On the Hamming Distance of Repeated-Root Cyclic Codes of Length $6p^s$

HAI Q. DINH$^{1,3}$, XIAOQIANG WANG$^2$, AND PARAVEE MANEEJUK$^4$

$^1$Division of Computational Mathematics and Engineering, Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
$^2$Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
$^3$Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China
$^4$Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University, Chiang Mai 50200, Thailand

Corresponding author: Xiaoqiang Wang (waxiqg@163.com)

This work was supported in part by the Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University, Thailand.

**ABSTRACT** Let $p$ be an odd prime, $s$, $m$ be positive integers such that $p^m \equiv 2 \pmod{3}$. In this paper, using the relationship about Hamming distances between simple-root cyclic codes and repeated-root cyclic codes, the Hamming distance of all cyclic codes of length $6p^s$ over finite field $\mathbb{F}_{p^m}$ is obtained. All maximum distance separable (MDS) cyclic codes of length $6p^s$ are established.

**INDEX TERMS** Simple-root code, repeated-root code, Hamming distance, MDS code.

I. INTRODUCTION

Cyclic codes over finite fields have been well studied since the late 1950s because of their rich algebraic structures and practical implementations. Many well known codes, such as BCH, Kerdock, Golay, Reed-Muller, Preparata, Justesen, and binary Hamming codes, are either cyclic codes or constructed from cyclic codes. All of those explain their preferred role in engineering.

Let $\mathbb{F}_{p^m}$ be a finite field. Cyclic codes of length $n$ over $\mathbb{F}_{p^m}$ are classified as the ideals $(g(x))$ of the quotient ring $\mathbb{F}_{p^m}[x]/(x^n - 1)$, where the generator polynomial $g(x)$ is the unique monic polynomial of minimum degree in the code, which is a divisor of $x^n - 1$. In general, cyclic codes are grouped into two classes: simple-root cyclic codes, where the generator polynomial $g(x)$ has no repeated irreducible factors; and repeated-root cyclic codes, where the generator polynomial $g(x)$ has repeated roots. Repeated-root cyclic codes were first initiated in the most generality by Castagnoli et al. in [1] and Van Lint in [21], where it was proved that they are asymptotically bad, nevertheless, it turns out that optimal repeated-root cyclic codes still exist, which have motivated the researchers to further study these codes (see, for example, [14], [20].)

The classification of codes plays an important role in studying their structures, but in general, it is very difficult. In a series of paper [4]–[8], Dinh determined the algebraic structure in terms of polynomial generators of all cyclic codes over finite field $\mathbb{F}_{p^m}$ of length $p^s$, $2p^s$, $3p^s$, $4p^s$ and $6p^s$. Since then, these results have been extended to more general code lengths (see, for example, [2], [3], [11], [19].)

However, little work has been done on determining the Hamming distance of cyclic codes as it is a very hard task in general. By now, only a few results have been obtained. In [4], Dinh determined the Hamming distance of cyclic codes of length $p^s$ over $\mathbb{F}_{p^m}$. Later, in [16] the authors computed the Hamming distance of cyclic codes of length $2p^s$ by using the result of [1]. Recently, based on the relationship of Hamming distances between simple-root cyclic codes and repeated-root cyclic codes, the Hamming distance of cyclic codes of length $3p^s$ were determined for the case gcd($3, p^m - 1$) = 1 in [11]. Motivated by these, in this paper, we get all Hamming distance of cyclic codes of length $6p^s$ over the finite field $\mathbb{F}_{p^m}$ for the case $p^m \equiv 2 \pmod{3}$. As an application, all such MDS cyclic codes of length $6p^s$ are obtained, which can be used to construct quantum MDS codes using well known constructions such as CSS construction.

The remainder of this paper is organized as follows. Section 2 recalls some preliminary results. In Section 3, the Hamming distance of cyclic codes of length $6p^s$ are given for the case $p^m \equiv 2 \pmod{3}$. Using that, Section 4 identifies all MDS codes among such cyclic codes. Section 5 concludes the paper.

II. PRELIMINARIES

Let $\mathbb{F}_{p^m}$ be the finite field of order $p^m$. A code $C$ of length $n$ over $\mathbb{F}_{p^m}$ is a nonempty subset of $\mathbb{F}_{p^m}^n$. A linear code $C$ over
Clearly, for any positive integer \( s \) and \( 0 \leq \theta \leq s - 1 \),
the Hamming distance of cyclic codes of length \( 6p^s \) over \( \mathbb{F}_{p^m} \) for the case \( p^m \equiv 2 \pmod{3} \),
all cyclic codes of length \( 6p^s \) have the form
\[
C = \{(x^2 + x + 1)^t(x^2 - x + 1)^i(x - 1)^u(x^3 + 1)^v) \mid 0 \leq i, j, u, v \leq p^s - 1, \text{ and the equality holds when} \]
\[
eq (x^2 + x + 1)^t(x^2 - x + 1)^i(x - 1)^u(x^3 + 1)^v, \quad (1)
\]
where \( \tilde{C} \) is defined in Proposition 2.2.

3.1. Case 0: \( 0 \leq v \leq u \leq j \leq i \leq p^s \)

We now determine the Hamming distance of \( C = \{(x^2 + x + 1)^t(x^2 - x + 1)^i(x - 1)^u(x^3 + 1)^v) \) for the case \( 0 \leq v \leq u \leq j \leq i \leq p^s \).
We start with the following proposition.

Proposition 3.1: Let \( 0 \leq v \leq u \leq j \leq i \leq p^s \). Let \( \tilde{C} = (\bar{g}(x)) \) be a cyclic code of length 6 over \( \mathbb{F}_{p^m} \), where \( \bar{g}(x) \) is defined in (1). Then
\[
d_H(\tilde{C}) = \begin{cases} 
1, & \text{if } v \leq u \leq j \leq i \leq z, \\
1, & \text{if } v \leq u \leq j \leq \tilde{z} < i, \\
(\bar{x}^2 + x + 1)(\bar{x}^2 - x + 1), & \text{if } v \leq u \leq \tilde{z} < j \leq i, \\
(\bar{x}^5 - \bar{x}^4 + \bar{x}^3 - \bar{x}^2 + x - 1), & \text{if } v \leq \tilde{z} < u \leq j \leq i.
\end{cases}
\]

Proof: There are 4 possibilities.

Case 1: \( v \leq u \leq j \leq \tilde{z} \leq i \). In this case, clearly, \( \tilde{C} = \langle 1 \rangle \).
Then \( d_H(\tilde{C}) = 1 \).
Case 2: $v \leq u \leq j < z < i$. In this case, $\tilde{C}_z = (x^2 + x + 1)$, obviously, $(x^2 + x + 1)(x - 1) = (x^3 - 1) \in \tilde{C}_z$ and $\text{wt}_H(x^3 - 1) = 2$. Hence, by Lemma 2.1, $d_H(\tilde{C}_z) = 2$.

Case 3: $v \leq u \leq z < j < i$. In this case, we have $\tilde{C}_z = ((x^2 + x + 1)(x^2 - x + 1)) = (x^3 + x^2 + 1)$, and then exists a polynomial $x^j - a \in \mathbb{F}_p[x]$ such that $x^j - a = (x^j - 1)$, where $a \in \mathbb{F}_p$. By the Division Algorithm, we can assume $l < 6$. Let $\zeta$ be a 6th root of unity, then $\zeta$ and $\zeta^2$ are solutions of $x^4 + x^2 + 1 = 0$. It follows that $\zeta$ and $\zeta^2$ are solutions of $x^i - a$, i.e., $\zeta^i = 1$, which is contradictory to $l < 6$. So, $d_H(\tilde{C}_z) = 3$.

Case 4: $v \leq z < u \leq j < i$. In this case, it is easy to get $\tilde{C}_z = ((x^3 + x + 1)(x^3 - x + 1)(x + 1)) = (x^3 + x^2 + 1)$, and therefore, the elements of $\tilde{C}_z$ are precisely $r(x^5 + x^4 + x^3 + x^2 + 1)$, where $r \in \mathbb{F}_p^*$. So, $d_H(\tilde{C}_z) = 6$.

Combining all the cases, the result follows.

We here state the Hamming distance of $C$ for the case $v = 0$.

**Lemma 3.2:** Let $v = 0$ and $0 \leq u \leq j < i \leq p^s$ be integers. Then,

$$d_H(C) = \begin{align*}
1, & \quad \text{if } i = j = u = 0, \\
2, & \quad \text{if } j = u = 0 \text{ and } 0 < i \leq p^s, \\
& \quad \text{or } 0 \leq u \leq j \leq i \leq p^{s-1} \text{ (but not } i = j = u = 0), \\
3, & \quad \text{if } u = 0, 0 < j \leq p^s \text{ and } p^{s-1} < i \leq p^s, \\
& \quad \text{or } 0 < u \leq j \leq p^{s-1} \text{ and } p^{s-1} < i \leq 2p^{s-1}, \\
4, & \quad \text{if } 0 < u \leq j \leq 3p^{s-1} \text{ and } 2p^{s-1} < i \leq 3p^{s-1}, \\
& \quad \text{or } 0 < u \leq j \leq p^{s-1} \text{ and } 2p^{s-1} < i \leq p^s, \\
5, & \quad \text{if } 0 < u \leq 4p^{s-1} \text{ and } p^{s-1} < i \leq 4p^{s-1}, \\
& \quad \text{and } 3p^{s-1} < i \leq 4p^{s-1}, \\
6, & \quad \text{if } 0 < u \leq p^s, p^{s-1} < j < p^s \text{ and } 4p^{s-1} < i \leq p^s.
\end{align*}$$

**Proof:** By Proposition 2.2 and Proposition 3.1, we have

$$d_H(C) = \min_{0 \leq u \leq j < i \leq p^s} \text{wt}_H((x^6 - 1)^0) \cdot d_H(\tilde{C}_z) \mid 0 \leq z \leq p^s - 1 \} \leq \text{wt}_H((x^6 - 1)^0) \cdot d_H(\tilde{C}_z) \leq 6.$$

So, $d_H(C) = 1, 2, 3, 4, 5$, or 6. Thus, we only need to find out what values of $v$, $i$, $j$, $u$ such that $d_H(C) = 1, 2, 3, 4, 5$ or 6 (the remaining values of $v$, $i$, $j$, $u$ will give $d_H(C) = 6$) we consider 2 cases.

