned}$$

By unique factorization, we have $x^2+\gamma x+\gamma^2=(x-\xi^{\frac{(p^m-1)}{3}}\gamma)(x-\xi^{\frac{2(p^m-1)}{3}}\gamma)$. This implies that $x^2+\gamma x+\gamma^2$ is reducible over $\mathbb{F}_{p^m}$.
(2.) $\Rightarrow$ (3.) Suppose that $x^2+\gamma x+\gamma^2$ is reducible over $\mathbb{F}_{p^m}$. There exists $\beta\in\mathbb{F}_{p^m}$ such that $\beta^2+\beta+1=0$. Thus, we have $4\beta^2+4\beta+4=0$. We consider that

$$\begin{aligned}-3&=0-3\\&=4\beta^2+4\beta+4-3\\&=(2\beta+1)^2.\end{aligned}$$

This means that -3 is a square element of $\mathbb{F}_{p^m}$.
(3.) $\Rightarrow$ (1.) Suppose that -3 is a square element of $\mathbb{F}_{p^m}$, i.e., there exists $\delta\in\mathbb{F}_{p^m}$ such that $\delta^2=-3$. Note that

$$\begin{aligned}[(-1+\delta)2^{-1}]^2+(-1+\delta)2^{-1}+1=&(1-2\delta-3)2^{-2}+(-1+\delta)2^{-1}+1\\=&(-1-\delta)2^{-1}+(-1+\delta)2^{-1}+1\\=&0.\end{aligned}$$

Set $\beta=(-1+\delta)2^{-1}$, and then $\beta^2+\beta+1=0$. Since $x^3-1=(x-1)(x^2+x+1)$, we have $\beta^3-1=0$. This means that $1=\beta^3$. The order of β, $ord(\beta)$, is equal to 1 or 3. If $ord(\beta)=1$, then $0=\beta^2+\beta+1=1+1+1=3$. It is a contradiction. Thus, we get $ord(\beta)=3$ implying that $3|(p^m-1)$. Therefore, we obtain that $p^m\equiv 1 \pmod 3$. ∎

However, for each $\delta\in\mathbb{F}_{p^m}$, there exists $\delta_0\in\mathbb{F}_{p^m}$ such that $\delta_0^{p^s}=\delta$ from [10].

Proposition 2.3. *Let $\delta=\delta_0^{p^s}$ be a unit of $\mathbb{F}_{p^m}$ and n be a positive integer such that $(p,n)=1$. Then δ is a nth-power element if and only if δ_0 is a nth-power element.*

Proof. Suppose that δ is a nth-power element. There exists $\delta_1\in\mathbb{F}_{p^m}$ such that $\delta_1^n=\delta$. Since $(p,n)=1$, there exist $a,b\in\mathbb{Z}$ such that $na+p^sb=1$. We consider that

$$\delta_0=\delta_0^{na+p^sb}=(\delta_0^a)^n\delta^b=(\delta_0^a\delta_1^b)^n.$$

This means that δ_0 is a nth-power element. On the other hand, it is obvious. ∎

Let α be a non-square and non-cube unit of $\mathbb{F}_{p^m}$. There exists $\alpha_0\in\mathbb{F}_{p^m}$ such that $\alpha_0^{p^s}=\alpha$. We will show that $x^6-\alpha_0$ is irreducible over $\mathbb{F}_{p^m}$. Assume that $x^6-\alpha_0$ is reducible over $\mathbb{F}_{p^m}$. There exist an irreducible polynomial $f(x)$ and a polynomial $g(x)$ over $\mathbb{F}_{p^m}$ such that $f(x)g(x)=x^6-\alpha_0$.

Case 1: $\deg(f(x))=1$. There exists $\beta\in\mathbb{F}_{p^m}$ such that $f(\beta)=0$. Thus, we get $0=f(\beta)g(\beta)=\beta^6-\alpha_0$. This means that $\alpha_0=\beta^6$. This is a contradiction.

Case 2: $\deg(f(x)) = 2$. There exist $\beta_0, \beta_1, \gamma_0, \gamma_1, \gamma_2, \gamma_3 \in \mathbb{F}_{p^m}$ such that $f(x) = x^2 + \beta_1 x + \beta_0$ and $g(x) = x^4 + \gamma_3 x^3 + \gamma_2 x^2 + \gamma_1 x + \gamma_0$. We consider that

$$\begin{aligned} x^6 - \alpha_0 &= f(x)g(x) \\ &= (x^2 + \beta_1 x + \beta_0)(x^4 + \gamma_3 x^3 + \gamma_2 x^2 + \gamma_1 x + \gamma_0) \\ &= x^6 + (\gamma_3 + \beta_1)x^5 + (\gamma_2 + \beta_1\gamma_3 + \beta_0)x^4 \\ &\quad + (\gamma_1 + \beta_1\gamma_2 + \beta_0\gamma_3)x^3 + (\gamma_0 + \beta_1\gamma_1 + \beta_0\gamma_2)x^2 \\ &\quad + (\beta_1\gamma_0 + \beta_0\gamma_1)x + \beta_0\gamma_0. \end{aligned}$$

This implies that

$$\gamma_3 + \beta_1 = 0 \tag{2.1}$$
$$\gamma_2 + \beta_1\gamma_3 + \beta_0 = 0 \tag{2.2}$$
$$\gamma_1 + \beta_1\gamma_2 + \beta_0\gamma_3 = 0 \tag{2.3}$$
$$\gamma_0 + \beta_1\gamma_1 + \beta_0\gamma_2 = 0 \tag{2.4}$$
$$\beta_1\gamma_0 + \beta_0\gamma_1 = 0 \tag{2.5}$$
$$\beta_0\gamma_0 = -\alpha_0. \tag{2.6}$$

From Equations (2.1)−(2.4), we have

$$\gamma_3 = -\beta_1 \tag{2.7}$$
$$\gamma_2 = -\beta_0 + \beta_1^2 \tag{2.8}$$
$$\gamma_1 = 2\beta_0\beta_1 - \beta_1^3 \tag{2.9}$$
$$\gamma_0 = -3\beta_0\beta_1^2 + \beta_1^4 + \beta_0^2. \tag{2.10}$$

Again, Equations (2.5), (2.9) and (2.10), we get

$$0 = \beta_1^4 + 3\beta_0^2 - 4\beta_0\beta_1^2 = (\beta_1^2 - 3\beta_0)(\beta_1^2 - \beta_0).$$

As Equations (2.6) and (2.10), we obtain $-\alpha_0 = -3\beta_0^2\beta_1^2 + \beta_0\beta_1^4 + \beta_0^3$.

If $\beta_1^2 - 3\beta_0 = 0$, then $\beta_1^2 = 3\beta_0$. We get $-\alpha_0 = -3\beta_0^2(3\beta_0) + \beta_0(9\beta_0^2) + \beta_0^3 = \beta_0^3$. This means that $\alpha_0 = -\beta_0^3 = (-\beta_0)^3$ which is a contradiction.

