IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 22, 2020, accepted February 20, 2020, date of publication February 27, 2020, date of current version March 17, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2976536

On the Hamming Distances of Constacyclic Codes of Length $5p^s$

HAI Q. DINH[1,3], XIAOQIANG WANG[2], AND JIRAKOM SIRISRISAKULCHAI[4]

[1]Division of Computational Mathematics and Engineering, Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[2]Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China
[3]Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[4]Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University, Chiang Mai 52000, Thailand

Corresponding author: Xiaoqiang Wang (waxiqq@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 a prime, s, m be positive integers, and λ be a nonzero element of the finite field $\mathbb{F}_{p^m}$. In this paper, the algebraic structures of constacyclic codes of length $5\,p^s$ ($p \neq 5$) are obtained, which provide all self-dual, self-orthogonal and dual containing codes. Moreover, the exact values of the Hamming distances of all such codes are completely determined. Among other results, we obtain the degrees of the generator polynomials of all MDS repeated-root constacyclic codes of arbitrary length. As applications, several new and optimal codes are provided.

INDEX TERMS Constacyclic code, generator polynomial, repeated-root code, simple-root code, Hamming distance.

I. INTRODUCTION

Cyclic codes over finite fields have been well studied because of their rich algebraic structures and practical implementations, which explains their preferred role in engineering. Constacyclic codes are a direct generalization of cyclic codes, and they also play a very significant role in the theory of error-correcting codes.

For a prime p, let $\mathbb{F}_{p^m}$ be the finite field of order p^m. Given a nonzero element $\lambda \in \mathbb{F}_{p^m}$, λ-constacyclic codes of length n over $\mathbb{F}_{p^m}$ are defined by the ideals $\langle g(x)\rangle$ of quotient ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n-\lambda\rangle}$, where the generator polynomial $g(x)$ is the unique monic polynomial of minimum degree in the code, which is a divisor of $x^n - \lambda$. In general, constacyclic codes are grouped into two classes: simple-root constacyclic codes, where the generator polynomial $g(x)$ has no repeated irreducible roots, and repeated-root constacyclic codes, where the code length n is divisible by the characteristic p of the finite field. In 1991, Castagnoli *et al.* [2] and Van Lint [24] showed that repeated-root cyclic codes have a concatenated construction and are asymptotically bad. However, it turns out that optimal repeated-root cyclic codes still exist, which have motivated the researchers to further study these codes (see, e.g., [1], [5]–[11], [22].)

The associate editor coordinating the review of this manuscript and approving it for publication was Khmaies Ouahada.

In a series of papers [3], [4], [6]–[9], [15] and [22], the authors determined the algebraic structures in terms of polynomial generators of all constacyclic codes over $\mathbb{F}_{p^m}$ of different lengths. However, litter work has been done on determining the Hamming distances of constacyclic codes as it is a very hard task in general. By now, only a few results have been obtained.

In [6], Dinh determined the Hamming distances of cyclic codes of length p^s over $\mathbb{F}_{p^m}$. In 2013, by using the "weight-retaining" property of polynomials (see [19, Theorem 1.1]), [17] determined the Hamming distances of constacyclic codes of length ηp^s with generator polynomials $x^\eta + \gamma$ and $(x^{\eta'} + \gamma')(x^{\eta'} - \gamma')$, where $\eta = 2\eta'$, γ' and γ are the nonzero elements in the finite field. Later, based on the relationships of Hamming distances between simple-root cyclic codes and repeated-root cyclic codes (see [2, Theorem 1]), in [20] and [15], the authors computed the Hamming distances of cyclic codes of length $2p^s$ and the Hamming distances of cyclic codes of length $3p^s$ for the case $\gcd(3, p^m - 1) = 1$, respectively. Continuing this line of research, recently, we determined the Hamming distances of all constacyclic codes of length $3p^s$ for the remainder case of $\gcd(3, p^m-1) = 2$ [12], and those of all constacyclic codes of length $4p^s$ [13]. Moreover, all MDS constacyclic codes of length $3p^s$ and $4p^s$ are obtained in [12] and [13].

Motivated by these, in this paper, we aim to establish the Hamming distances of all constacyclic codes of length $5p^s$.

We first obtain the relationships about Hamming distances between simple-root constacyclic codes and repeated-root constacyclic codes to give the degrees of generator polynomials of all MDS repeated-root λ-constacyclic codes of arbitrary length. It is known that MDS constacyclic codes can be used to construct quantum MDS codes using well known constructions such as CSS construction. Hence, obtaining MDS code is very important for practical application. Let ℓ be a prime different from p, based on the algebraic structures of constacyclic codes of length ℓp^s, which is given by [3], we provide the precise algebraic structures of constacyclic codes of length 5 p^s explicitly, then the Hamming distances of all such constacyclic codes are given. As applications, we obtain some codes which are optimal with respect to the online databases of best codes known maintained at http://www.codetables.de, see Example 3.5, Example 5.10.

The remainder of this paper is organized as follows. Section II recalls some preliminary results. In Section III, the degrees of generator polynomials of all MDS repeated-root constacyclic codes are given. In Section IV, the algebraic structures of all constacyclic codes of length $5p^s$ are established, this structure also provides the necessary and sufficient conditions for the existence of self-dual, self-orthogonal and dual containing codes. In Section V, we obtain the Hamming distances of all constacyclic codes of length $5p^s$. Section VI concludes the paper.

II. PRELIMINARIES

Let $\mathbb{F}_{p^m}$ be the finite field of order p^m, where p is a prime and m is a positive integer. 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 the finite field $\mathbb{F}_{p^m}$ is a linear subspace of $\mathbb{F}_{p^m}^n$. Moreover, for a nonzero element λ of $\mathbb{F}_{p^m}$, if $(c_0, c_1, \cdots, c_{n-1}) \in C$ implies $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C$, C is called a λ-constacyclic code. In light of this definition, λ-constacyclic codes are called cyclic codes if $\lambda = 1$, and λ-constacyclic codes are called negacyclic codes if $\lambda = -1$. The following fact is well-known and straightforward.

Proposition 2.1 ([14], [18], [21]): A linear code C of length n over $\mathbb{F}_{p^m}$ is a λ-constacyclic code if and only if C is an ideal of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n-\lambda\rangle}$.