**Case 1:** $v = 0$. In this case, by Proposition 3.1, we have

$$\text{wt}_H((x^6 - 1)^0) \cdot d_H(\tilde{C}_z) = \begin{align*}
1, & \quad \text{if } i = j = u = 0, \\
2, & \quad \text{if } j = u = 0 \text{ and } 0 < i \leq p^s, \\
3, & \quad \text{if } u = 0 \text{ and } 0 < j \leq i \leq p^s,
\end{align*}$$

and $\text{wt}_H((x^6 - 1)^0) \cdot d_H(\tilde{C}_z) = 6$ for the other values of $i, j, u$.

**Case 2:** $1 \leq z \leq p^s - 1$. There are 4 possibilities.

**Case 2.1:** $u \leq j \leq i \leq z$. From Proposition 3.1, we get $d_H(\tilde{C}_z) = 1$. By Lemma 2.4, we obtain

$$\min_{0 \leq u \leq j < i \leq p^s} \text{wt}_H((x^6 - 1)^0) \cdot d_H(\tilde{C}_z) \mid 1 \leq z \leq p^s - 1 \} = 4,$$

and

$$\min_{0 \leq u \leq j < i \leq p^s} \text{wt}_H((x^6 - 1)^0) \cdot d_H(\tilde{C}_z) \mid 1 \leq z \leq p^s - 1 \} = 4,$$

$$\min_{0 \leq u \leq j < i \leq p^s} \text{wt}_H((x^6 - 1)^0) \cdot d_H(\tilde{C}_z) \mid 1 \leq z \leq p^s - 1 \} = 4.$$
Then \(d_{H}(C) = \min\{0, 2s, 2(2s+2)p^{2s}, 3(2s+2)p^{2s}, 6(3s+2)p^{2s}\}. \quad \square

By similar arguments as Lemma 3.2, we obtain the following lemmas immediately.

**Lemma 3.4:** Let \(i = p^d, v \leq u \leq j \) be integers such that
\[
p^d - p^{d-1} + \beta_1 p^{d-1} + 1 \leq j \leq p^d - p^{d-1} + (\beta_1 + 1)p^{d-1},
\]
\[
p^d - p^{d-2} + \beta_2 p^{d-2} + 1 \leq u \leq p^d - p^{d-2} + (\beta_2 + 1)p^{d-2},
\]
\[
p^d - p^{d-3} + \beta_3 p^{d-3} + 1 \leq v \leq p^d - p^{d-3} + (\beta_3 + 1)p^{d-3}.
\]
Then \(d_{H}(C) = \min\{2(\beta_1 + 1)p^{2s}, 3(2s+2)p^{2s}, 6(3s+2)p^{2s}\}. \quad \square

**Lemma 3.5:** Let \(i = j = p^d, v \leq u \leq j \) be integers such that
\[
p^d - p^{d-1} + \beta_1 p^{d-1} + 1 \leq j \leq p^d - p^{d-1} + (\beta_1 + 1)p^{d-1},
\]
\[
p^d - p^{d-2} + \beta_2 p^{d-2} + 1 \leq u \leq p^d - p^{d-2} + (\beta_2 + 1)p^{d-2},
\]
\[
p^d - p^{d-3} + \beta_3 p^{d-3} + 1 \leq v \leq p^d - p^{d-3} + (\beta_3 + 1)p^{d-3}.
\]
Then \(d_{H}(C) = \min\{2s+2)p^{2s}, 3(2s+2)p^{2s}, 6(3s+2)p^{2s}\}. \quad \square

**Lemma 3.6:** Let \(i = j = u = p^s, v \leq u \) be an integer such that
\[
p^{s} - p^{s-1} + \beta_1 p^{s-1} + 1 \leq j \leq p^{s} - p^{s-1} + (\beta_1 + 1)p^{s-1},
\]
\[
p^{s} - p^{s-2} + \beta_2 p^{s-2} + 1 \leq u \leq p^{s} - p^{s-2} + (\beta_2 + 1)p^{s-2},
\]
\[
p^{s} - p^{s-3} + \beta_3 p^{s-3} + 1 \leq v \leq p^{s} - p^{s-3} + (\beta_3 + 1)p^{s-3}.
\]
Then \(d_{H}(C) = 6(3s+2)p^{2s}. \quad \square

Remark 3.8: Using the above technique, it is easy to check that the corresponding cases \(0 \leq v \leq u \leq j \leq i \leq p^s, 0 \leq v \leq u \leq i \leq j \leq p^s, 0 \leq u \leq v \leq i \leq j \leq p^s, 0 \leq v \leq u \leq j \leq \leq i \leq p^s \) in Theorem 3.7. For example, in case \(v \leq u \leq i \leq j \leq p^s, \) if \(i = j = v = p^s \) and \( p^s - p^{s-2} + \beta_3 p^{s-2} + 1 \leq u \leq p^{s} - p^{s-3} + (\beta_3 + 1)p^{s-3}. \)
$p^r - p^{r-t_0} + (\beta_3 + 1)p^{s-t_0-1}$, the Hamming distance $d_H(C)$ is $6(\beta_3 + 2)p^3$.

**Example 3.9:** Let $p = 5$, $s = i = j = 1$ and $u = v = 0$, then $C$ is an [30, 26, 3] code by Theorem 3.7, which is optimal respect to the tables of best codes known maintained at http://www.codetables.de.

### 3.2. Case 2: $0 \leq j \leq i \leq v \leq u \leq p^r$

We here determine the Hamming distance of $C = \langle x^2 + x + 1 \rangle(x^2 - x + 1)(x - 1)^6(x + 1)^3$ for the case $0 \leq j \leq i \leq v \leq u \leq p^r$. Using the similar way as we show the Hamming distance of $C$ for the case $0 \leq v \leq u \leq j \leq i \leq p^r$, we first determine the Hamming distance of $\tilde{C}_i$, for the case $0 \leq j \leq i \leq v \leq u \leq p^r$.

**Proposition 3.10:** Let $0 \leq j \leq i \leq v \leq u \leq p^r$. Let $\tilde{C}_i = (\tilde{g}_i(x))$ be a cyclic code of length 6 over $\mathbb{F}_{p^r}$, where $\tilde{g}_i(x)$ is defined in (1). Then

$$d_H(\tilde{C}_i) = \begin{cases} 
1, & \text{if } j \leq i \leq v \leq u \leq z, \\
2, & \text{if } j \leq i \leq v < z < u, \\
3, & \text{if } j \leq i \leq z < v < u, \\
4, & \text{if } j \leq z < i \leq v < u.
\end{cases}$$

**Proof:** There are 4 possibilities.

**Case 1:** $j \leq i \leq v \leq u \leq z$. In this case, clearly, $\tilde{C}_i = \langle 1 \rangle$. Then $d_H(\tilde{C}_i) = 1$.

**Case 2:** $j \leq i \leq v < z < u$. In this case, obviously, $\tilde{C}_i = \langle x - 1 \rangle$. From Lemma 2.1, $d_H(\tilde{C}_i) = 2$.

**Case 3:** $j \leq i \leq z < v < u$. In this case, we have, $\tilde{C}_i = \langle x + 1 \rangle(x - 1)$. From Lemma 2.1, $d_H(\tilde{C}_i) = 2$.

**Case 4:** $j \leq z < i \leq v < u$. In this case, it is easy to get $\tilde{C}_i = \langle x - 1 \rangle(x + 1)(x^2 + x + 1) = \langle x^4 + x^3 - x - 1 \rangle$ and $w_H(x^4 + x^3 - x - 1) = 4$.

Let $c(x)$ be an arbitrary nonzero codeword in $\tilde{C}_i$, then $c(x)$ can be expressed as $c(x) = (ax^4 + bx^3 - (a + b)x - b) \in \mathbb{F}_{p^r}$, and $(a, b) \neq (0, 0)$. Obviously, $w_H(c(x)) \geq 4$, implying $d_H(\tilde{C}_i) = 4$.

Combining all the cases, the result follows. □

We now state the Hamming distance of $C$ for the case $0 \leq j \leq i \leq v \leq u \leq p^r$. Firstly, we consider the case for $j = 0$.

**Lemma 3.11:** Let $j = 0$ and $0 \leq i \leq v \leq u \leq p^r$ be integers. Then,

$$d_H(C) = \begin{cases} 
1, & \text{if } i = u = v = 0, \\
2, & \text{if } i = u = 0, \ 0 \leq v \leq p^r \text{ and } 0 < u < p^r, \\
3, & \text{if } 0 < i \leq v \leq u \leq p^r \text{ (but not } i = u = v = 0), \\
4, & \text{if } 0 < i \leq v \leq p^r \text{ and } 2p^{s-1} < u \leq p^r.
\end{cases}$$

**Proof:** By Proposition 2.1 and Proposition 3.10, we have

$$d_H(C) = \min\{w_H((x^6 - 1)^3) \cdot d_H(\tilde{C}_i) | 0 \leq z \leq p^r - 1\} \leq w_H((x^6 - 1)^3) \cdot d_H(\tilde{C}_i) \leq 4.$$

So, $d_H(C) = 1, 2, 3$ or 4. Thus, we only need to find out what values of $i, u, v$ such that $d_H(C) = 1, 2$ or 3 (the remaining values of $i, u, v$ will give $d_H(C) = 4$). We consider 2 cases.