If $\beta_1^2 - \beta_0 = 0$, then $\beta_1^2 = \beta_0$. We have

$-\alpha_0 = -3\beta_0^2\beta_0 + \beta_0\beta_0^2 + \beta_0^3 = -\beta_0^3$, implying that $\alpha_0 = \beta_0^3$. It is a contradiction.

Case 3: $\deg(f(x)) = 3$. There exist $\beta_0, \beta_1, \beta_2, \gamma_0, \gamma_1, \gamma_2 \in \mathbb{F}_{p^m}$ such that $f(x) = x^3 + \beta_2 x^2 + \beta_1 x + \beta_0$ and $g(x) = x^3 + \gamma_2 x^2 + \gamma_1 x + \gamma_0$. We consider that

$$\begin{aligned} x^6 - \alpha_0 &= f(x)g(x) \\ &= (x^3 + \beta_2 x^2 + \beta_1 x + \beta_0)(x^3 + \gamma_2 x^2 + \gamma_1 x + \gamma_0) \\ &= x^6 + (\gamma_2 + \beta_2)x^5 + (\gamma_1 + \beta_2\gamma_2 + \beta_1)x^4 + (\gamma_0 + \beta_2\gamma_1 + \beta_1\gamma_2 + \beta_0)x^3 \\ &\quad + (\beta_2\gamma_0 + \beta_1\gamma_1 + \gamma_0\gamma_2)x^2 + (\beta_1\gamma_0 + \beta_0\gamma_1)x + \beta_0\gamma_0. \end{aligned}$$

Thus, we have

$$\gamma_2+\beta_2=0 \tag{2.11}$$
$$\gamma_1+\beta_2\gamma_2+\beta_1=0 \tag{2.12}$$
$$\gamma_0+\beta_2\gamma_1+\beta_1\gamma_2+\beta_0=0 \tag{2.13}$$
$$\beta_2\gamma_0+\beta_1\gamma_1+\beta_0\gamma_2=0 \tag{2.14}$$
$$\beta_1\gamma_0+\beta_0\gamma_1=0 \tag{2.15}$$
$$\beta_0\gamma_0=-\alpha_0. \tag{2.16}$$

From Equations (2.11)−(2.13), we obtain that

$$\gamma_2=-\beta_2 \tag{2.17}$$
$$\gamma_1=-\beta_1+\beta_2^2 \tag{2.18}$$
$$\gamma_0=2\beta_1\beta_2-\beta_0-\beta_2^3. \tag{2.19}$$

As Equations (2.14), (2.17)−(2.19), we have

$$\begin{aligned}0&=\beta_2(2\beta_1\beta_2-\beta_0-\beta_2^3)+\beta_1(-\beta_1+\beta_2^2)+\beta_0(-\beta_2)\\&=2\beta_1\beta_2^2-\beta_0\beta_2-\beta_2^4-\beta_1^2+\beta_1\beta_2^2-\beta_0\beta_2\\&=3\beta_1\beta_2^2-2\beta_0\beta_2-\beta_2^4-\beta_1^2.\end{aligned} \tag{2.20}$$

Again, Equations (2.18), (2.19) and (2.15), we get

$$\begin{aligned}0&=\beta_1(2\beta_1\beta_2-\beta_0-\beta_2^3)+\beta_0(-\beta_1+\beta_2^2)\\&=2\beta_1^2\beta_2-2\beta_0\beta_1-\beta_1\beta_2^3+\beta_0\beta_2^2\\&=-\beta_1\beta_2(\beta_2^2-2\beta_1)+\beta_0(\beta_2^2-2\beta_1)\\&=(\beta_2^2-2\beta_1)(\beta_0-\beta_1\beta_2).\end{aligned}$$

This means that $\beta_2^2-2\beta_1=0$ or $\beta_0-\beta_1\beta_2=0$.

If $\beta_0-\beta_1\beta_2=0$, then $\beta_0=\beta_1\beta_2$. As Equation (2.20), we have

$$0=3\beta_1\beta_2^2-2\beta_1\beta_2^2-\beta_2^4-\beta_1^2=\beta_2^4-\beta_1\beta_2^2+\beta_1^2.$$

By Theorem 2.2, we obtain that β_1 exists if and only if $x^2-\beta_2^2x+\beta_2^4$ has a solution if and only if $p^m\equiv 1 \pmod 3$. This implies that $p^m\equiv 1 \pmod 3$. We consider that

$$0=\beta_2^4-\beta_1\beta_2^2+\beta_1^2=(\beta_1+\delta\beta_2^2)(\beta_1+\delta^{-1}\beta_2^2),$$

where $\delta+\delta^{-1}=-1$. If $\beta_1=-\delta\beta_2^2$, by Equation (2.10), we have

$$\gamma_0=2\beta_1\beta_2-\beta_1\beta_2-\beta_2^3=\beta_1\beta_2-\beta_2^3=-\delta\beta_2^3-\beta_2^3=(-\delta-1)\beta_2^3.$$

This means that $-\alpha_0=\gamma_0\beta_0=(-\delta-1)\beta_2^3(-\delta\beta_2^3)=(\delta^2+\delta)\beta_2^6=-\beta_2^6$, which contradicts the property of α_0. Similarly, if $\beta_1=-\delta^{-1}\beta_2^2$, it is a contradiction.

If $\beta_2^2-2\beta_1=0$, then $\beta_2^2=2\beta_1$. As Equation (2.20), we obtain that

$$\begin{aligned}0&=3\cdot 2^{-1}\beta_2^2\beta_2^2-2\beta_0\beta_2-\beta_2^4-2^{-2}\beta_2^4\\&=(3\cdot 2^{-1}-1-2^{-2})\beta_2^4-2\beta_0\beta_2\\&=\beta_2((3\cdot 2^{-1}-1-2^{-2})\beta_2^3-\beta_0),\end{aligned}$$

implying that $\beta_2=0$ or $(3\cdot 2^{-1}-1-2^{-2})\beta_2^3-\beta_0=0$. If $\beta_2=0$, then $\gamma_0=-\beta_0$ as Equation (2.10). Thus, we have $-\alpha_0=\gamma_0\beta_0=-\beta_0^2$. Thus, we get $\alpha_0=\beta_0^2$. This is a

contradiction. If $(3 \cdot 2^{-1} - 1 - 2^{-2})\beta_2^3 - \beta_0 = 0$, then $4\beta_0 = (6 - 4 - 1)\beta_2^3 = \beta_2^3$. From Equation (2.10), we get $\gamma_0 = 2(2^{-1}\beta_2^2)\beta_2 - \beta_2^3 - \beta_2^3 = -\beta_2^3$. Therefore, we obtain that $\alpha_0 = -\gamma_0\beta_0 = \beta_2^3 2^{-2}\beta_2^3 = 2^{-2}\beta_2^6$ which is a contradiction.

For the cases $\deg(f(x)) = 4$ and $\deg(f(x)) = 5$, it is straightforward. Summarizing the result, we obtain the following proposition.