For a codeword $\mathbf{a} = (c_0, c_1, \cdots, c_{n-1}) \in C$, the Hamming weight of $\mathbf{a}$ is denoted by the number of nonzero components c_i for $0 \le i \le n-1$. For two codewords $\mathbf{a}$ and $\mathbf{b}$, the Hamming distance $\mathrm{d_H}(\mathbf{a}, \mathbf{b})$ is the Hamming weight $\mathrm{wt_H}(\mathbf{a}-\mathbf{b})$ of $\mathbf{a}-\mathbf{b}$. For a code C of length n over $\mathbb{F}_{p^m}$, the Hamming distance of C is defined as:

$$\mathrm{d_H}(C) = \min\{\mathrm{wt_H}(\mathbf{a}-\mathbf{b}) \mid (\mathbf{a}, \mathbf{b}) \neq (0,0),\ \mathbf{a}, \mathbf{b} \in C\}.$$

Clearly, for a linear code C, the smallest Hamming weight and the Hamming distance $\mathrm{d_H}(C)$ are the same, i.e.,

$$\mathrm{d_H}(C) = \min\{\mathrm{wt_H}(\mathbf{x}) \mid \mathbf{x} \neq 0,\ \mathbf{x} \in C\}.$$

From that, it is easy to see the following simple lemma.

Lemma 2.2: Let C be a nonzero constacyclic code and $C \neq \frac{\mathbb{F}_{p^m}[x]}{\langle x^n-\lambda\rangle}$. Then $\mathrm{d_H}(C) \ge 2$.

In [3], Chen *et al*. considered the algebraic structures of constacyclic codes of length ℓp^s over $\mathbb{F}_{p^m}$, where ℓ is a prime different from p. They showed that all constacyclic codes of length ℓp^s over $\mathbb{F}_{p^m}$ have the following algebraic structures.

Proposition 2.3 ([3, Theorem 4.1]): Let ℓ be a prime integer with $\gcd(\ell, p^m - 1) = 1$. Then all λ-constacyclic codes of length ℓp^s are ℓp^s-equivalent to the cyclic codes; in other words, there exists a unique element $a \in \mathbb{F}_{p^m}^*$ such that $a^{\ell p^s}\lambda = 1$. Further, the map

$$\varphi_a : \frac{\mathbb{F}_{p^m}[x]}{\langle x^{\ell p^s} - 1\rangle} \to \frac{\mathbb{F}_{p^m}[x]}{\langle x^{\ell p^s} - \lambda\rangle},$$
$$f(x) \mapsto f(ax),$$

which maps $f(x)$ to $f(ax)$ is a ring isomorphism.

Proposition 2.4 ([3, Theorem 4.2]): Assume that ℓ is a prime divisor of $q-1$. Let $\mu \in \mathbb{F}_{p^m}$ be a primitive ℓ-th root of unity in $\mathbb{F}_{p^m}$, and $\mathbb{F}_{p^m}^* = \langle\xi\rangle$. Let C be a λ-constacyclic code of length ℓp^s over $\mathbb{F}_{p^m}$. Then one of the following two cases holds:

I. either $\lambda \in \langle\xi^\ell\rangle$, then there exists $b \in \mathbb{F}_{p^m}^*$ such that $b^{\ell p^s}\lambda = 1$, and we have

$$C = \left\langle \left(\prod_{i=0}^{\ell-1}(x - b^{-1}\mu^i)^{\varsigma_i}\right)\right\rangle, \quad 0 \le \varsigma_i \le p^s,$$

for any $i = 0, 1, \cdots, \ell-1$.

II. or $\lambda \notin \langle\xi^\ell\rangle$, then there exists $d \in \mathbb{F}_{p^m}^*$ and a unique integer j, $1 \le j \le \ell-1$ such that $\lambda d^{\ell p^s} = \xi^{jp^s}$, and we have

$$C = \left\langle (x^\ell - d^{-1}\xi^j)^\varsigma \right\rangle,\ 0 \le \varsigma \le p^s.$$

In order to compute the Hamming distances of λ-constacyclic codes, we will use the so-called "weight-retaining" property of polynomial $x^n - c$, which was initiated in [19].

Lemma 2.5 ([19, Theorem 6.3]): Let N, n be positive integers, then for any polynomial $P(x)$ over $\mathbb{F}_{p^m}$, and any nonzero element c of $\mathbb{F}_{p^m}$, the Hamming weight of $P(x)(x^n + c)^N$ satisfies

$$\mathrm{wt_H}(P(x)(x^n + c)^N) \ge \mathrm{wt_H}\left(P(x) \pmod{x^n + c}\right) \cdot \mathrm{wt_H}((x^n + c)^N).$$

Let $N < p^s$ and $0 \le b_0, b_1, \cdots, b_{s-1} \le p-1$ be positive integers such that $N = b_{s-1}p^{s-1} + \cdots + b_1 p + b_0$, $0 \le b_i < p$, is the p-adic expansion of N. By Lemma 1 of [19], we have

$$\mathrm{wt_H}((x^n + c)^N) = \prod_{i=0}^{s-1}(b_i + 1). \tag{1}$$

Clearly, for any positive integer s and $0 \le \theta \le s-1$, $p^s - p^{s-\theta} = (p-1)p^{s-1} + (p-1)p^{s-2} + \cdots + (p-1)p^{s-\theta+1} + (p-1)p^{s-\theta}$. Then, combining with Theorem 7.5 of [17], we have the following lemma.

Lemma 2.6: Let $0 \le \varphi \le p-2$, *and* $0 \le \theta \le s-1$. *Assume that* $p^s - p^{s-\theta} + \varphi p^{s-\theta-1} + 1 \le i \le p^s - p^{s-\theta} + (\varphi+1)p^{s-\theta-1}$, *then* $\mathrm{wt_H}((x^n+c)^i) \ge (\varphi+2)p^\theta$ *and the equality holds when* $i = p^s - p^{s-\theta} + (\varphi+1)p^{s-\theta-1}$. *Moreover, if* $i \le j \le p^s - 1$, *we have* $\mathrm{wt_H}((x^n+c)^j) \ge (\varphi+2)p^\theta$.