**Case 1:** $z = 0$. In this case, by Proposition 3.10, we have

$$w_H((x^6 - 1)^3) \cdot d_H(\tilde{C}_i) = \begin{cases} 
1, & \text{if } i = u = v = 0, \\
2, & \text{if } i = 0, 0 \leq v \leq p^r \text{ and } 0 < u \leq p^r,
\end{cases}$$

and $w_H((x^6 - 1)^3) \cdot d_H(\tilde{C}_i) = 4$ for the other values of $i, u, v$.

**Case 2:** $1 \leq z \leq p^r - 1$. There are 4 possibilities.

**Case 2.1:** $i \leq v < z < u$. From Proposition 3.10, we get $d_H(\tilde{C}_i) = 1$. By Lemma 2.4, we obtain

$$\min\{w_H((x^6 - 1)^3) \cdot d_H(\tilde{C}_i) | 0 < z < p^r - 1\} = 2,$$

and $\min\{w_H((x^6 - 1)^3) \cdot d_H(\tilde{C}_i) | p^r - 1 < z \leq 2p^{s-1}\} = 3$.

**Case 2.2:** $i \leq v < z < u$. From Proposition 3.10, clearly, $d_H(\tilde{C}_i) = 2$. By Lemma 2.4, we have $w_H((x^6 - 1)^3) \cdot d_H(\tilde{C}_i) \geq 2 w_H((x^6 - 1)^3) \geq 4$ for $1 \leq z \leq p^r - 1$.

**Case 2.3:** $i \leq z < v < u$. From Proposition 3.10, obviously, $d_H(\tilde{C}_i) = 2$. By Lemma 2.4, we have $w_H((x^6 - 1)^3) \cdot d_H(\tilde{C}_i) \geq 2 w_H((x^6 - 1)^3) \geq 4$ for $1 \leq z \leq p^r - 1$.

**Case 2.4:** $z < i \leq v < u$. From Proposition 3.10, clearly, $d_H(\tilde{C}_i) = 4$. By Lemma 2.4, we have $w_H((x^6 - 1)^3) \cdot d_H(\tilde{C}_i) \geq 4 w_H((x^6 - 1)^3) \geq 8$ for $1 \leq z \leq p^r - 1$.

Therefore, combining with **Case 2.1**, **Case 2.2**, **Case 2.3** and **Case 2.4**, we get

$$\min\{w_H((x^6 - 1)^3) \cdot d_H(\tilde{C}_i) | 1 \leq z \leq p^r - 1\} = \begin{cases} 
2, & \text{if } 0 \leq i \leq v \leq u \leq p^r - 1, \\
3, & \text{if } 0 \leq i \leq v < u \leq 2p^{s-1},
\end{cases}$$

and $w_H((x^6 - 1)^3) \cdot d_H(\tilde{C}_i) \geq 4$ for the other values of $i, u, v$.

Combining with Proposition 2.2, (4) and (5), the result follows. □

In the following, we consider the Hamming distance of $C$ for the case $j > 0$. Recall that $0 \leq \beta_0, \beta_1, \beta_2, \beta_3 \leq p - 2$, and $0 \leq t_1 \leq t_2 \leq t_3 \leq t_4 \leq s - 1$.

**Lemma 3.12:** Let $0 < j \leq i \leq v \leq u \leq p^r - 1$ be integers such that

$$p^r - p^{r-t_0} + \beta_0 p^{r-t_0-1} + 1 \leq u \leq p^r - p^{r-t_0} + (\beta_0 + 1)p^{s-t_0-1},$$

$$p^r - p^{r-t_1} + \beta_1 p^{r-t_1-1} + 1 \leq v \leq p^r - p^{r-t_1} + (\beta_1 + 1)p^{s-t_1-1},$$

$$p^r - p^{r-t_2} + \beta_2 p^{r-t_2-1} + 1 \leq i \leq p^r - p^{r-t_2} + (\beta_2 + 1)p^{s-t_2-1},$$

$$p^r - p^{r-t_3} + \beta_3 p^{r-t_3-1} + 1 \leq j \leq p^r - p^{r-t_3} + (\beta_3 + 1)p^{s-t_3-1}.$$
2)p^{3_j}, 4(\beta_3 + 2)p^{3_k}). As \(v \geq i\), one can verify that \(\tau_1 > \tau_2\), or \(\tau_1 = \tau_2\) and \(\beta_1 \leq \beta_2\). This means that \(2(\beta_1 + 2)p^{3_j} \geq 2(\beta_2 + 2)p^{3_k}\). Therefore, \(d_H(C) = \min((\beta_0 + 2)p^{3_0}, 2(\beta_2 + 2)p^{3_2}, 4(\beta_3 + 2)p^{3_3})\). □

Using the same arguments as Lemma 3.2 and Lemma 3.3, we can get the Hamming distance of \(C\) for the case \(0 < j \leq i \leq v \leq u \leq p^s\). We here omit the proof. The Hamming distance of \(C\) for the case \(0 \leq j \leq i \leq v \leq u \leq p^s\) is shown as follows.

**Theorem 3.13:** Let \(0 \leq \beta_0, \beta_1, \beta_2, \beta_3 \leq p - 2\), and \(0 \leq \tau_3 \leq \tau_2 \leq \tau_1 \leq t_0 \leq s - 1\). Let \(0 \leq j \leq s \leq u \leq p^s\).

Then \(C = (x^2 + x + 1)^{(x^2 - x + 1)(x - 1)^u(x + 1)^{A}}(x)\) is a \([6p^s, 6p^s - 2i - 2j - u - v]_0\) code with Hamming distance:

\[
d_H(C) = \begin{cases} 
1, & \text{if } i = j = v = u = 0, \\
2, & \text{if } i = j = 0, 0 \leq v \leq p^s \text{ and } 0 < u \leq p^s, \\
& \text{or } j = 0 \text{ and } 0 \leq i \leq v \leq u \leq p^s - 1 \\
& \text{but not } i = u = v = 0, \\
3, & \text{if } j = 0, 0 < i \leq v \leq 2p^{s-1} \\
& \text{and } p^{s-1} < u \leq 2p^{s-1}, \\
4, & \text{if } j = 0, 0 < i \leq v \leq p^s \\
& \text{and } 2p^{s-1} < u \leq p^s, \\
\min((\beta_0 + 2)p^{3_0}, & \text{if } p^{s-1} - p^{s-1} + \beta_0 p^{s-1} - 1 \leq u \leq p^s, \\
-\beta^{3_0} + (\beta_1 + 1)p^{3_1}, & \text{if } p^{s-1} - p^{s-1} + \beta_1 p^{s-1} - 1 \leq v \leq p^s \\
-\beta^{3_1} + (\beta_2 + 1)p^{3_2}, & \text{if } p^{s-1} - p^{s-1} + \beta_2 p^{s-1} - 1 \leq i \leq p^s \\
-\beta^{3_2} + (\beta_3 + 1)p^{3_3}, & \text{if } p^{s-1} - p^{s-1} + \beta_3 p^{s-1} - 1 \leq j \leq p^s \\
\end{cases}
\]

**Remark 3.14:** Using the above technique, it is easy to check that the corresponding cases \(0 \leq i \leq j \leq u \leq v \leq p^s\), \(0 \leq i \leq u \leq j \leq v \leq p^s\), \(0 \leq j \leq i \leq v \leq u \leq p^s\), \(0 \leq j \leq i \leq u \leq v \leq p^s\), \(0 \leq i \leq u \leq v \leq p^s\), and \(0 \leq j \leq v \leq u \leq i \leq p^s\) have the same Hamming distance as the case \(0 \leq j \leq i \leq v \leq u \leq p^s\) in Theorem 3.13. For example, in case \(0 \leq i \leq j \leq u \leq v \leq p^s\),

\[
d_H(C) = \min\{w_{H}(x^6 - 1)^v \cdot d_H(C_0) \mid 0 \leq z \leq p^s - 1\} \leq w_{H}(x^6 - 1)^v \cdot d_H(C_0) \leq 6.
\]

**Example 3.15:** Let \(p = 5\), \(j = 0\), \(s = i = v = 1\) and \(u = 3\), then \(C\) is an \([30, 24, 4]\) code by Theorem 3.13, which is almost optimal respect to the tables of best codes known maintained at http://www.codetables.de.

**3.3. Case 3:** \(0 \leq v \leq j \leq u \leq i \leq p^s\)

We here determine the Hamming distance of \(C = ((x^2 + x + 1)(x^2 - x + 1)(x - 1)^u(x + 1)^{A})\) for the case \(0 \leq v \leq j \leq u \leq i \leq p^s\). Using the similar way as we show the Hamming distance of \(C\) for the case \(0 \leq v \leq u \leq j \leq i \leq p^s\), we first determine the Hamming distance of \(C_0\) for the case \(0 \leq v \leq j \leq u \leq i \leq p^s\).