Proposition 2.4. *Let α be a non-square and non-cube unit of $\mathbb{F}_{p^m}$. Then the irreducible factorization of $x^{6p^s} - \alpha$ over $\mathbb{F}_{p^m}$ is given as $x^{6p^s} - \alpha = (x^6 - \alpha_0)^{p^s}$ where $\alpha_0^{p^s} = \alpha$.*

Next, we give facts of the algebraic coding theory. A *code* C of length n over $\mathtt{R}$ is a nonempty subset of $\mathtt{R}^n$. For an $\mathtt{R}$-submodule C of $\mathtt{R}^n$, it is a *linear code* of length n over $\mathtt{R}$ and each element of C is called *a codeword* of C. The number of codewords of C is denoted by $N_c(C)$. For a unit γ of $\mathtt{R}$, a linear code C is called *a γ-constacyclic code* if $(\gamma c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$, for each $(c_0, c_1, \ldots, c_{n-1}) \in C$ (γ-constacyclic shift). For specific cases, it is called a *cyclic code* when $\gamma = 1$ and it is called a *negacyclic code* when $\gamma = -1$.

Each codeword $\mathbf{a} = (a_0, a_1, ..., a_{n-1})$ is transformed to be its polynomial representation as $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ and, then a code C is viewed as the set of all polynomials representations of its codewords. Thus, in the ring $\frac{\mathtt{R}[x]}{\langle x^n - \gamma\rangle}$, $xa(x)$ corresponds to the γ-constacyclic shift of $\mathbf{a}$. Therefore, each linear code C of length n is a γ-constacyclic code over $\mathtt{R}$ if and only if C is an ideal of the ring $\frac{\mathtt{R}[x]}{\langle x^n - \gamma\rangle}$ by [1].

For a n-tuple $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathtt{R}^n$, the *Hamming weight* of $\mathbf{a}$ is the number of nonzero components of $\mathbf{a}$, denoted by $WT_H(\mathbf{a})$. The number of different components in two elements $\mathbf{a}, \mathbf{b} \in \mathtt{R}^n$ is said to be their *Hamming distance*, denoted by $dist_H(\mathbf{a}, \mathbf{b})$. For a nonzero linear code C, the *Hamming distance* and *Hamming weight* of C is defined as $dist_H(C) = \min\{WT_H(\mathbf{x}) : \mathbf{x} \neq \mathbf{0}, \mathbf{x} \in C\}$. The zero code has Hamming distance 0.

Now, Hamming distance of some repeated-root δ-constacyclic codes of length np^s over $\mathbb{F}_{p^m}$ is provided as follows.

Theorem 2.5. [17] *Let $\delta \in \mathbb{F}_{p^m} \setminus \{0\}$. Suppose that $x^n + \delta_0$ is irreducible over $\mathbb{F}_{p^m}$ where $-\delta_0^{p^s} = \delta$. Then δ-constacyclic codes of length np^s over $\mathbb{F}_{p^m}$ are of the form $C[j] = \langle (x^n + \delta_0)^l \rangle$, where $0 \leq j \leq p^s$. Then*

$$dist_H(C[j]) = \begin{cases} 1, & \text{if } j = 0, \\ 2, & \text{if } 1 \leq j \leq p^{s-1}, \\ l+2, & \text{if } lp^{s-1} + 1 \leq j \leq (l+1)p^{s-1}, \text{ where } l \in \{1, 2, \ldots, p-2\}, \\ (\nu+1)p^k, & \text{if } p^s - p^{s-k} + (\nu-1)p^{s-k-1} + 1 \leq j \leq p^s - p^{s-k} \\ & \quad + \nu p^{s-k-1} \text{ where } \nu \in \{1, 2, \ldots, p-1\} \text{ and} \\ & \quad k \in \{1, 2, \ldots, s-1\}, \\ 0, & \text{if } j = p^s. \end{cases}$$

Let $\mathcal{R}$ denote $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$. Then the set $\mathcal{R}$ consists all polynomials of degree less than 2 with indeterminate u. It is close under usual polynomial addition but its multiplication is polynomial multiplication modulo u^2. It is a routine to obtain that $\mathcal{R}$ is a chain ring with the maximal ideal $\langle u \rangle$ and $a + ub$ is a unit of $\mathcal{R}$ if and only if a is a unit of $\mathbb{F}_{p^m}$, for

any $a, b \in \mathbb{F}_{p^m}$. For each polynomial $f(x)$ of degree n over $\mathcal{R}$, it can be expressed as

$$f(x) = \sum_{i=0}^{n} a_i x^i + u \sum_{i=0}^{n} b_i x^i,$$

where $\sum_{i=0}^{n} a_i x^i$ and $\sum_{i=0}^{n} b_i x^i$ are polynomials over $\mathbb{F}_{p^m}$.

In 2020, Dinh et. al. [15] studied Hamming distance of all constacyclic codes of length $2p^s$ over $\mathcal{R}$ and gave the Singleton Bound for linear codes over $\mathcal{R}$ as follows:

Theorem 2.6. [15] *(Singleton Bound) Let C be a linear code of length n over $\mathcal{R}$ with Hamming distance $dist_H(C)$. Then, the Singleton bound is given by*

$$N_c(C) \leq p^{2m(n-dist_H(C)+1)}.$$

A linear code C of length n over $\mathcal{R}$ is said to be *a maximum distance separable code* if $N_c(C) = p^{2m(n-dist_H(C)+1)}$.

In this work, we investigate the structure of Hamming distance of $(\alpha+u\beta)$-constacyclic codes of length $6p^s$ over $\mathcal{R}$ where $\alpha + u\beta$ is a non-square and non-cube unit of $\mathcal{R}$. This means that each $(\alpha + u\beta)$-constacyclic code is an ideal of $\frac{\mathcal{R}[x]}{\langle x^{6p^s} - (\alpha+u\beta)\rangle}$. We separate the result into 2 cases, i.e., $\beta \neq 0$ and $\beta = 0$. First of all, we determine the structure of Hamming distance of all $(\alpha + u\beta)$-constacyclic codes of such length where α and β are units of $\mathbb{F}_{p^m}$.

3. Hamming distance of $(\alpha + u\beta)$-constacyclic codes of length $6p^s$ over $\mathcal{R}$

First of all, $\mathcal{R}_{\alpha,\beta}$ denotes the quotient ring $\frac{\mathcal{R}[x]}{\langle x^{6p^s} - (\alpha+u\beta)\rangle}$. Let α_0 be an element of $\mathbb{F}_{p^m}$ such that $\alpha_0^{p^s} = \alpha$. Since β is a unit, we obtain that $u = \beta^{-1}(x^{6p^s} - \alpha) = \beta^{-1}(x^6 - \alpha_0)^{p^s}$. In $\mathcal{R}_{\alpha,\beta}$, we have $x^6 - \alpha_0$ is a nilpotent element with index $2p^s$. By Proposition 2.4 and a result in [13, Proposition 3.1], the following lemma is obtained.