III. HAMMING DISTANCES OF REPEATED-ROOT CONSTACYCLIC CODES OF ARBITRARY LENGTH

Let $\mathcal{C} = \langle g(x) \rangle$ be a repeated-root λ-constacyclic code of length lp^s over $\mathbb{F}_{p^m}$, where l is a positive integer and $\gcd(l, p) = 1$. By Proposition 2.1, such code can be seen as an ideal of the ambient ring

$$\mathcal{R}_{lp^s,\lambda} = \frac{\mathbb{F}_{p^m}[x]}{\langle x^{lp^s} - \lambda \rangle}.$$

Clearly, for any nonzero element $\lambda \in \mathbb{F}_{p^m}$, there exists a unique element $\gamma \in \mathbb{F}_{p^m}$ such that $\lambda = \gamma^{p^s}$ since $\gcd(p^s, p^m - 1) = 1$. Let

$$x^l - \gamma = \prod_{i=1}^{t} m_i(x) \tag{2}$$

be the factorization of $x^l - \gamma$ into product of pairwise coprime irreducible factors. Then the generator polynomial $g(x)$ of $\mathcal{C}$ can be expressed as $g(x) = \prod_{i=1}^{t} m_i(x)^{e_i}$, where $0 \le e_i \le p^s$. Let $\bar{\mathcal{C}}_z = \langle \bar{g}_z(x) \rangle$ be a simple-root γ-constacyclic code of length l over $\mathbb{F}_{p^m}$, where $\bar{g}_z(x)$ is defined as the product of those irreducible factors $m_i(x)$ of $g(x)$ that occur with times $z < e_i$ in $g(x)$ (If $z \ge e_i$ for $i = 1, 2, \cdots, t$, then $\bar{g}_z(x) = 1$.)

Example 3.1: Assume that $5 \mid p^m - 1$ and $\varepsilon \in \mathbb{F}_{p^m}$ is a primitive 5th root of unity in $\mathbb{F}_{p^m}$. Let $\mathcal{C}$ be a constacyclic code of length $5\,p^s$ with the generator polynomial

$$g(x) = (x-1)^i (x-\varepsilon)^j (x-\varepsilon^2)^y (x-\varepsilon^3)^u (x-\varepsilon^4)^v,$$

where $0 \le v \le u \le y \le j \le i \le p^s$. Then the generator polynomial of $\bar{\mathcal{C}}_z$ is

$$\bar{g}_z(x) = \begin{cases} 1, & \text{if } v \le u \le y \le j \le i \le z, \\ x-1, & \text{if } v \le u \le y \le j \le z < i, \\ (x-1)(x-\varepsilon), & \text{if } v \le u \le y \le z < j \le i, \\ (x-1)(x-\varepsilon)(x-\varepsilon^2), & \text{if } v \le u \le z < y \le j \le i, \\ (x-1)(x-\varepsilon)(x-\varepsilon^2)(x-\varepsilon^3), & \text{if } v \le z < u \le y \le j \le i. \end{cases}$$

We start with the following result.

Theorem 3.2: Let constacyclic codes $\mathcal{C}$ *and* $\bar{\mathcal{C}}_z$ *be defined as above. Then* $\mathrm{d_H}(\mathcal{C}) = \min\{\mathrm{wt_H}((x^l-\gamma)^z) \cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\}$, *where* $\min\{e_1, e_2, \cdots, e_t\} \le z \le p^s - 1$.

Proof: Obviously, the theorem holds trivially for the zero code. Now, we assume that $\mathcal{C}$ is not zero. Let $c_0(x)$ be the nonzero element of $\bar{\mathcal{C}}_z$ such that $\mathrm{d_H}(\bar{\mathcal{C}}_z) = \mathrm{wt_H}(c_0(x))$. Then the generator polynomial $g(x)$ of $\mathcal{C}$ satisfies

$$g(x) \mid (x^l - \gamma)^z (c_0(x))^{p^s},$$

where $\min\{e_1, e_2, \cdots, e_t\} \le z \le p^s - 1$.

It is easy to see that $c_1(x) = (x^l-\gamma)^z (c_0(x))^{p^s} \pmod{x^{lp^s} - \lambda}$ belongs to $\mathcal{C}$. Hence,

$$\begin{aligned} \mathrm{d_H}(\mathcal{C}) &\le \mathrm{wt_H}(c_1(x)) \\ &= \mathrm{wt_H}\left((x^l-\gamma)^z \cdot c_0(x)^{p^s} \pmod{x^{lp^s} - \lambda}\right) \\ &\le \mathrm{wt_H}((x^l-\gamma)^z) \cdot \mathrm{wt_H}(c_0(x)^{p^s}) \\ &= \mathrm{wt_H}((x^l-\gamma)^z) \cdot \mathrm{wt_H}(c_0(x)) \\ &= \mathrm{wt_H}((x^l-\gamma)^z) \cdot \mathrm{d_H}(\bar{\mathcal{C}}_z). \end{aligned} \tag{3}$$

Therefore, we have $\mathrm{d_H}(\mathcal{C}) \le \min\{\mathrm{wt_H}((x^l-\gamma)^z) \cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\}$, where $\min\{e_1, e_2, \cdots, e_t\} \le z \le p^s - 1$.

We now show that $\mathrm{d_H}(\mathcal{C}) \ge \min\{\mathrm{wt_H}((x^l-\gamma)^z) \cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\}$, where $\min\{e_1, e_2, \cdots, e_t\} \le z \le p^s - 1$. Let $c(x)$ be a nonzero element of $\mathcal{C}$ such that $\mathrm{d_H}(\mathcal{C}) = \mathrm{wt_H}(c(x))$. Clearly, there exist an integer r and a polynomial $f(x)$ such that

$$c(x) = (x^l - \gamma)^r f(x),$$

where r is the largest integer such that $(x^l-\gamma)^r \mid c(x)$. Clearly, we have $\min\{e_1, e_2, \cdots, e_t\} \le r \le p^s - 1$. Let $v(x) = f(x) \pmod{x^l - \gamma}$, then $v(x) \in \bar{\mathcal{C}}_r$. Hence, by Lemma 2.5, we have

$$\begin{aligned} \mathrm{wt_H}(c(x)) &= \mathrm{wt_H}((x^l-\gamma)^r \cdot f(x)) \\ &\ge \mathrm{wt_H}((x^l-\gamma)^r) \cdot \mathrm{wt_H}(f(x) \pmod{x^l - \gamma}) \\ &= \mathrm{wt_H}\left((x^l-\gamma)^r\right) \cdot \mathrm{wt_H}(v(x)) \\ &\ge \mathrm{wt_H}\left((x^l-\gamma)^r\right) \cdot \mathrm{d_H}(\bar{\mathcal{C}}_r). \end{aligned}$$