**Proposition 3.16:** Let \(0 \leq v \leq j \leq u \leq i \leq p^s\). Let \(C_0 = (\bar{g}_C(x))\) be a cyclic code of length \(6\) over \(\mathbb{F}_{p^s}\), where \(\bar{g}_C(x)\) is defined in (1). Then

\[
d_H(C_0) = \begin{cases} 
1, & \text{if } v \leq j \leq u \leq i \leq z, \\
2, & \text{if } v \leq j \leq u \leq z < i, \\
& \text{or } j \leq v \leq z < u \leq i, \\
6, & \text{if } v \leq z < j \leq u \leq i.
\end{cases}
\]

**Proof:** There are 4 possibilities.

**Case 1:** \(v \leq j \leq u \leq i \leq z\). In this case, clearly, \(C_0 = (1)\). Then \(d_H(C_0) = 1\).

**Case 2:** \(v \leq j \leq u \leq z \leq i\). In this case, \(C_0 = (x^2 + x + 1)\).

Obviously, \((x^2 + x + 1)(x - 1) = (x^3 - 1)\). Thus, \(C_0 = (x^3 - 1)\). From Lemma 2.1, \(d_H(C_0) = 2\).

**Case 3:** \(v \leq j \leq z \leq u \leq i\). In this case, we have, \(C_0 = ((x^2 + x + 1)(x - 1)) = (x^3 - 1)\). From Lemma 2.1, \(d_H(C_0) = 2\).

**Case 4:** \(v \leq z \leq j \leq u \leq i\). From the Proposition 3.1 of Case 4, we have \(d_H(C_0) = 6\).

Combining all the cases, the result follows. □

We here state the Hamming distance of \(C\) for the case \(v = 0\).

**Lemma 3.17:** Let \(v = 0\) and \(0 \leq j \leq u \leq i \leq p^s\). Then

\[
d_H(C) = \begin{cases} 
1, & \text{if } i = j = u = 0, \\
2, & \text{if } j = 0, 0 \leq u \leq p^s \text{ and } 0 < i \leq p^s, \\
& \text{or } 0 \leq u \leq j < i \leq p^{s-1} \text{ (but not } i = j = u = 0), \\
3, & \text{if } 0 < j \leq u \leq 2p^{s-1} \text{ and } 2p^{s-1} < i \leq 2p^{s-1}, \\
4, & \text{if } 0 < j \leq u \leq 2p^{s-1} \text{ and } 2p^{s-1} < i \leq 3p^{s-1}, \\
& \text{or } 0 < i \leq p^{s-1} \text{ and } 0 < u \leq p^s \text{ and } p^{s-1} < i \leq p^s, \\
5, & \text{if } p^{s-1} < i \leq u \leq 4p^{s-1} \text{ and } 3p^{s-1} < i \leq 4p^{s-1}, \\
6, & \text{if } p^{s-1} < i \leq u \leq p^s \text{ and } 4p^{s-1} < i \leq p^s.
\end{cases}
\]

**Proof:** By Proposition 2.2 and Proposition 3.16, we have

\[
d_H(C) = \min\{w_{H}(x^6 - 1)^v \cdot d_H(C_0) \mid 0 \leq z \leq p^s - 1\} \leq w_{H}(x^6 - 1)^v \cdot d_H(C_0) \leq 6.
\]
So, \(d_H(C) = 1, 2, 3, 4, 5 \text{ or } 6\). Thus, we only need to find out what values of \(i, j, u\) such that \(d_H(C) = 1, 2, 3, 4 \text{ or } 5\) (the remaining values of \(i, j, u\) will give \(d_H(C) = 6\)). We consider 2 cases.

**Case 1:** \(z = 0\). In this case, by Proposition 3.16, we have

\[
wt_H((x^6 - 1)^0) \cdot d_H(C_0) = \begin{cases} 
1, & \text{if } i = j = u = 0, \\
2, & \text{if } j = 0, 0 \leq u \leq p^s \text{ and } 0 < i \leq p^s, 
\end{cases} 
\]

and \(wt_H((x^6 - 1^0) \cdot d_H(C_0) = 6\) for the other values of \(i, j, u\).

**Case 2:** \(1 \leq z \leq p^s - 1\). There are 4 possibilities.

**Case 2.1:** \(j \leq u \leq i \leq z\). From Proposition 3.16, we get \(d_H(C_z) = 1\). By Lemma 2.4, we obtain

\[
\text{min}(wt_H((x^6 - 1)^2) \cdot d_H(C_0)) \leq (t - 2)p^{s - 1} < z \leq (t - 1)p^{s - 1} = t, 
\]

and

\[
\text{min}(wt_H((x^6 - 1)^2) \cdot d_H(C_z) | 4p^{s - 1} < z \leq p^s - 1) \geq 6, 
\]

where \(t = 2, 3, 4, 5\).

**Case 2.2:** \(j \leq u \leq z < i\), or \(j \leq z < u \leq i\). From Proposition 3.16, clearly, \(d_H(C_z) = 2\). By Lemma 2.4, we have

\[
\text{min}(wt_H((x^6 - 1)^2) \cdot d_H(C_z) | 1 \leq z \leq p^s - 1) = 4, 
\]

and

\[
\text{min}(wt_H((x^6 - 1)^2) \cdot d_H(C_z) | p^s - 1 < z \leq p^s - 1) \geq 6. 
\]

**Case 2.3:** \(z < j < u \leq i\). From Proposition 3.16, obviously, \(d_H(C_z) = 6\). By Lemma 2.4, we have

\[
wt_H((x^6 - 1)^2) \cdot d_H(C_z) \geq 6 \text{ wt}_H((x^6 - 1)^2) \geq 12 \text{ for } 1 \leq z \leq p^s - 1. 
\]

Therefore, combining with **Case 2.1**, **Case 2.2** and **Case 2.3**, we get

\[
\text{min}(wt_H((x^6 - 1)^2) \cdot d_H(C_z) | 1 \leq z \leq p^s - 1) = 
\begin{cases} 
2, & \text{if } 0 \leq j \leq u \leq i \leq p^s - 1, \\
3, & \text{if } 0 \leq j \leq u \leq 2p^{s - 1} \text{ and } p^s - 1 < i \leq 2p^{s - 1}, \\
4, & \text{if } 0 \leq j \leq u \leq 3p^{s - 1} \text{ and } 2p^{s - 1} < i \leq 3p^{s - 1}, \\
\quad \text{or } 0 \leq j \leq p^{s - 1}, 0 \leq u \leq p^s \text{ and } 2p^{s - 1} < i \leq p^s, \\
5, & \text{if } p^s - 1 < j \leq u \leq 4p^{s - 1} \text{ and } 3p^{s - 1} < i \leq 4p^{s - 1}, 
\end{cases} 
\]

and \(wt_H((x^6 - 1)^2) \cdot d_H(C_z) = 6\) for the other values of \(i, j, u\).

Combining with Proposition 2.2, (6) and (7), the result follows.

By the similar arguments as we determine the Hamming distance of \(C\) for the case \(0 \leq v \leq u \leq j \leq i \leq p^s\). Combining with Proposition 3.16 and Lemma 3.17, we show the Hamming distance of \(C\) for the case \(0 \leq v \leq j \leq u \leq i \leq p^s\), immediately.

**Theorem 3.18:** Let \(0 \leq \beta_0, \beta_1, \beta_2, \beta_3 \leq p - 2\), and \(0 \leq \tau_3 \leq \tau_2 \leq \tau_1 \leq \tau_0 \leq s - 1\). Let \(0 \leq v \leq j \leq u \leq i \leq p^s\). Then \(C = \langle x^2 + x + 1 \rangle((x^2 - x + 1)(x - 1)^s(x + 1)^s)\) is a \(6p^s, 6p^s - 2i - 2j - u - v\) code with Hamming distance:

\[
d_H(C) = \begin{cases} 
1, & \text{if } i = j = u = v = 0, \\
2, & \text{if } j = v = 0, 0 \leq u \leq p^s \text{ and } 0 < i \leq p^s, \\
\quad \text{or } v = 0 \text{ and } 0 \leq u \leq j \leq i \leq p^{s - 1} \text{ (but not } i = j = k = 0), \\
3, & \text{if } v = 0, 0 < j \leq u \leq 2p^{s - 1}, \text{ and } p^{s - 1} < i \leq p^{s - 1}, \\
4, & \text{if } v = 0, 0 < j \leq u \leq 2p^{s - 1}, \text{ and } p^{s - 1} < i \leq 3p^{s - 1}, \\
\quad \text{or } v = 0, 0 < j \leq p^{s - 1}, \\
0 \leq u \leq p^s \text{ and } p^{s - 1} < i \leq p^s, \\
5, & \text{if } v = 0, p^{s - 1} < j \leq u \leq 4p^{s - 1}, \text{ and } 3p^{s - 1} < i \leq 4p^{s - 1}, \\
6, & \text{if } v = 0, p^{s - 1} < j \leq u \leq p^s, \text{ and } 4p^{s - 1} < i \leq p^s, \\
\quad \text{min}(\beta_0 + 2p^{s - 1}), \\
\quad \text{min}(\beta_0 + 2p^{s - 1} + \beta_0 p^{s - 1} + 1 \leq i \leq p^{s - 1}), \\
2(\beta_2 + 2p^{s - 1}), \\
6(\beta_3 + 2p^{s - 1}), \\
6(\beta_3 + 3p^{s - 1}), \\
6(\beta_3 + 2p^{s - 1}), \\
6(\beta_3 + 3p^{s - 1}), \\
\quad \text{if } i = v = 0, \\
6(\beta_3 + 2p^{s - 1}), \\
\quad \text{if } i = j = u = v = 0, \\
6(\beta_3 + 2p^{s - 1}), \\
\quad \text{if } i = j = u = v = 0, \\
6(\beta_3 + 2p^{s - 1}), \\
6(\beta_3 + 2p^{s - 1}), \\
6(\beta_3 + 2p^{s - 1}), \\
\quad \text{if } i = j = u = v = 0, \\
0, & \text{if } i = j = u = v = 0. 
\end{cases} 
\]