Lemma 3.1. *The non-zero polynomial $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$ is invertible in $\mathcal{R}_{\alpha,\beta}$ where $a_i \in \mathbb{F}_{p^m}$ for $i = 0, 1, \ldots, 5$.*

Let $f(x)$ be an arbitrary element in $\mathcal{R}_{\alpha,\beta}$. Then $f(x)$ can be (uniquely) written as

$$\begin{aligned} f(x) = &\sum_{i=0}^{p^s-1} (a_{0i} + a_{1i}x + a_{2i}x^2 + a_{3i}x^3 + a_{4i}x^4 + a_{5i}x^5)(x^6 - \alpha_0)^i \\ &+ u \sum_{i=0}^{p^s-1} (b_{0i} + b_{1i}x + b_{2i}x^2 + b_{3i}x^3 + b_{4i}x^4 + b_{5i}x^5)(x^6 - \alpha_0)^i, \end{aligned} \tag{3.1}$$

where a_{ji} and b_{ji} are elements of $\mathbb{F}_{p^m}$ for $i = 0, 1, \ldots, p^s - 1$ and $j = 0, 1, \ldots, 5$. We consider that

$$f(x) = \sum_{i=0}^{p^s-1} (a_{0i} + a_{1i}x + a_{2i}x^2 + a_{3i}x^3 + a_{4i}x^4 + a_{5i}x^5)(x^6 - \alpha_0)^i$$

$$
\begin{aligned}
&+ u\sum_{i=0}^{p^s-1}(b_{0i}+b_{1i}x+b_{2i}x^2+b_{3i}x^3+b_{4i}x^4+b_{5i}x^5)(x^6-\alpha_0)^i\\
&= a_{0,0}+a_{1,0}x+a_{2,0}x^2+a_{3,0}x^3+a_{4,0}x^4+a_{5,0}x^5\\
&\quad+(x^6-\alpha_0)\sum_{i=1}^{p^s-1}(a_{0i}+a_{1i}x+a_{2i}x^2+a_{3i}x^3+a_{4i}x^4+a_{5i}x^5)(x^6-\alpha_0)^{i-1}\\
&\quad+\beta^{-1}(x^6-\alpha_0)^{p^s}\sum_{i=0}^{p^s-1}(b_{0i}+b_{1i}x+b_{2i}x^2+b_{3i}x^3+b_{4i}x^4+b_{5i}x^5)(x^6-\alpha_0)^i\\
&= a_{0,0}+a_{1,0}x+a_{2,0}x^2+a_{3,0}x^3+a_{4,0}x^4+a_{5,0}x^5+(x^6-\alpha_0)g(x),
\end{aligned}
$$

where $g(x)=\sum_{i=1}^{p^s-1}(a_{0i}+a_{1i}x+a_{2i}x^2+a_{3i}x^3+a_{4i}x^4+a_{5i}x^5)(x^6-\alpha_0)^{i-1}+\beta^{-1}(x^6-\alpha_0)^{p^s-1}\sum_{i=0}^{p^s-1}(b_{0i}+b_{1i}x+b_{2i}x^2+b_{3i}x^3+b_{4i}x^4+b_{5i}x^5)(x^6-\alpha_0)^i$. Hence, we obtain that $f(x)$ is invertible in $\mathcal{R}_{\alpha,\beta}$ if and only if $a_{0,0}+a_{1,0}x+a_{2,0}x^2+a_{3,0}x^3+a_{4,0}x^4+a_{5,0}x^5\neq 0$. This implies that the set of all non-invertible elements of $\mathcal{R}_{\alpha,\beta}$ is $\langle x^6-\alpha_0\rangle$. Therefore, $\mathcal{R}_{\alpha,\beta}$ is a local ring with the unique maximal ideal $\langle x^6-\alpha_0\rangle$. By Proposition 2.1, the following theorem is obtained as:

Theorem 3.2. *Let $\alpha+u\beta$ a non-square and non-cube unit of $\mathcal{R}$ and $\alpha_0^{p^s}=\alpha$. Then $\mathcal{R}_{\alpha,\beta}$ is a chain ring whose ideals $\langle(x^6-\alpha_0)^j\rangle$, for $j\in\{0,1,\ldots,2p^s\}$. Each $(\alpha+u\beta)$-constacyclic code of length $6p^s$ over $\mathcal{R}$ is of the form $\langle(x^6-\alpha_0)^j\rangle\subseteq\mathcal{R}_{\alpha,\beta}$, for $j\in\{0,1,\ldots,2p^s\}$. Moreover, the number of codewords of $\langle(x^6-\alpha_0)^j\rangle$ is equal to $p^{6m(2p^s-j)}$.*

Now, we need to determine the Hamming distance of each $\alpha+u\beta$-constacyclic code of length $6p^s$ over $\mathcal{R}$.

Theorem 3.3. *Let notation be as Theorem 3.2. Then the Hamming distance of $C=\langle(x^6-\alpha_0)^j\rangle$ is given as*

$$
dist_H(C)=\begin{cases}
1, & \text{if } 0\le j\le p^s,\\
2, & \text{if } p^s+1\le j\le p^s+p^{s-1},\\
l+2, & \text{if } p^s+lp^{s-1}+1\le j\le p^s+(l+1)p^{s-1},\\
 & \quad \text{where } l\in\{1,2,\ldots,p-2\},\\
(\nu+1)p^k, & \text{if } 2p^s-p^{s-k}+(\nu-1)p^{s-k-1}+1\le j\le 2p^s-p^{s-k}\\
 & \quad +\nu p^{s-k-1},\ \text{where } \nu\in\{1,2,\ldots,p-1\} \text{ and}\\
 & \quad k\in\{1,2,\ldots,s-1\},\\
0, & \text{if } j=2p^s.
\end{cases}
$$

Proof. It is obvious that $dist_H(\langle(x^6-\alpha_0)^0\rangle)=1$ and $dist_H(\langle(x^6-\alpha_0)^{2p^s}\rangle)=0$. We remain the case $1\le j\le 2p^s-1$ and separate the integer i into 2 cases, i.e., $1\le j\le p^s$ and $p^s+1\le j\le 2p^s-1$.

Case 1: $1\le j\le p^s$**.** We consider that $u=\beta^{-1}(x^6-\alpha_0)^{p^s}=\beta^{-1}(x^6-\alpha_0)^{p^s-j}(x^6-\alpha_0)^j\in\langle(x^6-\alpha_0)^j\rangle$. As $WT_H(u)=1$, we obtain that $dist_H(\langle(x^6-\alpha_0)^j\rangle)=1$.