Therefore, $\mathrm{d_H}(\mathcal{C}) \ge \mathrm{wt_H}\left((x^l-\gamma)^r\right) \cdot \mathrm{d_H}(\bar{\mathcal{C}}_r) \ge \min\{\mathrm{wt_H}((x^l-\gamma)^z) \cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\}$, where $\min\{e_1, e_2, \cdots, e_t\} \le z \le p^s - 1$. Combining with (3), the result follows. □

Remark 3.3: In the special case that $\mathcal{C}$ *is a cyclic code, Theorem* 3.2 *was proved in [2]. We generalize their result for cyclic codes to constacyclic codes in general. The idea of Theorem* 3.2 *comes from [2], but the proof of Theorem* 3.2 *is more concise than the proof in [2].*

If C is a linear code with length n, dimension k and Hamming distance $\mathrm{d_H}$ over the finite field $\mathbb{F}_{p^m}$, then the Singleton bound holds true that $\mathrm{d_H} \le n - k + 1$.

If the equality holds, i.e., $\mathrm{d_H} = n - k + 1$, then C is called an MDS code. It is well known that MDS codes have the best possible error-correction capability. Hence, constructing MDS codes is one of the central topics in coding theory. We now determine the degrees of generator polynomials of all MDS repeated-root constacyclic codes of arbitrary length.

Theorem 3.4: Let notions be as in Theorem 3.2 *and* $g(x)$ *be the generator polynomial of* $\mathcal{C}$. *Then the code* $\mathcal{C}$ *is an MDS code if and only if one of the following conditions holds:*

- *If* $l = s = 1$, *then* $\deg(g(x)) = i$, *for* $0 \le i \le p-1$; *in this case,* $\mathrm{d_H}(\mathcal{C}) = i + 1$.

- *If $l \geq 2$, then*
  - $\deg(g(x)) = 0$*; in this case,* $\mathrm{d_H}(\mathcal{C}) = 1$.
  - $\deg(g(x)) = 1$*; in this case,* $\mathrm{d_H}(\mathcal{C}) = 2$.
  - $\deg(g(x)) = lp^s - 1$*; in this case,* $\mathrm{d_H}(\mathcal{C}) = lp^s$.

Proof: It is easy to check that if s, l and the degree of $g(x)$ satisfies above conditions, then $\mathcal{C}$ is an MDS code. In the following, we only need to show that if $\mathcal{C}$ is an MDS code, $g(x)$ must satisfy above conditions. We consider two cases.

Case 1: $l = 1$. Clearly, in this case, $\mathcal{C}$ is a λ-constacyclic code of length p^s, and the ambient ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-\lambda\rangle}$ is a chain ring, whose ideals are precisely $\langle (x-\gamma)^i \rangle$, where $0 \leq i \leq p^s$ and $\gamma^{p^s} = \lambda$. There are two possibilities.

Case 1.1: $s = 1$. By (1) and Lemma 2.5, we get that if $\mathcal{C} = \langle (x-\gamma)^i \rangle$, then $\mathrm{d_H}(\mathcal{C}) = i+1$ for $0 \leq i \leq p-1$, and if $\mathcal{C} = \langle (x-\gamma)^p \rangle = \langle 0 \rangle$, then $\mathrm{d_H}(\mathcal{C}) = 0$. By the definition of MDS codes, it is easy to check that if $\mathcal{C}$ is an MDS code, then $0 \leq i \leq p-1$.

Case 1.2: $s > 1$. Obviously, $\mathcal{C}$ can be expressed as $\mathcal{C} = \langle (x-\gamma)^i \rangle$, where $0 \leq i \leq p^s$. For the trivial case, when $i = 0$ and $i = p^s$, it is easy to see that $\mathcal{C}$ is an MDS code if and only if $i = 0$, i.e., $\mathcal{C}$ is an MDS code if and only if $\deg(g(x)) = 0$, implying $\mathrm{d_H}(\mathcal{C}) = 1$.

Now, we consider $1 \leq i \leq p^s - 1$. Let $0 \leq \beta \leq p-2$ and $0 \leq \tau \leq s-1$, clearly, there exist β and τ such that $p^s - p^{s-\tau} + \beta p^{s-\tau-1} + 1 \leq i \leq p^s - p^{s-\tau} + (\beta+1)p^{s-\tau-1}$ for any i. By Theorem 4.11 of [6], we have that if $p^s - p^{s-\tau} + \beta p^{s-\tau-1} + 1 \leq i \leq p^s - p^{s-\tau} + (\beta+1)p^{s-\tau-1}$, then $\mathrm{d_H}(\mathcal{C}) = (\beta+2)p^\tau$.

Obviously, the dimension of $\mathcal{C} = \langle (x-\gamma)^i \rangle$ is $p^s - i$. Then

$$\begin{aligned}
p^s - (p^s - i) + 1 &= i + 1 \\
&\geq p^s - p^{s-\tau} + \beta p^{s-\tau-1} + 1 + 1 \\
&= p^{s-\tau}(p^\tau - 1) + \beta p^{s-\tau-1} + 2 \\
&\geq p(p^\tau - 1) + \beta p^{s-\tau-1} + 2 \\
&\quad \text{(equality when } \tau = s-1, \text{ or } \tau = 0) \\
&\geq (\beta+2)(p^\tau - 1) + \beta p^{s-\tau-1} + 2 \\
&\quad \text{(equality when } p = \beta + 2) \\
&= (\beta+2)p^\tau + (p^{s-\tau-1} - 1)\beta \\
&= \mathrm{d_H}(\mathcal{C}) \\
&\quad \text{(equality when } \tau = s-1, \text{ or } \beta = 0.)
\end{aligned}$$

Therefore, $p^s - (p^s - i) + 1 \geq \mathrm{d_H}(\mathcal{C})$ with equality holds if and only if $p = \beta + 2$ and $\tau = s-1$ (in this case $i = \deg(g(x)) = p^s - 1$, $\mathrm{d_H}(\mathcal{C}) = p^s$;) or $\beta = \tau = 0$ (in this case $i = \deg(g(x)) = 1$, $\mathrm{d_H}(\mathcal{C}) = 2$.)