**Remark 3.19:** Using the above technique, it is easy to check that the corresponding cases \(0 \leq v \leq j \leq i \leq u \leq p^s, 0 \leq u \leq i \leq v \leq j \leq p^s, \text{ and } 0 \leq v \leq j \leq u \leq i \leq p^s\) have the same Hamming distance as the case \(0 \leq i \leq u \leq j \leq v \leq p^s\) in Theorem 3.18. For example, in case \(0 \leq v \leq j \leq i \leq u \leq p^s\), if \(i = j = u = p^s\) and \(p^s - p^{s - 1} + \beta_0 p^{s - 1} + 1 \leq v \leq p^s - p^{s - 1} + (\beta_3 + 1)p^{s - 1} - 1\), the Hamming distance \(d_H(C)\) is \(6(\beta_3 + 2)p^{s - 1}\).
Example 3.20: Let \( p = 5, v = 0, s = u = j = 1 \) and \( i = 3 \), then \( \mathcal{C} \) is an \([30, 19, 5]\) code by Theorem 3.18.

3.4. Case 4: \( 0 \leq j \leq u \leq v \leq i \leq p^s \)

We now determine the Hamming distance of \( \mathcal{C} = \langle x^2 + x + 1 \rangle^s \langle x^2 - x + 1 \rangle^s \langle x^2 + 1 \rangle^s \langle x^2 + 1 \rangle^s \) for the case \( 0 \leq j \leq u \leq v \leq i \leq p^s \). Using the similar way as we show the Hamming distance of \( \mathcal{C} \) for the case \( 0 \leq v \leq u \leq j \leq i \leq p^s \), we first determine the Hamming distance of \( \bar{C}_z \) for the case \( 0 \leq j \leq u \leq v \leq i \leq p^s \).

Proposition 3.21: Let \( 0 \leq j \leq u \leq v \leq i \leq p^s \). Let \( \bar{C}_z = \langle g_z(x) \rangle \) be a cyclic code of length 6 over \( \mathbb{F}_{p^s} \), where \( g_z(x) \) is defined in (1). Then

\[
d_H(\bar{C}_z) = \begin{cases} 
1, & \text{if } j \leq u \leq v \leq i \leq z, \\
2, & \text{if } j \leq u \leq v \leq z < i, \\
4, & \text{if } j \leq u \leq z < v < i, \\
4, & \text{if } j \leq z < u \leq v \leq i.
\end{cases}
\]

Proof: There are 4 possibilities.

Case 1: \( j \leq u \leq v \leq z \leq i \). In this case, clearly, \( \bar{C}_z = \langle 1 \rangle \). Then \( d_H(\bar{C}_z) = 1 \).

Case 2: \( j \leq u \leq v < z \leq i \). In this case, \( \bar{C}_z = \langle x^2 + x + 1 \rangle \). Obviously, \( (x^2 + x + 1)(x - 1) = (x^3 - 1) \in \bar{C}_z \) and \( w_{th}(x^3 - 1) = 2 \). Hence, by Lemma 2.2, \( d_H(\bar{C}_z) = 2 \).

Case 3: \( j \leq u < z \leq v \leq i \). In this case, we have \( \bar{C}_z = \langle (x^2 + x + 1)(x + 1) \rangle \). Let \( (c(x) \) be an arbitrary nonzero codeword in \( \bar{C}_z \), then we consider the following 4 cases.

Case 3.1: \( c(x) = rx^i(x^2 + x + 1)(x + 1) \), where \( i = 0, 1 \) or 2, and \( r \in \mathbb{F}_{p^s}^* \). So obviously, \( w_{th}(c(x)) = 4 \).

Case 3.2: \( c(x) = (x^2 + x + 1)(x + 1)(bx + c) = bx^4 + (2b + c)x^3 + (2b + 2c)x^2 + (b + 2c)x + c \), where \( b, c \in \mathbb{F}_{p^s}^* \). Obviously, at most one of \( 2b + c, 2b + 2c \) and \( b + 2c \) is zero. Hence, \( w_{th}(c(x)) \geq 4 \).

Case 3.3: \( c(x) = (x^2 + x + 1)(x + 1)(ax^2 + c) = ax^5 + 2ax^4 + (a + 2c)x^3 + 2cx + c, \) where \( a, c \in \mathbb{F}_{p^s}^* \). Obviously, at most one of \( a + 2c \) and \( 2a + c \) is zero. Hence, \( w_{th}(c(x)) \geq 5 \).

Case 3.4: \( c(x) = (x^2 + x + 1)(x + 1)(ax^2 + bx + c) = ax^5 + (2a + b)x^4 + (2a + 2b + c)x^3 + (a + 2b + 2c)x^2 + (b + 2c)x + c, \) where \( a, b, c \in \mathbb{F}_{p^s}^* \). One can verify that at most two of \( 2a + b, 2a + 2b + c, a + 2b + 2c \) and \( b + 2c \) are zero. Hence, \( w_{th}(c(x)) \geq 4 \).

Therefore, in this case, \( d_H(\bar{C}_z) = 4 \).

Case 4: \( j \leq z < u \leq v \leq i \). By Case 4 of Proposition 3.10, we have \( d_H(\bar{C}_z) = 4 \).

Combining all the cases, the result follows. \( \square \)

We now compute the Hamming distance of \( \mathcal{C} \) for the case \( j = 0 \).

Lemma 3.22: Let \( j = 0 \) and \( 0 \leq u \leq v \leq i \leq p^s \) be integers. Then,

\[
d_H(\mathcal{C}) = \begin{cases} 
1, & \text{if } i = u = v = 0, \\
2, & \text{if } u = v = 0 \text{ and } i > 0, \text{ or } 0 \leq u \leq v \leq i \leq p^{s-1} \\
& \text{but not } i = u = v = 0, \\
3, & \text{if } 0 \leq u \leq 2p^{s-1}, 0 \leq v \leq 2p^{s-1} \text{ and } p^{s-1} < i \leq 2p^{s-1}, \\
4, & \text{if } 0 \leq u \leq p^s, 0 \leq v \leq p^s \text{ and } 2p^{s-1} < i \leq p^s.
\end{cases}
\]

Proof: By Proposition 2.2 and Proposition 3.21, we have

\[
d_H(\mathcal{C}) = \min\{w_{th}(x^6 - 1)^i \cdot d_H(\bar{C}_z) \mid 0 \leq z \leq p^s - 1 \}
\]

\[
\leq w_{th}(x^6 - 1)^i \cdot d_H(\bar{C}_0) \leq 4.
\]

So, \( d_H(\mathcal{C}) = 1, 2, 3 \) or 4. Thus, we only need to find out what values of \( i, u, v \) such that \( d_H(\mathcal{C}) = 1, 2 \) or 3 (the remaining values of \( i, u, v \) will give \( d_H(\mathcal{C}) = 4 \)). We consider 2 cases.

Case 1: \( z = 0 \). In this case, by Proposition 3.21, we have

\[
\begin{align*}
\text{Case 2.1: } u & \leq v \leq i \leq z. \text{ From Proposition 3.21, we get } d_H(\bar{C}_z) = 1. \text{ By Lemma 2.4, we obtain } \\
& \min\{w_{th}(x^6 - 1)^i \cdot d_H(\bar{C}_z) \mid 0 \leq z \leq p^{s-1} \} = 2, \\
& \min\{w_{th}(x^6 - 1)^i \cdot d_H(\bar{C}_z) \mid p^{s-1} < z \leq 2p^{s-1} \} = 3, \\
& \min\{w_{th}(x^6 - 1)^i \cdot d_H(\bar{C}_z) \mid 3p^{s-1} < z \leq p^s - 1 \} = 4.
\end{align*}
\]

Therefore, combining with Case 2.1, Case 2.2 and Case 2.3, we get

\[
\begin{align*}
\min\{w_{th}(x^6 - 1)^i \cdot d_H(\bar{C}_z) \mid 1 \leq z \leq p^s - 1 \} = \begin{cases} 
2, & \text{if } 0 \leq u \leq v \leq i \leq p^{s-1}, \\
3, & \text{if } 0 \leq u \leq v \leq 2p^{s-1} \text{ and } p^{s-1} < i \leq 2p^{s-1},
\end{cases}
\end{align*}
\]

and \( w_{th}(x^6 - 1)^i \cdot d_H(\bar{C}_z) \geq 4 \) for the other values of \( i, u, v \).
Combining with Proposition 2.2, (8) and (9), the result follows. □

Similar to the process as we compute the Hamming distance of $C$ for the case $0 \leq v \leq u \leq j \leq i \leq p^s$ and $0 \leq j \leq i \leq v \leq u \leq p^s$, combining with Proposition 3.21 and Lemma 3.22, we here summarize the Hamming distance $d_H(C)$ for the case $0 \leq j \leq u \leq v \leq i \leq p^s$.