Case 2: $p^s+1\le j\le 2p^s-1$**.** Note that $u=\beta^{-1}(x^6-\alpha_0)^{p^s}$. Let $f(x)$ be an arbitrary element in $\langle(x^6-\alpha_0)^j\rangle$. Then $f(x)$ can be expressed as

$$
f(x)=u(x^6-\alpha_0)^{j-p^s}\sum_{i=0}^{p^s-1}(a_{0i}+a_{1i}x+a_{2i}x^2+a_{3i}x^3+a_{4i}x^4+a_{5i}x^5)(x^6-\alpha_0)^i,
$$

where $a_{0i}, a_{1i}, a_{2i}, a_{3i}, a_{4i}$ and $a_{5i} \in \mathbb{F}_{p^m}$. Note that $1 \leq j - p^s \leq p^s - 1$. $C[l]$ denotes an ideal with the generator $(x^6 - \alpha_0)^l$ of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{6p^s} - \alpha\rangle}$. Thus, each element $f(x)$ can be identified as an element in $uC[j - p^s]$, implying that $dist_H(\langle (x^6 - \alpha_0)^j\rangle) = dist_H(C[j - p^s])$. As Theorem 2.5, $dist_H(C[l])$ is given, and then $dist_H(\langle (x^6 - \alpha_0)^j\rangle)$ is also obtained. ∎

In the remaining result of this section, we identify the maximum distance separable $(\alpha + u\beta)$-constacyclic codes of length $6p^s$ over $\mathcal{R}$.

Theorem 3.4. *Let notation be as Theorem 3.2 and $C = \langle (x^6 - \alpha_0)^j\rangle$ for $0 \leq j \leq 2p^s$. Then, the only maximum distance separable $(\alpha + u\beta)$-constacyclic code of length $6p^s$ over $\mathcal{R}$ is $\mathcal{R}_{\alpha,\beta}$.*

Proof. Note that $N_c(C) = p^{6m(2p^s - j)}$. We divide this proof into 5 cases as the value $dist_H(C)$ in Theorem 3.3.

Case 1: $j \in \{0, 1, \ldots, p^s\}$. We obtain that $d(C) = 1$. Thus, C is MDS code if $p^{6m(2p^s - j)} = p^{2m(6p^s - 1 + 1)} = p^{12mp^s}$. This implies that $2p^s - j = 2p^s$, i.e., $j = 0$.

Case 2: $j \in \{p^s + 1, p^s + 2, \ldots, p^s + p^{s-1}\}$. Note that $dist_H(C)$ is equal to 2. We consider that $p^{6m(2p^s - j)} = N_c(C) = p^{2m(6p^s - 2 + 1)} = p^{12mp^s - 2m}$. We get $12mp^s - 6mi = 12mp^s - 2m$, and then $j = \frac{1}{3}$. It is impossible.

Case 3: $j \in \{p^s + lp^{s-1} + 1, p^s + lp^{s-1} + 2, dots, p^s + (l+1)p^{s-1}\}$, where $l \in \{1, 2, \ldots, p-2\}$. In this case, we have $dist_H(C) = l + 2$. We consider that $p^{6m(2p^s - j)} = N_c(C) = p^{2m(6p^s - (l+2) + 1)} = p^{12mp^s - 2ml - 2m}$. This implies that $12mp^s - 6mi = 12mp^s - 2ml - 2m$, i.e., $i = \frac{l+1}{3}$. Thus, we obtain that $\frac{2}{3} \leq j \leq \frac{p-1}{3}$ but minimum value j is $p^s + p^{s-1} + 1$. It is impossible.

Case 4: $j \in \{2p^s - p^{s-k} + (\nu - 1)p^{s-k-1} + 1, 2p^s - p^{s-k} + (\nu - 1)p^{s-k-1} + 2, \ldots, 2p^s - p^{s-k} + \nu p^{s-k-1}\}$, where $\nu \in \{1, 2, \ldots, p - 1\}$ and $k \in \{1, 2, \ldots, s - 1\}$. By Theorem 3.3, the Hamming distance of C is $(\nu + 1)p^k$. We consider $p^{6m(2p^s - j)} = N_c(C) = p^{2m(6p^s - (\nu+1)p^k + 1)} = p^{12mp^s - 2m\nu p^k - 2mp^k + 2m}$. This means that $12mp^s - 6mj = 12mp^s - 2m\nu p^k - 2mp^k + 2m$, and then $j = \frac{\nu p^k + p^k - 1}{3}$. However, $\frac{\nu p^k + p^k - 1}{3}$ is not in the interval $\left[2p^s - p^{s-k} + (\nu - 1)p^{s-k-1} + 1, 2p^s - p^{s-k} + \nu p^{s-k-1}\right]$. It is impossible.

Case 5: $j = 2p^s$. We get $dist_H(C) = 0$. We consider that $1 = N_c(C) = p^{2m(6p^s - 0 + 1)} = p^{2m(6p^s + 1)}$. This means that $6p^s + 1 = 0$. It is impossible.

Hence, there is only the quotient ring $\mathcal{R}_{\alpha,\beta}$ which is a MDS code. ∎

4. Hamming distance of α-constacyclic codes of length $6p^s$ over $\mathcal{R}$

In this section, we denote the quotient ring $\frac{\mathcal{R}[x]}{\langle x^{6p^s} - \alpha\rangle}$ by $\mathcal{R}_\alpha$. By the same method in [9–12], the following results are obtained.

Theorem 4.1. *Let notation be as Proposition 2.4. Then the quotient ring $\mathcal{R}_\alpha$ is a local ring with the maximal ideal $\langle x^6 - \alpha_0, u\rangle$ but it is not a chain ring. Moreover, ideals of $\mathcal{R}_\alpha$, α-constacyclic codes of length $6p^s$ over $\mathcal{R}$, are listed as follows:*

(1) (trivial ideals) $\langle 0\rangle$ and $\langle 1\rangle$,
(2) (principal ideals with nonmonic polynomial generators) $\langle u(x^6 - \alpha_0)^j\rangle$, where $0 \leq j \leq p^s - 1$,
(3) (principal ideals with monic polynomial generators) $\langle (x^6 - \alpha_0)^j + u(x^6 - \alpha_0)^t h(x)\rangle$, where $1 \leq j \leq p^s - 1, 0 \leq t < i$ and either $h(x)$

is 0 or $h(x)$ is a unit which can be represented as $h(x) = \sum_{i=0}^{p^s-1}(h_{0i} + h_{1i}x + h_{2i}x^2 + h_{3i}x^3 + h_{4i}x^4 + h_{5i}x^5)(x^6 - \alpha_0)^i$, with $h_{0i}, h_{1i}, h_{2i}, h_{3i}, h_{4i}, h_{5i} \in \mathbb{F}_{p^m}$ and $h_{0,0} + h_{1,0}x + h_{2,0}x^2 + h_{3,0}x^3 + h_{4,0}x^4 + h_{5,0}x^5 \neq 0$.

(4) (nonprincipal ideals) $\langle (x^6 - \alpha_0)^j + u(x^6 - \alpha_0)^t h(x), u(x^6 - \alpha_0)^\omega \rangle$, with $h(x)$ as in Type 3 where $1 \leq j \leq p^s - 1$, $0 \leq t < j$, $\omega < T$ and T is the smallest positive integer such that $u(x^6 - \alpha_0)^T \in \langle (x^6 - \alpha_0)^j + u(x^6 - \alpha_0)h(x) \rangle$. Moreover, $T = j$, if $h(x) = 0$, otherwise $T = \min\{j, p^s - j + t\}$.