Case 2: $l > 1$. By (2), since $\mathcal{C}$ is an ideal of the ambient ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{lp^s}-\lambda\rangle}$, then $\mathcal{C}$ can be expressed as $\langle m_1(x)^{e_1} m_2(x)^{e_2} \cdots m_t(x)^{e_t} \rangle$, where $0 \leq e_1, e_2, \cdots, e_t \leq p^s$ and $m_1(x), m_2(x), \cdots, m_t(x)$ are defined in (2).

Obviously, the degree of generator polynomial $g(x)$ of $\mathcal{C}$ satisfies

$$\begin{aligned}
\deg(g(x)) = e_1 \cdot \deg(m_1(x)) + e_2 \cdot \deg(m_2(x)) \\
+ \cdots + e_t \cdot \deg(m_t(x)).
\end{aligned}$$

So, the dimension of $\mathcal{C}$ is

$$\begin{aligned}
k(\mathcal{C}) = lp^s - (e_1 \cdot \deg(m_1(x)) + e_2 \cdot \deg(m_2(x)) \\
+ \cdots + e_t \cdot \deg(m_t(x))). \quad (4)
\end{aligned}$$

If $t = 1$, then $\mathcal{C}$ can be expressed as $\mathcal{C} = \langle (x^l - \gamma)^i \rangle$. By Theorem 7.5 of [17], we obtain that no matter $l = 1$ or $l > 1$, $\mathcal{C} = \langle (x^l - \gamma)^i \rangle$ has the same Hamming distance. Hence, using the same technique as **Case 1.2**, we get $\mathcal{C}$ is an MDS code if and only if $\deg(g(x)) = 0$. In the following, we always assume that $t > 1$. There are three possibilities.

Case 2.1: Some of $e_i = 0$, where $1 \leq i \leq t$. Without loss of generality, we can suppose that $e_1 = 0$ and $e_i > 0$ for $2 \leq i \leq t$. Then $m_2(x)^{p^s} m_3(x)^{p^s} \cdots m_t(x)^{p^s}$ must be a codeword of $\mathcal{C}$. Hence,

$$\begin{aligned}
\mathrm{d_H}(\mathcal{C}) &\leq \mathrm{wt_H}(m_2(x)^{p^s} m_3(x)^{p^s} \cdots m_t(x)^{p^s}) \\
&= l - \deg(m_1(x)) + 1. \quad (5)
\end{aligned}$$

On the other hand, it is easy to see

$$\begin{aligned}
\mathrm{d_H}(\mathcal{C}) &= lp^s - (lp^s - e_2 \cdot \deg(m_2(x)) \\
&\quad + \cdots + e_t \cdot \deg(m_t(x))) + 1 \\
&= e_2 \cdot \deg(m_2(x)) + \cdots + e_t \cdot \deg(m_t(x)) + 1 \\
&\geq \deg(m_2(x)) + \cdots + \deg(m_t(x)) + 1 \\
&\quad \text{(equality when } e_2 \cdots = e_t = 1) \\
&= l - \deg(m_1(x)) + 1. \quad (6)
\end{aligned}$$

Combining with (5) and (6), if $\mathcal{C}$ is an MDS code, then $e_1 = 0$ and $e_2 = e_3 = \cdots = e_t = 1$. Hence, the generator polynomial $g(x)$ of $\mathcal{C}$ can be expressed as

$$g(x) = m_2(x)m_3(x)\cdots m_t(x).$$

Obviously, $m_2(x)m_3(x)\cdots m_t(x) \,|\, x^l - \gamma$, then $\mathrm{d_H}(\mathcal{C}) \leq \mathrm{wt_H}(x^l - \gamma) = 2$. So, combining with Lemma 2.2, we have $\mathrm{d_H}(\mathcal{C}) = 2$. If $\mathcal{C}$ is an MDS code, then $2 = l - \deg(m_1(x)) + 1$, i.e., $l - \deg(m_1(x)) = 1$, implying

$$\begin{aligned}
l - \deg(m_1(x)) &= \deg(m_2(x)m_3(x)\cdots m_t(x)) \\
&= \deg(g(x)) = 1.
\end{aligned}$$

Case 2.2: $0 < e_i < p^s$, where $1 \leq i \leq t$. By Theorem 3.2, we obtain $\mathrm{d_H}(\mathcal{C}) = \min\{\mathrm{wt_H}((x^l - \gamma)^z) \cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\}$, where $\min\{e_1, e_2, \cdots, e_t\} \leq z \leq p^s - 1$. Without loss of generality, we assume that $e_t \geq \max\{e_1, e_2, \cdots, e_{t-1}\}$. Let $z = e_t$, by the definition of $\bar{\mathcal{C}}_z$, we have $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 1$. Then, $\mathrm{d_H}(\mathcal{C}) \leq \mathrm{wt_H}((x^l - \gamma)^z) \leq z + 1$. Obviously, if

$$z+1 = lp^s - (lp^s - (e_1 \cdot \deg(m_1(x)) + \cdots + z \cdot \deg(m_t(x)))) + 1,$$

then $e_1 = e_2 = \cdots = e_{t-1} = 0$ and $\deg(m_t(x)) = 1$, which is contradictory to $0 < e_i < p^s$ and $t > 1$. Therefore, there is no MDS code.

Case 2.3: $p^s = \max\{e_1, \cdots, e_t\}$ and $\min\{e_1, \cdots, e_t\} > 0$. Without loss of generality, we assume that $e_h = e_{h+1} = \cdots = e_t = p^s$ and $p^s > e_{h-1} \geq \max\{e_1, e_2, \cdots, e_{h-2}\}$, where $1 \leq h \leq t$.