**Theorem 3.23:** Let $0 \leq \beta_0, \beta_1, \beta_2, \beta_3 \leq p - 2$, and $0 \leq t_3 \leq t_2 \leq t_1 \leq t_0 \leq s - 1$. Let $0 \leq j \leq u \leq v \leq i \leq p^s$. Then $C = \langle (x^2 + x + 1)(x^2 - x + 1)(x - 1)^s(x + 1)^s \rangle$ is a $[6p^s, 6p^s - 2i - 2j - u - v]$ code with Hamming distance:

$$d_H(C) = \begin{cases} 
1, & \text{if } i = j = u = v = 0, \\
2, & \text{if } j = v = 0 \text{ and } 0 < i \leq p^s, \\
3, & \text{if } j = 0, 0 \leq u \leq 2p^{s-1}, 0 < v < 2p^{s-1} \text{ and } p^{s-1} < i < 2p^{s-1}, \\
4, & \text{if } j = 0, 0 \leq u \leq p^s, 0 < v < p^s \text{ and } 2p^{s-1} < i < p^s, \\
\min((\beta_0 + 2)p^{t_0}, 2(\beta_1 + 2)p^{t_1}, 4(\beta_3 + 2)p^{t_3}), & \text{if } p^s - p^{s-1} + \beta_0 p^{t_0} + 1 \leq i \leq p^s - p^{s-1} + (\beta_0 + 1)p^{t_0} - 1, \\
2(\beta_1 + 2)p^{t_1}, & \text{if } p^s - p^{s-1} + \beta_1 p^{t_1} + 1 \leq i \leq p^s - p^{s-1} + (\beta_1 + 1)p^{t_1} - 1, \\
4(\beta_3 + 2)p^{t_3}, & \text{if } p^s - p^{s-1} + \beta_3 p^{t_3} + 1 \leq i \leq p^s - p^{s-1} + (\beta_3 + 1)p^{t_3} - 1, \\
\end{cases}$$

Remark 3.24: Using the above technique, it is easy to check that the corresponding cases $0 \leq j \leq u \leq i \leq v \leq p^s$, $0 \leq i \leq v \leq j \leq u \leq p^s$, and $0 \leq j \leq v \leq u \leq j \leq p^s$ have the same Hamming distance as the case $0 \leq j \leq u \leq v \leq i \leq p^s$ in Theorem 3.23. For example, in case $0 \leq j \leq u \leq i \leq v \leq p^s$, if $i = u = v = p^s$ and $p^s - p^{s-1} + (\beta_3 + 1)p^{t_3} + 1 \leq j \leq p^s - p^{s-1} + (\beta_3 + 1)p^{t_3} + 1 + j \leq p^s - p^{s-1} + (\beta_3 + 1)p^{t_3}-1$, the Hamming distance $d_H(C)$ is $4(\beta_3 + 2)p^{t_3}$.

**Example 3.25:** Let $p = 5$, $j = u = 0$, $s = v = 1$ and $i = 2$, then $C$ is an $[30, 25, 3]$ code by Theorem 3.23, which is almost optimal with respect to the tables of best codes known maintained at http://www.codetables.de.

**3.5. Case 5:** $0 \leq u \leq j \leq v \leq i \leq p^s$

We now determine the Hamming distance of $C = \langle (x^2 + x + 1)(x^2 - x + 1)(x - 1)^s(x + 1)^s \rangle$ for the case $0 \leq u \leq j \leq v \leq i \leq p^s$. From Proposition 3.1 and Proposition 3.21, we get the following proposition, immediately.

**Proposition 3.26:** Let $0 \leq u \leq j \leq v \leq i \leq p^s$. Let $C = \langle \bar{C}_z(x) \rangle$ be a cyclic code of length 6 over $\mathbb{F}_{p^m}$, where $\bar{C}_z(x)$ is defined in (1). Then

$$d_H(C) = \begin{cases} 
1, & \text{if } u \leq j \leq v \leq i \leq z, \\
2, & \text{if } u \leq j \leq v \leq z < i, \\
3, & \text{if } u \leq j \leq z \leq v \leq i, \\
4, & \text{if } u \leq z < j \leq v \leq i, \\
5, & \text{if } u \leq z < j \leq v \leq i. \\
\end{cases}$$

We now compute the Hamming distance of $C$ for the case $u = 0$.

**Lemma 3.27:** Let $u = 0$ and $0 \leq j \leq v \leq i \leq p^s$ be integers. Then,

$$d_H(C) = \begin{cases} 
1, & \text{if } i = j = v = 0, \\
2, & \text{if } j = v = 0 \text{ and } 0 < i \leq p^s, \text{ or } 0 \leq j \leq v \leq i \leq p^{s-1}, \\
3, & \text{if } 0 \leq j \leq 2p^{s-1}, 0 < v < 2p^{s-1} \text{ and } p^{s-1} < i \leq 2p^{s-1}, \\
4, & \text{if } j = 0, 0 < v \leq p^s \text{ and } 2p^{s-1} < i \leq p^s, \\
5, & \text{if } 0 \leq j \leq 4p^{s-1}, \text{ or } 0 < j \leq 3p^{s-1}, \text{ and } 3p^{s-1} < i \leq 4p^{s-1}, \\
6, & \text{if } 0 \leq j < 4p^{s-1}, \text{ or } 0 < j \leq 4p^{s-1}, \text{ and } 4p^{s-1} < i \leq p^s. \\
\end{cases}$$

**Proof:** By Proposition 2.2 and Proposition 3.26, we have

$$d_H(C) = \min\{w_{H}(x^6 - 1)^2) \cdot d_H(\bar{C}_z) \mid 0 \leq z \leq p^s - 1\} \leq w_{H}(x^6 - 1)^2 \cdot d_H(\bar{C}_z) \leq 6.$$
Case 1: \( z = 0 \). In this case, by Proposition 3.26, we have
\[
\text{wt}_H((x^6 - 1)^0) \cdot d_H(\tilde{C}_0) = \begin{cases} 
1, & \text{if } i = j = v = 0, \\
2, & \text{if } j = v = 0 \text{ and } 0 < i \leq p^s, \\
4, & \text{if } j = 0, 0 < v \leq i \leq p^s, 
\end{cases}
\]
and \( \text{wt}_H((x^6 - 1)^0) \cdot d_H(\tilde{C}_0) = 6 \) for the other values of \( i, j, v \).

Case 2: \( 1 \leq z \leq p^s - 1 \). There are 4 possibilities.

Case 2.1: \( j \leq v \leq i \leq z \). From Proposition 3.26, we get \( d_H(\tilde{C}_z) = 1 \). By Lemma 2.4, we obtain
\[
\text{min}\{\text{wt}_H((x^6 - 1)^i) \cdot d_H(\tilde{C}_z) \mid (t-2)p^{s-1} < z \leq (t-1)p^{s-1}\} = t,
\]
and
\[
\text{min}\{\text{wt}_H((x^6 - 1)^i) \cdot d_H(\tilde{C}_z) \mid 4p^{s-1} < z \leq p^s - 1\} \geq 6,
\]
where \( t = 2, 3, 4, 5 \).

Case 2.2: \( j \leq v < z < i \). From Proposition 3.26, clearly, \( d_H(\tilde{C}_z) = 2 \). By Lemma 2.4, we have
\[
\text{min}\{\text{wt}_H((x^6 - 1)^i) \cdot d_H(\tilde{C}_z) \mid 1 \leq z \leq p^{s-1}\} = 4,
\]
and
\[
\text{min}\{\text{wt}_H((x^6 - 1)^i) \cdot d_H(\tilde{C}_z) \mid p^{s-1} < z \leq p^s - 1\} \geq 6.
\]

Case 2.3: \( j < z \leq v < i \). From Proposition 3.26, obviously, \( d_H(\tilde{C}_z) = 4 \). By Lemma 2.4, we have \( \text{wt}_H((x^6 - 1)^i) \cdot d_H(\tilde{C}_z) \geq 4 \) for \( 1 \leq z \leq p^s - 1 \).

Case 2.4: \( z < j \leq v \leq i \). From Proposition 3.26, we get \( d_H(\tilde{C}_z) = 6 \). By Lemma 2.4, we have \( \text{wt}_H((x^6 - 1)^i) \cdot d_H(\tilde{C}_z) \geq 6 \) for \( 1 \leq z \leq p^s - 1 \).

Therefore, combining with Case 2.1, Case 2.2, Case 2.3 and Case 2.4, we get
\[
\text{min}\{\text{wt}_H((x^6 - 1)^i) \cdot d_H(\tilde{C}_z) \mid 1 \leq z \leq p^{s-1}\} = \begin{cases} 
2, & \text{if } 0 \leq j \leq v \leq i \leq p^{s-1}, \\
3, & \text{if } 0 \leq j \leq v \leq 2p^{s-1} \text{ and } p^{s-1} < i \leq 2p^{s-1}, \\
4, & \text{if } 0 \leq j \leq v \leq 3p^{s-1} \text{ and } 2p^{s-1} < i \leq 3p^{s-1}, \text{ or} \\
\quad \text{or } 0 \leq j \leq p^{s-1}, 0 \leq v \leq p^{s-1} \text{ and } 2p^{s-1} < i \leq p^s, \\
5, & \text{if } 0 \leq j \leq 4p^{s-1}, p^{s-1} < v \leq 4p^{s-1} \text{ and } 3p^{s-1} < i \leq 4p^{s-1}, 
\end{cases}
\]
and \( \text{wt}_H((x^6 - 1)^i) \cdot d_H(\tilde{C}_z) \geq 6 \) for the other values of \( i, j, v \).