Proposition 4.2. *Let notation be as Theorem 4.1. Let C be an α-constacyclic code of length $6p^s$ over $\mathcal{R}$. Then the number of codewords of C is obtained as follows.*

(1) If $C = \langle 0 \rangle$, then $N_c(C) = 1$.

(2) If $C = \langle 1 \rangle$, then $N_c(C) = p^{12mp^s}$.

(3) $C = \langle u(x^6 - \alpha_0)^j \rangle$ where $j \in \{0, 1, \ldots, p^s - 1\}$, then $N_c(C) = p^{6m(p^s - j)}$.

(4) If $C = \langle (x^6 - \alpha_0)^j + u(x^6 - \alpha_0)^t h(x) \rangle$, where $j \in \{1, 2, \ldots, p^s - 1\}, t \in \{0, 1, \ldots, j - 1\}$, then

$$N_c(C) = \begin{cases} p^{12m(p^s-j)}, & \text{if } h(x) = 0, \\ p^{12m(p^s-j)}, & \text{if } h(x) \neq 0 \text{ and } j \in \{1, 2, \ldots, \lfloor \frac{p^s+t}{2} \rfloor\}, \\ p^{6m(p^s-t)}, & \text{if } h(x) \neq 0 \text{ and } j \in \{\lceil \frac{p^s+t}{2} \rceil, \lceil \frac{p^s+t}{2} \rceil + 1, \ldots, p^s - 1\}. \end{cases}$$

(5) If $C = \langle (x^6 - \alpha_0)^j + u(x^6 - \alpha_0)^t h(x), u(x^6 - \alpha_0)^\omega \rangle$ where $j \in \{1, 2, \ldots, p^s - 1\}$, $t \in \{0, 1, \ldots, j - 1\}$ and $\omega \leq T - 1$, then

$$N_c(C) = p^{6m(2p^s - j - \omega)} \text{ where } \omega < \begin{cases} j, & \text{if } h(x) = 0, \\ \min\{p^s - j + t, j\}, & \text{if } h(x) \neq 0. \end{cases}$$

Next, we determine the Hamming distances of α-constacyclic codes of length $6p^s$ over $\mathcal{R}$. For each codeword $\mathbf{r} = (r_0, r_1, \ldots, r_{n-1})$ in $\mathcal{R}^n$, it can be viewed as a polynomial $r(x)$ given as $r(x) = a(x) + ub(x)$, where $a(x) = \sum_{i=0}^{n-1} a_i x^i, b(x) = \sum_{i=0}^{n-1} b_i x^i \in \mathbb{F}_{p^m}[x]$ and $r_i = a_i + ub_i \in \mathcal{R}$. Two polynomials $a(x)$ and $b(x)$ corresponds words $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$ in $\mathbb{F}_{p^m}^n$. Thus, $r_i = 0$ if and only if $a_i = b_i = 0$, and then

$$WT_H(c(x)) \geq \max\{WT_H(a(x)), WT_H(b(x))\}. \tag{4.1}$$

In Type 1, the Hamming distances of $\langle 0 \rangle$ and $\langle 1 \rangle$ are equal to 0 and 1, respectively. For $C = \langle u(x^6 - \alpha_0)^j \rangle$ in Type 2, $0 \leq j \leq p^s - 1$, each codeword of C is an element multiplied by u in $C[j]$ where $C[j]$ is an ideal with the generator $(x^6 - \alpha_0)^j$ of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{6p^s} - \alpha \rangle}$. Hence, $dist_H(C) = dist_H(C[j]))$.

Theorem 4.3. *Let notation be as Theorem 4.1. If $C = \langle u(x^6 - \alpha_0)^j \rangle$ where $j \in \{0, 1, \ldots, p^s - 1\}$, then*

$$dist_H(C) = \begin{cases} 1, & \text{if } j = 0, \\ 2, & \text{if } 1 \leq j \leq p^{s-1}, \\ l + 2, & \text{if } lp^{s-1} + 1 \leq j \leq (l+1)p^{s-1}, \\ & \quad \text{where } l \in \{1, 2, \ldots, p - 2\}, \\ (\nu + 1)p^k, & \text{if } p^s - p^{s-k} + (\nu - 1)p^{s-k-1} + 1 \leq j \leq p^s - p^{s-k} \\ & \quad + \nu p^{s-k-1}, \text{ where } \nu\{1, 2, \ldots, p - 1\} \text{ and} \\ & \quad k \in \{1, 2, \ldots, s - 1\}. \end{cases}$$

For your convenience, an ideal with the generator $(x^6-\alpha_0)^j$ of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{6p^s}-\alpha\rangle}$ is denoted by $C[j]$ or $\langle (x^6-\alpha_0)^j\rangle_{\mathbb{F}_{p^m}}$, where $0\le j\le p^s$. Now, we determine the Hamming distances of all constacyclic codes in Type 3 as follows:

Theorem 4.4. *Let notation be as Theorem 4.1. If* $C=\langle (x^6-\alpha_0)^j+u(x^6-\alpha_0)^t h(x)\rangle$ *where* $j\in\{1,2,\ldots,p^s-1\}$ *and* $t\in\{0,1,\ldots,j-1\}$, *then*

$$dist_H(C)=\begin{cases}2, & \text{if } 1\le j\le p^{s-1},\\ l+2, & \text{if } lp^{s-1}+1\le j\le (l+1)p^{s-1},\\ & \quad \text{where } l\in\{1,2,\ldots,p-2\},\\ (\nu+1)p^k, & \text{if } p^s-p^{s-k}+(\nu-1)p^{s-k-1}+1\le j\le p^s-p^{s-k}\\ & \quad +\nu p^{s-k-1},\ \text{where } \nu\in\{1,2,\ldots,p-1\} \text{ and}\\ & \quad k\in\{1,2,\ldots,s-1\}.\end{cases}$$

Proof. Since $u(x^6-\alpha_0)^j\in C$, we have $dist_H(C)\le dist_H(\langle u(x^6-\alpha_0)^i\rangle)=dist_H(C[j])$. Let $f(x)\in C$. Then, there exist $f_1(x),f_2(x)\in\mathbb{F}_{p^m}[x]$ such that

$$\begin{aligned}f(x)&=\big(f_1(x)+uf_2(x)\big)\big((x^6-\alpha_0)^j+u(x^6-\alpha_0)^t h(x)\big)\\&=f_1(x)(x^6-\alpha_0)^j+ur(x),\end{aligned}$$

where $r(x)=f_2(x)(x^6-\alpha_0)^j+f_1(x)(x^6-\alpha_0)^t h(x)$ Thus, by inequality 4.1, we have

$$\begin{aligned}WT_H(f(x))&\ge\max\{WT_H(f_1(x)(x^6-\alpha_0)^j),WT_H(r(x))\}\\&\ge\max\{WT_H(f_1(x)(x^6-\alpha_0)^j),WT_H(f_2(x)(x^6-\alpha_0)^j)\}\\&\ge dist_H(C[j]).\end{aligned}$$