By Theorem 3.2, we obtain $\mathrm{d_H}(\mathcal{C}) = \min\{\mathrm{wt_H}((x^l-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\}$, where $\min\{e_1, e_2, \cdots, e_t\} \le z \le p^s - 1$. From the definition of $\bar{\mathcal{C}}_z$, we have $\bar{\mathcal{C}}_{h-1} = \langle m_h(x)m_{h+1}(x)\cdots m_t(x)\rangle$. Assume

$$\eta = \deg(m_h(x)m_{h+1}(x)\cdots m_t(x)),$$

then $\mathrm{d_H}(\bar{\mathcal{C}}_{h-1}) \le \eta + 1$. Hence,

$$\begin{aligned}\mathrm{d_H}(\mathcal{C}) &= \min\{\mathrm{wt_H}((x^l-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\}\\ &\le \mathrm{wt_H}((x^l-\gamma)^{e_{h-1}})\cdot \mathrm{d_H}(\bar{\mathcal{C}}_{h-1})\\ &\le (\eta+1)\cdot(e_{h-1}+1).\end{aligned}$$

Let $e_g = e_1\cdot\deg(m_1(x)) + e_2\cdot\deg(m_2(x)) + \cdots + e_{h-1}\cdot\deg(m_{h-1}(x))$. Clearly, $e_g \ge e_{h-1}$. From (4), the dimension of $\mathcal{C}$ can be expressed as $k(\mathcal{C}) = lp^s - \eta p^s - e_g$. Hence,

$$\begin{aligned}&lp^s - k(\mathcal{C}) + 1\\ &\quad= \eta p^s + e_g + 1\\ &\quad\ge \eta p^s + e_{h-1} + 1\\ &\qquad\text{(equality when } e_g = e_{h-1} \text{ and } \deg(m_{h-1}(x)) = 1)\\ &\quad\ge \eta(e_{h-1}+1) + e_{h-1} + 1\\ &\qquad\text{(equality when } e_{h-1} = p^s - 1)\\ &\quad= (\eta+1)(e_{h-1}+1).\end{aligned}$$

Hence, the equality holds if and only if $e_1 = p^s - 1$ and $\deg(m_1(x)) = 1$. Therefore, in this case, $\mathcal{C}$ is an MDS code if and only if the generator polynomial of $\mathcal{C}$ can be expressed as $g(x) = m_1(x)^{p^s-1}m_2(x)^{p^s}$ and $\deg(m_1(x)) = 1$. It follows that $\mathcal{C}$ is an MDS code if and only if $\deg(g(x)) = lp^s - 1$.

Combining all cases, the result follows. □

Example 3.5: Let $p = 23$, $s = l = 1$, and $\deg(g(x)) = i$, for $0 \le i \le 22$, then $\mathcal{C}$ is a $[23, 23-i, i+1]$ code by Theorem 3.4, which an MDS code.

IV. STRUCTURES OF CONSTACYCLIC CODES OF LENGTH $5p^s$

As discussed in Section III, λ-constacyclic codes of length $5p^s$ over $\mathbb{F}_{p^m}$ are ideals of the ring

$$\mathcal{R}_{5\,p^s,\lambda} = \frac{\mathbb{F}_{p^m}[x]}{\langle x^{5p^s} - \lambda\rangle}.$$

The purpose of this section is to give the algebraic structures in term of generator polynomials of all repeated root λ-constacyclic codes of length $5p^s$ over $\mathbb{F}_{p^m}$. Let $a, \mu \in \mathbb{F}_{p^m}^*$, recall from [3] that λ- and μ-constacyclic codes of length $5\,p^s$ are called equivalent if the map

$$\begin{aligned}\varphi_a : \frac{\mathbb{F}_{p^m}[x]}{\langle x^{5\,p^s} - \mu\rangle} &\to \frac{\mathbb{F}_{p^m}[x]}{\langle x^{5\,p^s} - \lambda\rangle},\\ f(x) &\mapsto f(ax),\end{aligned}$$

which maps $f(x)$ to $f(ax)$ is a ring isomorphism.

From the proof of Theorem 4.1 in [3], when $5 \mid p^m - 1$, we immediate have the following result.

Theorem 4.1: Let $\mathbb{F}_{p^m}$ be a finite field satisfying $5 \mid p^m - 1$, $\varepsilon \in \mathbb{F}_{p^m}$ be a primitive 5th root of unity in $\mathbb{F}_{p^m}$, and $\mathbb{F}_{p^m}^* = \langle\xi\rangle$. Assume that $\mathcal{C}$ is a λ-constacyclic code of length $5\ p^s$ over $\mathbb{F}_{p^m}$.

I. If $\lambda \in \langle\xi^5\rangle$, then all λ-constacyclic codes are equivalent to

$$\mathcal{C} = \left\langle (x-1)^i(x-\varepsilon)^j(x-\varepsilon^2)^y(x-\varepsilon^3)^u(x-\varepsilon^4)^v\right\rangle,$$

where $0 \le i, j, y, u, v \le p^s$.

II. If $\lambda \notin \langle\xi^5\rangle$, then all λ-constacyclic codes are equivalent to

$$\mathcal{C} = \left\langle (x^5 - \xi^\pi)^i\right\rangle, \text{ where } 0 \le i \le p^s \text{ and } 1 \le \pi \le 4.$$

We now consider the algebraic structures of λ-constacyclic codes of length $5p^s$ for the case $\gcd(5, p^m - 1) = 1$. We first recall some results from [16].

Definition 4.2 [16, Definition 2.24]: Let $\mathbb{F}_{p^m}$ be a finite field, n be a positive integer not divisible by p, and δ be a primitive n-th root of unity over $\mathbb{F}_{p^m}$. Then the polynomial

$$Q_n(x) = \prod_{\substack{1\le i\le n\\ \gcd(i,n)=1}}^{n} (x - \delta^i)$$

is called the n-th cyclotomic polynomial over $\mathbb{F}_{p^m}$.

Proposition 4.3 [16, Theorem 2.47]: Let $\mathbb{F}_{p^m}$ be a finite field, l be a positive integer satisfying $\gcd(l, p^m) = 1$. Then $x^l - 1 = \prod_{n\mid l} Q_n(x)$, and $Q_n(x)$ factors into $\phi(n)/d$ distinct monic irreducible polynomials in $\mathbb{F}_{p^m}[x]$ of the same degree d, where d is the least positive integer such that $p^{md} \equiv 1 \pmod{l}$.

Here, we give all generator polynomials of λ-constacyclic codes of length $5p^s$ for the case $\gcd(5, p^m - 1) = 1$.