Combining with Proposition 2.2, (10) and (11), the result follows. \( \square \)

Using a similar way as we compute the Hamming distance of \( \mathcal{C} \) for the case \( 0 \leq v < u \leq j \leq i \leq p^s \) and \( 0 \leq j \leq i \leq v \leq u \leq p^s \), combining with Proposition 3.22 and Lemma 3.23, we here summarize the Hamming distance \( d_H(\mathcal{C}) \) for the case \( 0 \leq u \leq j \leq v \leq i \leq \leq p^s \).

Theorem 3.28: Let \( 0 \leq \beta_0, \beta_1, \beta_2, \beta_3 \leq p - 2 \), and \( 0 \leq r_3 \leq r_2 \leq r_1 \leq r_0 \leq s - 1 \). Let \( 0 \leq u \leq j \leq v \leq i \leq p^s \).

Then \( \mathcal{C} = \langle (x^2 + x + 1)^j(x^2 - x + 1)^{v}(x + 1)^{u} \rangle \) is a \([6p^s, 6p^s - 2i - 2j - u - v]\) code with Hamming distance:
\[
d_H(\mathcal{C}) = \begin{cases} 
1, & \text{if } i = j = u = v = 0, \\
2, & \text{if } j = u = v = 0 \text{ and } i > 0, \\
3, & \text{if } u = 0, 0 < j < 2p^{s-1}, 0 < v < 2p^{s-1} \text{ and } p^{s-1} < i \leq 2p^{s-1}, \\
4, & \text{if } j = u = 0, 0 < v < \leq 2p^{s-1} \text{ and } p^{s-1} < i \leq 2p^{s-1}, \\
5, & \text{if } u = 0, 0 < j < 4p^{s-1}, \text{ or } p^{s-1} < i \leq 4p^{s-1}, \\
6, & \text{if } u = 0, 0 < j < 4p^{s-1}, \text{ or } p^{s-1} < i \leq 4p^{s-1}, \\
0, & \text{if } i = j = u = v = 0.
\end{cases}
\]

Remark 3.29: Using the above technique, it is easy to check that the corresponding cases \( 0 \leq u \leq j \leq v \leq i \leq \leq p^s \) and \( 0 \leq v \leq i \leq j \leq u \leq p^s \) have the same Hamming distance as the case \( 0 \leq u \leq j \leq v \leq i \leq p^s \) in Theorem 3.28. For example, in case \( 0 \leq v \leq i \leq u \leq j \leq p^s \).
$p^i$, if $i=j=u=p^i$ and $p^i - p^s - t_3 + \beta_3 p^{s-t_3-1} + 1 \leq v \leq p^i - p^{s-t_3} + (\beta_3 + 1)p^{s-t_3-1}$, the Hamming distance $d_{H}(C)$ is $6(\beta_3 + 2)p^{3s}$.

Example 3.30: Let $p = 5$, $j = u = 0$, $s = v = 1$ and $i = 3$, then $C$ is an $[30, 23, 4]$ code by Theorem 3.28, which is almost optimal respect to the tables of best codes known maintained at http://www.codetables.de.

IV. MDS CYCLIC CODES OF LENGTH $6p^s$ OVER $\mathbb{F}_{pm}$

It is well known that constructing MDS codes is one of the central topics in coding theory. In this section, we use the determination of the Hamming distance of cyclic codes in Section 3, under the same hypothesis, $p^{m} \equiv 2 \pmod{3}$, to identify all MDS cyclic codes of length $6p^s$. We start with the case $0 \leq v \leq u \leq j \leq i \leq p^s$.

Theorem 4.1: Let $0 \leq v \leq u \leq j \leq i \leq p^s$ and $C$ be a code of length $6p^s$ with generator polynomial $g(x) = (x^2 + x + 1)^{(x^2 - x + 1)/(x^{p^s} - 1)}$. Then the code $C$ is an MDS code if and only if one of the following conditions holds:

- $i = j = u = v = 0$; in this case, $d_{H}(C) = 1$.
- $i = j = u = p^i$, and $v = p^i - 1$; in this case, $d_{H}(C) = 6p^s$.

Proof: As the generator polynomial of $C$ is $g(x) = (x^2 + x + 1)^{(x^2 - x + 1)/(x^{p^s} - 1)}$, then the dimension of code $C$ is $6p^s - 2i - 2j - u - v$. By Singleton bound, $C$ is an MDS code if and only if $6p^s - 2i - 2j - u - v = 6p^s - d_{H}(C) + 1$, i.e., $2i + 2j + u + v = d_{H}(C) - 1$.

The Hamming distance of $C$ has been given in Theorem 3.7, then we can consider the conditions for the equations hold from the following 11 cases.

**Case 1**: $i = j = u = v = 0$. Then $d_{H}(C) = 1$, obviously, $0 = d_{H}(C) - 1$.

**Case 2**: $j = u = v = 0$ and $0 < i \leq p^s$, or $v = 0$ and $0 \leq u \leq j \leq i \leq p^s - 1$ (but not $i = j = u = 0$). Then $d_{H}(C) = 2$. Obviously, $2i + 2j + u + v \geq 2 > d_{H}(C) - 1$.

**Case 3**: $u = v = 0$, $0 < j < p^s$ and $p^s - 1 \leq i \leq p^s$, or $v = 0$, $0 < u \leq j \leq 2p^s - 1$ and $p^s - 1 < i \leq 2p^s - 1$. Then $d_{H}(C) = 3$, and $2i + 2j + u + v > 3 > d_{H}(C) - 1$.

**Case 4**: $v = 0$, $0 < u \leq j \leq 3p^s - 1$ and $2p^s - 1 < i \leq 3p^s - 1$, or $v = 0$, $0 < u \leq j \leq p^s - 1$ and $p^s - 1 < i \leq p^s$. Then $d_{H}(C) = 4$, and $2i + 2j + u + v > 4 > d_{H}(C) - 1$.

**Case 5**: $v = 0$, $0 < u \leq 4p^s - 1$, $p^s - 1 < j \leq 4p^s - 1$ and $3p^s - 1 < i \leq 4p^s - 1$. Then $d_{H}(C) = 5$, and $2i + 2j + u + v > 5 > d_{H}(C) - 1$.

**Case 6**: $v = 0$, $0 < u \leq p^s$, $p^s - 1 < j \leq p^s$ and $4p^s - 1 < i \leq p^s$. Then $d_{H}(C) = 6$, and $2i + 2j + u + v > 6 > d_{H}(C) - 1$.

**Case 7**: $0 < v \leq u \leq j \leq i \leq p^s - 1$ are integers such that


d_{H}(C) = \min((\beta_0 + 2)p^{s}, 2(\beta_1 + 2)p^{s}, 3(\beta_2 + 2)p^{s}, 6(\beta_3 + 2)p^{s}),

\begin{align*}
2i + 2j + u + v & \geq 6p^s - 2p^{s-t_0} - 2p^{s-t_1} - p^{s-t_2} - p^{s-t_3} + 2\beta_0 p^{s-t_0-1} + 2\beta_1 p^{s-t_1-1} + 2\beta_2 p^{s-t_2-1} + 3\beta_3 p^{s-t_3-1} + 6
\end{align*}

(equality when $\beta_0 = \beta_1 = \beta_2 = \beta_3$ and $t_0 = t_1 = t_2 = t_3$).

We have the following results:

**Case 8**: $i = p^i, 0 < v \leq u \leq j \leq p^i - 1$ are integers such that


d_{H}(C) = \min(2(\beta_1 + 2)p^{s}, 3(\beta_2 + 2)p^{s}, 6(\beta_3 + 2)p^{s}),

\begin{align*}
2i + 2j + u + v & \geq 6p^s - 2p^{s-t_0} - 2p^{s-t_1} - p^{s-t_2} + 2\beta_1 p^{s-t_1-1} + 2\beta_2 p^{s-t_2-1} + 3\beta_3 p^{s-t_3-1} + 4
\end{align*}

(equality when $\beta_0 = \beta_1 = \beta_2 = \beta_3$ and $t_1 = t_2 = t_3$).

**Case 9**: $i = p^i, 0 < v \leq u \leq p^i - 1$ are integers such that


d_{H}(C) = \min(3(\beta_2 + 2)p^{s}, 6(\beta_3 + 2)p^{s}),

\begin{align*}
2i + 2j + u + v & \geq 6p^s - p^{s-t_0} - p^{s-t_1} - p^{s-t_2} + 2\beta_1 p^{s-t_1-1} + 3\beta_3 p^{s-t_3-1} + 2
\end{align*}

(equality when $\beta_2 = \beta_3 = \beta_0$ and $t_0 = t_1 = t_2 = t_3$).

There are no MDS codes.
\[ \geq 4p^4 + 2(\beta_2 + 2)(p^{r_2} - 1) + 2\beta_1 + 2 \]
\[ = 4p^4 + 2(\beta_2 + 2)p^{r_2} - 2 \]
\[ > 3(\beta_2 + 2)p^{r_2} - 1 \]
\[ \geq \min\{3(\beta_2 + 2)p^{r_2}, 6(\beta_3 + 2)p^{r_2}\} - 1 \]
\[ = d_H(C) - 1. \]

Therefore, there is no MDS code.