Hence, it implies that $dist_H(C)=dist_H(C[j])$. ∎

Example 4.5. Given $p=5,s=1$ and $m=2$, then $\mathbb{F}_{25}:=\frac{\mathbb{Z}_5[w]}{\langle w^2+4w+2\rangle}$ and $x^{30}-w=(x^6-(4w+1))^5$. Let $C=\langle (x^6-(4w+1))^4\rangle$ be a w-constacyclic code of length 30 over $\mathbb{F}_{25}+u\mathbb{F}_{25}$. Each codeword $c(x)$ in C is expressed as

$$c(x)=(x^6-(4w+1))^4\big((a_0+a_1x+a_2x^2+a_3x^3+a_4x^4)+(b_0+b_1x+b_2x^2+b_3x^3+b_4x^4)u\big),$$

where $a_i,b_i\in\mathbb{F}_{p^m}$, $i=0,1,2,3,4$. Thus, the number of codewords of C is $(25^2)^5$. By Theorem 4.4, the Hamming distance of C is equal to 5. Thus, we get $p^{2m(n-dist_H(C)+1)}=5^{4(30-5+1)}=5^{104}$. By Singleton Bound, we obtain $N_c(C)=5^{20}<5^{104}=p^{2m(n-dist_H(C)+1)}$, implying that C is not a maximum distance separable code.

Theorem 4.6. *Let notation be as Theorem 4.1. If* $C=\langle (x^6-\alpha_0)^j+u(x^6-\alpha_0)^t h(x),u(x^6-\alpha_0)^\omega\rangle$ *where* $j\in\{1,2,\ldots,p^s-1\}$, $t\in\{0,1,\ldots,j-1\}$ *and* $\omega\le T-1$, *then*

$$dist_H(C)=\begin{cases}2, & \text{if } 1\le\omega\le p^{s-1},\\ l+2, & \text{if } lp^{s-1}+1\le\omega\le(l+1)p^{s-1},\ \text{where } l\in 1,2,\ldots,p-2,\\ (\nu+1)p^k, & \text{if } p^s-p^{s-k}+(\nu-1)p^{s-k-1}+1\le\omega\le p^s-p^{s-k}\\ & \quad +\nu p^{s-k-1},\ \text{where } \nu\in\{1,2,\ldots,p-1\} \text{ and}\\ & \quad k\in\{1,2,\ldots,s-1\}.\end{cases}$$

Proof. Since $u(x^6-\alpha_0)^\omega \in C$, we have $dist_H(C) \leq dist_H(\langle u(x^6-\alpha_0)^\omega\rangle) = dist_H(C[\omega])$. Let $c(x) \in C$. There exist $f_1(x)+uf_2(x), g_1(x)+ug_2(x) \in \mathcal{R}[x]$ such that

$$\begin{aligned} c(x) &= \big(f_1(x)+uf_2(x)\big)\big((x^6-\alpha_0)^j + u(x^6-\alpha_0)^t h(x)\big) \\ &\quad + \big(g_1(x)+ug_2(x)\big)u(x^6-\alpha_0)^\omega \\ &= f_3(x)(x^6-\alpha_0)^\omega + ur(x), \end{aligned}$$

where $f_3(x) = f_1(x)(x^6-\alpha_0)^{j-\omega}$ and $r(x) = f_1(x)(x^6-\alpha_0)^t h(x) + f_2(x)(x^6-\alpha_0)^j + g_1(x)(x^6-\alpha_0)^\omega$. Note that

$$\begin{aligned} r(x) &= f_1(x)(x^6-\alpha_0)^t h(x) + f_2(x)(x^6-\alpha_0)^j + g_1(x)(x^6-\alpha_0)^\omega \\ &= f_1(x)h(x)(x^6-\alpha_0)^t + r_1(x)(x^6-\alpha_0)^\omega, \end{aligned}$$

where $r_1(x) = f_2(x)(x^6-\alpha_0)^{j-\omega} + g_1(x)$. By Inequality 4.1, we obtain that

$$\begin{aligned} WT_H(c(x)) &\geq \max\{WT_H(f_3(x)(x^6-\alpha_0)^\omega), WT_H(r(x))\} \\ &\geq \max\{WT_H(f_3(x)(x^6-\alpha_0)^\omega), WT_H(r_1(x)(x^6-\alpha_0)^\omega)\} \\ &\geq dist_H(C[\omega]). \end{aligned}$$

Thus, $dist_H(C) \geq dist_H(C[\omega])$, implying that $dist_H(C) = dist_H(C[\omega])$. ∎

The rest of this section to determine of MDS α-constacyclic codes of length $6p^s$ over $\mathcal{R} = \frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$.

Theorem 4.7. *Let notation be as Theorem 4.1. Then, the only maximum distance separable α-constacyclic code of length $6p^s$ over $\mathcal{R}$ is $\mathcal{R}_\alpha$.*

Proof. **Type 1:** If $C = \langle 0\rangle$, then $dist_H(C) = 0$. We consider that $1 = N_c(C) = p^{2m(6p^s-0+1)}$. This means that $6p^s+1 = 0$. It is impossible. If $C = \langle 1\rangle$, then $dist_H(C) = 1$. For C is a MDS code, we have $N_c(C) = p^{12mp^s} = p^{2m(6p^s-1+1)}$. Thus, $C = \langle 1\rangle$ is a MDS code.

Type 2: Let $C = \langle u(x^6-\alpha_0)^j\rangle$ be an α-constacyclic code of length $6p^s$ over $\mathcal{R}$ where $j \in \{0,1,\ldots,p^s-1\}$. If $j = 0$, then $dist_H(C) = 1$. We consider that $p^{6mp^s} = N_c(C) = p^{2m(6p^s-1+1)} = p^{12mp^s}$ which is a contradiction. If $j \in \{1,2,\ldots,p^{s-1}\}$, then $dist_H(C) = 2$. For C is MDS, we have $p^{6m(p^s-j)} = N_c(C) = p^{2m(6p^s-2+1)}$. Thus, we get $j = -\frac{3p^s+1}{3}$ which is impossible. If $j \in \{lp^{s-1}+1, lp^{s-1}+2,\ldots,(l+1)p^{s-1}\}$ where $l \in \{1,2,\ldots,p-2\}$, then $dist_H(C) = l+1$. We consider that $p^{6m(p^s-j)} = N_c(C) = p^{2m(6p^s-(l+1)+1)}$. This implies that $j = -\frac{3p^s-l}{3}$. It is impossible. if $j \in \{p^s-p^{s-k}+(\nu-1)p^{s-k-1}+1, p^s-p^{s-k}+(\nu-1)p^{s-k-1}+2,\ldots,p^s-p^{s-k}+\nu p^{s-k-1}\}$ where $\nu \in \{1,2,\ldots,p-1\}$ and $k \in \{1,2,\ldots,s-1\}$, then $dist_H(C) = (\nu+1)p^k$. Assume that C is a MDS code. We have $p^{6m(p^s-j)} = N_c(C) = p^{2m(6p^s-(\nu+1)p^k+1)}$, and then $j = -\frac{3mp^s-(\nu+1)p^k+1}{3}$. It is a contradiction.