Theorem 4.4: Let $\mathbb{F}_{p^m}$ be a finite field satisfying $\gcd(5, p^m - 1) = 1$, i.e., $p^m \equiv 2, 3, \text{or } 4 \pmod 5$. Then all λ-constacyclic codes of length $5\ p^s$ are equivalent to the cyclic codes. If $p^m \equiv 4 \pmod 5$, then

$$\mathcal{C} = \langle (x-1)^i(x^2 - (\epsilon+\epsilon^4)x + 1)^j(x^2 - (\epsilon^2+\epsilon^3)x + 1)^u\rangle,$$

where $0 \le i, j, u \le p^s$ and $\epsilon \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ is a 5th root of unity. If $p^m \equiv 2 \text{ or } 3 \pmod 5$, then

$$\mathcal{C} = \left\langle (x-1)^i(x^4 + x^3 + x^2 + x + 1)^j\right\rangle,$$

where $0 \le i, j \le p^s$.

Proof: If $\gcd(5, p^m - 1) = 1$, By Proposition 4.3, we know that the ideals of ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{5p^s}-\lambda\rangle}$ and the ideals of ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{5p^s}-1\rangle}$ are isomorphic. Thus, in order to get the algebraic structures of all λ-constacyclic codes of length $5\ p^s$, we only need to get the irreducible factors of $x^{5p^s} - 1$. Obviously,

$$x^5 - 1 = Q_1(x)Q_5(x) = (x-1)(x^4 + x^3 + x^2 + x + 1),$$

where $Q_1(x)$ and $Q_5(x)$ are defined in Definition 4.2. Recall that from Proposition 4.3, d is the positive integer such that $p^{md} \equiv 1 \pmod 5$, i.e., d is a factor of $\phi(5)$. As $\phi(5) = 4$, it is clear that $d = 1, 2$ or 4. Now, we consider three cases for these values of d.

TABLE 1. λ-constacyclic codes of length $5p^s$.

p, m	λ	λ-constacyclic codes
Case 1. $p^m \equiv 4 \pmod 5$	$\lambda \in \mathbb{F}_{p^m}^*$	$\mathcal{C} = \langle (x-1)^i (x^2-(\epsilon+\epsilon^4)x+1)^j (x^2-(\epsilon^2+\epsilon^3)x+1)^u \rangle$
Case 2. $p^m \equiv 2$ or $3 \pmod 5$	$\lambda \in \mathbb{F}_{p^m}^*$	$\mathcal{C} = \langle (x-1)^i (x^4+x^3+x^2+x+1)^j \rangle$
Case 3. $p^m \equiv 1 \pmod 5$	$\lambda \in \langle \xi^5 \rangle$	$\mathcal{C} = \langle (x-1)^i (x-\varepsilon)^j (x-\varepsilon^2)^y (x-\varepsilon^3)^u (x-\varepsilon^4)^v \rangle$
Case 4. $p^m \equiv 1 \pmod 5$	$\lambda \notin \langle \xi^5 \rangle$	$\mathcal{C} = \langle (x^5-\xi^\pi)^i \rangle$

where $0 \le i, j, y, u, v \le p^s$, $1 \le \pi \le 4$, ξ is a primitive element of $\mathbb{F}_{p^m}$, ε is a 5th root of unity in $\mathbb{F}_{p^m}$ and ϵ is a 5th root of unity in $\epsilon \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$.

Case 1: $d = 1$. By Proposition 4.3, $p^m \equiv 1 \pmod 5$, which is impossible since $\gcd(5, p^m - 1) = 1$.

Case 2: $d = 2$. By Proposition 4.3, $p^{2m} \equiv 1 \pmod 5$. This means that $p^m \equiv 1$ or $4 \pmod 5$. However, $p^m \equiv 1 \pmod 5$ contradicts to $\gcd(5, p^m - 1) = 1$. Therefore, $p^m \equiv 4 \pmod 5$. Let $\epsilon \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ be a 5th root of unity. Then

$$\begin{aligned} Q_5(x) &= (x-\epsilon)(x-\epsilon^2)(x-\epsilon^3)(x-\epsilon^4) \\ &= \left(x^2-(\epsilon+\epsilon^4)x+1\right)\left(x^2-(\epsilon^2+\epsilon^3)x+1\right). \end{aligned}$$

By Proposition 4.3, we obtain $x^2-(\epsilon+\epsilon^4)x+1$ and $x^2-(\epsilon^2+\epsilon^3)x+1$ are irreducible polynomials over $\mathbb{F}_{p^m}$. Hence,

$$\mathcal{C} = \langle (x-1)^i (x^2-(\epsilon+\epsilon^4)x+1)^j (x^2-(\epsilon^2+\epsilon^3)x+1)^u \rangle,$$

where $0 \le i, j, u \le p^s$.

Case 3: $d = 4$. By Proposition 4.3, $Q_5(x)$ is an irreducible polynomial over $\mathbb{F}_{p^m}$. Hence,

$$\mathcal{C} = \left\langle (x-1)^i (x^4+x^3+x^2+x+1)^j \right\rangle,$$

where $0 \le i, j \le p^s$.

Combining all cases, the results follows. □

By the classification in Theorem 4.1 and Theorem 4.4, each λ-constacyclic code of length $5p^s$ over $\mathbb{F}_{p^m}$ is isomorphic to one specific constacyclic code via a ring isomorphism. We now list the structures of all λ-constacyclic codes of length $5p^s$ over $\mathbb{F}_{p^m}$ in Table 1.

For a linear code C over $\mathbb{F}_{p^m}$, its *dual code* $C^\perp$ is defined as

$$C^\perp = \{x \in \mathbb{F}_{p^m}^n \mid x \cdot y = 0, \forall y \in C\}.$$

Clearly, C is called *self-orthogonal* if $C \subseteq C^\perp$, and C is *dual-containing* if $C^\perp \subseteq C$. Moreover, C called *self-dual* if $C = C^\perp$. These kinds of codes have been an interesting class with a lot of applications in coding theory for a long time. We now give the necessary and sufficient conditions for λ-constacyclic codes of length $5p^s$ over $\mathbb{F}_{p^m}$ to be self-dual, self-orthogonal, or dual containing.

Theorem 4.5: Let $\mathcal{C}$ be a nonzero λ-constacyclic code of length $5p^s$ over $\mathbb{F}_{p^m}$. If $p^m \equiv 4 \pmod 5$, then

(a) $\mathcal{C}$ is dual containing if and only if $\lambda^2 = 1$ and $0 \le i, j, k \le p^s/2$.