**Case 10:** \( i = j = u = p^s, 0 < v \leq p^s - 1 \) is an integer such that
\[ p^s - p^{s-r_3} + 3p^{s-r_3-1} + 1 \leq v \leq p^s - p^{s-r_3} + 3p^{s-r_3-1}. \]

Then \( d_H(C) = 6(\beta_3 + 2)p^{r_3}, \) and
\[ 2i + 2j + u + v \]
\[ \geq 6p^{r_3} - p^{s-r_3} + 3p^{s-r_3-1} + 1 \]
\[ = 6p^{r_3+1} - p + \beta_3 + 1 \quad (\text{equality when } r_3 = s - 1) \]
\[ = d_H(C) = 6p^{r_3}. \]

Therefore, \( 2i + 2j + u + v \geq 6p^{r_3} - p + \beta_3 + 1 \) with equality when \( p = \beta_3 + 2 \) and \( r_3 = s - 1 \) (in this case \( i = j = k = p^s, l = p^s - 1, \) i.e., \( \deg g(x) = 6p^s - 1, d_H(C) = 6p^s. \))

**Case 11:** \( i = u = v = p^s. \) Then \( d_H(C) = 0, \) obviously, \( 6p^s > d_H(C) - 1. \]

Using the same technique as above, combining the Hamming distance of cyclic codes of length \( 6p^s \) given in Section 3, we can determine the sufficient and necessary conditions for such codes to be MDS codes.

Here, we show the main steps for the proof and omit the details. Without losing the generality, we use the code \( C \) for \( 0 \leq j \leq i \leq v \leq u \leq p^s \) as an example.

**Proposition 4.2:** Procedure to obtain MDS codes among cyclic codes of length \( 6p^s \) of the form \( C \) for \( 0 \leq j \leq i \leq v \leq u \leq p^s. \)

**Step 1.** Using the same way as Theorem 4.1, by definition, one can verify that \( C \) is an MDS code if and only if \( 2i + 2j + u + v = d_H(C) - 1. \)

**Step 2.** For the trivial cases (\( d_H(C) = 0, 1, 2, 3, 4, \)) it is easy to check that there is no MDS code except for \( d_H(C) = 1, 2. \)

**Step 3.** For the non-trivial cases, we always let \( \tau_1 = s - 1 \) and \( \beta_2 = p - 2 \) in the proof, where \( 0 \leq i, j \leq 3. \) The details for the proof are similar to Case 7.

**Case 8, Case 9 and Case 10 of Theorem 4.1.** Then, we can get that there is no MDS code.

From above, the degrees of generator polynomials of all MDS cyclic codes of length \( 6p^s \) over \( \mathbb{F}_{p^m} \) can be shown as follows.

**Theorem 4.3:** Let \( C \) be a repeated-root cyclic code of length \( 6p^s \) with generator polynomial \( g(x) \). Then \( C \) is an MDS code if and only if
\[ \deg(g(x)) = 0; \text{ in this case, } d_H(C) = 1. \]
\[ \deg(g(x)) = 1; \text{ in this case, } d_H(C) = 2. \]
\[ \deg(g(x)) = 6p^s - 1; \text{ in this case, } d_H(C) = 6p^s. \]

**V. CONCLUSION**

In this paper, based on the relationship of the Hamming distances between simple-root cyclic codes and repeated-root cyclic codes, the Hamming distance of cyclic codes of length \( 6p^s \) are obtained for the case \( p^m \equiv 2 \pmod{3} \). Moreover, we determine all MDS cyclic codes of length \( 6p^s \) for the case \( p^m \equiv 2 \pmod{3} \).

When \( p^m \equiv 1 \pmod{3}, \) from [8], we know that all cyclic codes of length \( 6p^s \) have the form
\[ C = \left( (x - 1)^i (x + 1)^j (x - \xi p^{m-1})^k (x - \xi^{2p^{m-1}})^l \right) \times (x - \xi^{3p^{m-1}})^m (x - \xi^{4p^{m-1}})^n, \]
where \( 0 \leq i, j, k, l, m, n \leq p^s \) and \( \xi \in \mathbb{F}_{p^m} \) is a primitive \((p^m - 1)\)th root of unity. Our computation technique here can be used to determine the Hamming distances of all such cyclic codes.

**ACKNOWLEDGMENT**

The authors sincerely thank the reviewers and the editor for their helpful comments and valuable suggestions, which have greatly improved the presentation of this article.

**REFERENCES**

[1] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seemann, “On repeated-root cyclic codes,” IEEE Trans. Inf. Theory, vol. 37, no. 2, pp. 337–342, Mar. 1991.
[2] B. Chen, H. Q. Dinh, and H. Liu, “Repeated-root constacyclic codes of length \( (p^i) \) and their duals,” Discrete Appl. Math., vol. 177, pp. 60–70, Nov. 2014.
[3] B. Chen, H. Q. Dinh, and H. Liu, “Repeated-root constacyclic codes of length \( 2^m p^i \),” Finite Fields Appl., vol. 33, pp. 137–159, May 2015.
[4] H. Q. Dinh, “On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions,” Finite Fields Appl., vol. 14, no. 1, pp. 22–40, Jan. 2008.
[5] H. Q. Dinh, “Repeated-root constacyclic codes of length \( 2^m p^i \),” Finite Fields Appl., vol. 18, 2012, pp. 133–143.
[6] H. Q. Dinh, “Structure of repeated-root constacyclic codes of length \( 3p^i \) and their duals,” Discrete Math., vol. 313, no. 9, pp. 983–991, May 2013.
[7] H. Q. Dinh, “On repeated-root constacyclic codes of length \( 4p^i \),” Asian Eur. J. Math, vol. 6, pp. 1–25, Jun. 2013.
[8] H. Q. Dinh, “Structure of repeated-root cyclic codes and negacyclic codes of length \( 6p^s \) and their duals,” Contemp. Math., vol. 609, pp. 69–87, Feb. 2014.
[9] H. Q. Dinh, X. Wang, H. Liu, and S. Sriboonchitta, “On the Hamming distances of repeated-root constacyclic codes of length \( 4p^i \),” Discrete Math., vol. 342, pp. 1456–1470, May 2019.
[10] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[11] L. Liu, L. Q. Li, X. S. Kai, and S. X. Zhu, “Repeated-root constacyclic codes of length \( 3p^i \) and their dual codes,” Finite Fields Appl., vol. 42, 2016, pp. 269–295.
[12] S. R. López-Permouth, H. Özadam, F. Özbudak, and S. Szabo, “Polsyclic codes over Galois rings with applications to repeated-root constacyclic codes,” Finite Fields Their Appl., vol. 19, no. 1, pp. 16–38, Jan. 2013.
[13] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes. Amsterdam, The Netherlands: North-Holland, 1998.
[14] C.-S. Nedeloaia, “Weight distributions of cyclic self-dual codes,” IEEE Trans. Inf. Theory, vol. 49, no. 6, pp. 1582–1591, Jun. 2003.
[15] J. L. Massey, D. J. Costello, and J. Justesen, “Polynomial weights and code constructions,” IEEE Trans. Inf. Theory, vol. IT-19, no. 1, pp. 101–110, Jan. 1973.
[16] H. Özadam and F. Özbudak, “The minimum Hamming distance of cyclic codes of length $2^p$,” in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (Lecture Notes in Computer Science), vol. 5527. Springer, 2009, pp. 92–100.

[17] V. Pless and W. C. Huffman, *Handbook of Coding Theory*. Amsterdam, The Netherlands: Elsevier, 1998.

[18] C. E. Shannon, “A mathematical theory of communication,” *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul./Oct. 1948.

[19] A. Sharma and S. Rani, “Repeated-root constacyclic codes of length $4\ell^m p^s$,” *Finite Fields Appl.*, vol. 40, no. C, pp. 163–200, Jul. 2016.

[20] L.-Z. Tang, C. B. Soh, and E. Gunawan, “A note on the q-ary image of a q"-ary repeated-root cyclic code,” *IEEE Trans. Inf. Theory*, vol. 43, no. 2, pp. 732–737, Mar. 1997.

[21] J. H. van Lint, “Repeated-root cyclic codes,” *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 343–345, Mar. 1991.

**Hai Q. Dinh** received the B.Sc., M.Sc., and Ph.D. degrees in mathematics from Ohio University, USA, in 1998, 2000, and 2003, respectively. He worked one year as a Visiting Professor with North Dakota State University, USA. Since 2004, he has been working as a Tenured Professor in mathematics with Kent State University, USA, where he is currently a Professor in applied mathematics with the Department of Mathematical Sciences. Since 2004, he has also been published more than 75 articles at high-level SCI(E) research journals, such as the *Journal of Algebra*, the *Journal of Pure and Applied Algebra*, the *IEEE Transactions in Information Theory*, the *IEEE Communication Letters*, *Finite Fields and Their Applications*, *Applicable Algebra in Engineering, Communication and Computing*, and *Discrete Applied Mathematics*. His research interests include algebra and coding theory. He has also been a well-known invited/keynote speaker at numerous international conferences and mathematics colloquium. Other than universities in the USA, he also gave many honorary tutorial lectures at international universities in China, Indonesia, Kuwait, Mexico, Singapore, Thailand, and Vietnam.

**Xiaoqiang Wang** received the Ph.D. degree from the School of Mathematics and Statistics, Central China Normal University, China, in 2019. His Ph.D. was on algebraic techniques of encoding/decoding cyclic codes over finite fields and rings. Since 2019, he has been a Postdoctoral Researcher with the Faculty of Mathematics and Statistics, Hubei University, China. His research interests include algebra and coding theory. He has published ten articles in high-ranked peer review journals, such as *Designs, Codes and Cryptography*, *Discrete Mathematics*, and *Finite Fields and Their Applications*.

**Paravee Maneejuk** has been working as a Lecturer with the Faculty of Economics, Chiang Mai University, Thailand, since 2018. Her research interests include information theory, economic development, growth, and applied econometrics. She has also worked with a research team from the Centre of Excellence in Econometrics, and has published about 50 articles in SCOPUS/ISI. She is currently working with the research team in applying the econometric models to solve several economic issues.