Type 3: Let $C = \langle (x^6-\alpha_0)^j + u(x^6-\alpha_0)^t h(x)\rangle$ where $j \in \{1,2,\ldots,p^s-1\}$ and $t \in \{0,1,\ldots,j-1\}$. In the case $h(x) = 0$, we have $N_c(C) = p^{12m(p^s-j)}$. Assume that C is MDS. Thus, we get $p^{12m(p^s-j)} = N_c(C) = p^{2m(6p^s-dist_H(C)+1)}$, implying that $j = \frac{dist_H(C)-1}{6}$. If $j \in \{1,2,\ldots,p^{s-1}\}$, then $dist_H(C) = 2$. This means that $j = \frac{1}{3}$. It is impossible. If $j \in \{lp^{s-1}+1, lp^{s-1}+2,\ldots,(l+1)p^{s-1}\}$ for $l \in \{1,2,\ldots,p-2\}$, then $j = \frac{l+1}{3} \leq \frac{p-2}{3}$ which is a contradiction. If $j \in \{p^s-p^{s-k}+(\nu-1)p^{s-k-1}+1, p^s-p^{s-k}+(\nu-1)p^{s-k-1}+2,\ldots,p^s-p^{s-k}+\nu p^{s-k-1}\}$ such that $\nu \in \{1,2,\ldots,p-1\}$

and $k \in \{1, 2, \ldots, s-1\}$, then $j = \frac{(\nu+1)p^k-1}{3} \leq \frac{p^s-1}{3}$. It is impossible. In the case $h(x) \neq 0$ and $j \in \{1, 2, \ldots, \lfloor \frac{p^s+t}{2} \rfloor\}$, we have $N_c(C) = p^{12m(p^s-j)}$. As the above case, it is impossible. For the remaining case $h(x) \neq 0$ and $j \in \{\lceil \frac{p^s+t}{2} \rceil, \lceil \frac{p^s+t}{2} \rceil + 1, \ldots, p^s-1\}$, we have $N_c(C) = p^{6m(p^s-t)}$. We consider that $p^{6m(p^s-t)} = N_c(C) = p^{2m(6p^s-dist_H(C)+1)}$, implying that $t = -\frac{6p^s-dist_H(C)+1}{3}$ which is a contradiction.

Type 4: Let $C = \langle (x^6-\alpha_0)^j + u(x^6-\alpha_0)^t h(x), u(x^6-\alpha_0)^\omega \rangle$ where $j \in \{1, 2, \ldots, p^s-1\}$, $t \in \{0, 1, \ldots, j-1\}$ and $\omega \leq T-1$. Then $N_c(C) = p^{6m(2p^s-j-\omega)}$. Assume that C is MDS. We get $p^{6m(2p^s-j-\omega)} = N_c(C) = p^{2m(6p^s-dist_H(C)+1)}$. Thus, we have $3j + 3\omega = dist_H(C) - 1$ and consider

$$3\omega = dist_H(C) - 1 - 3j < dist_H(C) - 1 - 3\omega.$$

This means that $\omega < \frac{dist_H(C)-1}{6}$. Therefore, it follows from Type 3, and then it is impossible. Hence, $\mathcal{R}_\alpha$ is only MDS code. ∎

5. Conclusion

Let $\alpha + u\beta$ be a non-square and non-cube unit of $\mathcal{R} = \frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$. The Hamming distances of all $(\alpha + u\beta)$-constacyclic codes of length $6p^s$ over $\mathcal{R}$ can be obtained from Hamming distances of α-constacyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$. Furthermore, the MDS $(\alpha + u\beta)$-constacyclic codes of length $6p^s$ over $\mathcal{R}$ is only $\frac{\mathcal{R}[x]}{\langle x^{6p^s}-(\alpha+u\beta)\rangle}$ (both $\beta \neq 0$ and $\beta = 0$). However, the case $\alpha + u\beta$ is a square or cube unit, it is still an open problem for the future work.

Acknowledgements

This project is funded by National Research Council of Thailand (Grant No. NRCT5-RSA63011-05).

References

[1] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

[2] D. I. N. G. Jian, L. I. Hongju, The Hamming distances of a class of p-ary negacyclic codes, Chin. J. Electron. 27(1) (2018) 46-51.

[3] N. T. Bac, Hamming distances of repeated-root constacyclic codes of prime power lengths over $\mathbb{F}_{5^m} + u\mathbb{F}_{5^m}$, Southeast Asian J. Soc. Sci. 6(1) (2018) 10-16.

[4] X. Liu, S. Zhu, The distributions of distances of $(1+\lambda u)$-constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{k-1}\mathbb{F}_{p^m}$, J. Univ. Sci. Technol. China. 11 (2012).

[5] 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.

[6] S.D. Berman, Semisimple cyclic and Abelian codes. II, Kibernetika (Kiev) 3 (1967) 21–30 (in Russian); translated as Cybernetics 3 (1967) 17–23.

[7] G. Castagnoli, J. L. Massey, P. A. Schoeller, N. von Seemann, On repeated-root cyclic codes, IEEE Trans. Inf. Theory. 37 (1991) 337–342.

[8] J. H. van Lint, Repeated-root cyclic codes, IEEE Trans. Inf. Theory. 37 (1991) 343–345.

[9] B. Chen, H. Q. Dinh, H. Liu, L. Wang, Constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, Finite Fields Appl. 37 (2016) 108-130.

[10] H. Q. Dinh, Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, J. Algebra. 324(5) (2010) 940-950.

[11] J. Phuto, C. Klin-Eam, Explicit constructions of cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, Discrete Math Algorithms Appl. 12(05) (2020) 2050063.

[12] Y. Cao, Y. Cao, H. Q. Dinh, F. W. Fu, J. Gao, S. Sriboonchitta, Constacyclic codes of length np^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, Adv. Math. Commun. 12(2) (2018) 231-262.

[13] W. Zhao, X. Tang, Z. Gu, All $\alpha+u\beta$-constacyclic codes of length np^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, Finite Fields Appl. 50 (2018) 1-16.

[14] H. Q. Dinh, B. T. Nguyen, A. K. Singh, S. Sriboonchitta, Hamming and Symbol-Pair Distances of Repeated-Root Constacyclic Codes of Prime Power Lengths Over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, IEEE Commun. Lett. 22(12) (2018) 2400-2403.

[15] H. Q. Dinh, A. Gaur, I. Gupta, A. K. Singh, M. K. Singh, R. Tansuchat, Hamming distance of repeated-root constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, Appl. Algebra Eng. Commun. Comput. 31 (2020) 291-305.

[16] H. Q. Dinh, S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inf. Theory. 50(8) (2004) 1728-1744.

[17] S. R. López-Permouth, H. Özadam, F. Özbuda, S. Szabo, Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes, Finite Fields Appl. 19(1) (2013) 16-38.