(b) $\mathcal{C}$ is self-orthogonal if and only if $\lambda^2 = 1$ and $p^s/2 \le i, j, k \le p^s$.

(c) $\mathcal{C}$ is self-dual if and only if $\lambda^2 = 1$, $p = 2$, and $i = j = k = 2^{s-1}$.

If $p^m \equiv 2$ or $3 \pmod 5$, then

(a) $\mathcal{C}$ is dual containing if and only if $\lambda^2 = 1$ and $0 \le i, j \le p^s/2$.

(b) $\mathcal{C}$ is self-orthogonal if and only if $\lambda^2 = 1$ and $p^s/2 \le i, j \le p^s$.

(c) $\mathcal{C}$ is self-dual if and only if $\lambda^2 = 1$, $p = 2$, and $i = j = 2^{s-1}$.

If $p^m \equiv 1 \pmod 5$, then

(a) $\mathcal{C}$ is dual containing if and only if $\lambda^2 = 1$, $0 \le i \le p^s/2$, $j + v \le p^s$ and $y + u \le p^s$.

(b) $\mathcal{C}$ is self-orthogonal if and only if $\lambda^2 = 1$, $0 \le i \le p^s/2$, $j + v \ge p^s$ and $y + u \ge p^s$.

(c) $\mathcal{C}$ is self-dual if and only if $\lambda^2 = 1$, $p = 2$, and $i = j = y = u = v = 2^{s-1}$.

Proof: It is well-known that the dual of a λ-constacyclic code is a λ^{-1}-constacyclic code. Then, by [9, Proposition 2.5], we can obtain that if $\lambda^2 \ne \pm 1$, there do not exist the λ-constacyclic codes of length $5p^s$ over $\mathbb{F}_{p^m}$ to be self-dual, self-orthogonal, or dual containing. This means if there exist self-dual, self-orthogonal, or dual containing codes, then these constacyclic codes must be cyclic or negacyclic codes, i.e., $\lambda = \pm 1$.

Let ε be defined in Table 1 and $i = 1, 2, 3, 4$, assume that $(x-\varepsilon^i)^*$ is the reciprocal of $x - \varepsilon^i$, then $(x-\varepsilon^i)^* = x(x^{-1} - \varepsilon^i) = -\varepsilon^i x + 1 = -\varepsilon^i (x - \varepsilon^{5-i})$. By Table 1 and [9, Proposition 2.4], if $p^m \equiv 4 \pmod 5$, we have

$$\begin{aligned} \mathcal{C}^\perp = \big\langle &(x-1)^{p^s-i} (x^2-(\epsilon+\epsilon^4)x+1)^{p^s-j} \\ &(x^2-(\epsilon^2+\epsilon^3)x+1)^{p^s-u} \big\rangle; \end{aligned}$$

if $p^m \equiv 2$ or $3 \pmod 5$, we obtain

$$\mathcal{C}^\perp = \left\langle (x-1)^{p^s-i} (x^4+x^3+x^2+x+1)^{p^s-j} \right\rangle;$$

if $p^m \equiv 4 \pmod 5$, we get

$$\begin{aligned} \mathcal{C}^\perp = \big\langle &(x-1)^{p^s-i} (x-\varepsilon)^{p^s-v} (x-\varepsilon^2)^{p^s-u} \\ &(x-\varepsilon^3)^{p^s-y} (x-\varepsilon^4)^{p^s-j} \big\rangle. \end{aligned}$$

From the generator polynomial of $\mathcal{C}^\perp$, the result follows.

V. HAMMING DISTANCES OF CONSTACYCLIC CODES OF LENGTH $5p^s$

In this section, we give the Hamming distances of all λ-constacyclic codes of length $5p^s$. The Hamming distances of Case 4 in Table 1 have been given in Theorem 7.5 of [17]. We present this result in simplified forms here.

Lemma 5.1 ([17, Theorem 7.9]): Assume $0 \le \beta_0 \le p-2$, and $0 \le \tau_0 \le s-1$. Let p be a prime, m be a positive integer, $1 \le \pi \le 4$, ξ be a primitive element of $\mathbb{F}_{p^m}$. If the constacyclic codes of length $5p^s$ over $\mathbb{F}_{p^m}$ are of the form

$\mathcal{C} = \langle (x^5 - \xi^\pi)^i \rangle$ *for* $0 \le i \le p^s$, *then the Hamming distances* $\mathrm{d_H}(\mathcal{C})$ *are determined by:*

$$\mathrm{d_H}(\mathcal{C}) = \begin{cases} 1, & \text{if } i = 0, \\ (\beta_0 + 2)p^{\tau_0}, & \text{if } p^s - p^{s-\tau_0} + \beta_0 p^{s-\tau_0-1} + 1 \le i \\ & \quad \le p^s - p^{s-\tau_0} + (\beta_0 + 1)p^{s-\tau_0-1}, \\ 0, & \text{if } i = p^s. \end{cases}$$

5.1 Case 1

As discussed in Section III, recall that z is an integer such that $\min\{i, j, u\} \le z \le p^s - 1$. Let $e_{z,t} = 1$ if $t > z$, otherwise, $e_{z,t} = 0$, where $t = i, j$, or u. Then the generator polynomial of simple-root γ-constacyclic code $\bar{\mathcal{C}}_z$ can be expressed as

$$\bar{g}_z(x) = (x-1)^{e_{i,z}}(x^2 - (\epsilon + \epsilon^4)x + 1)^{e_{j,z}} (x^2 - (\epsilon^2 + \epsilon^3)x + 1)^{e_{u,z}}, \quad (7)$$

where ϵ is a 5th root of unity in $\epsilon \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$. Here, we consider the Hamming distance of $\bar{\mathcal{C}}_z = \langle \bar{g}_z(x) \rangle$.

Proposition 5.2: Assume $0 \le u \le j \le i \le p^s$. *Let* $\bar{\mathcal{C}}_z = \langle \bar{g}_z(x) \rangle$ *be a* γ*-constacyclic code of length* 5 *over* $\mathbb{F}_{p^m}$, *where* $\bar{g}_z(x)$ *is defined in (7). Then*

$$\mathrm{d_H}(\bar{\mathcal{C}}_z) = \begin{cases} 1, & \text{if } u \le j \le i \le z, \\ 2, & \text{if } u \le j \le z < i, \\ 4, & \text{if } u \le z < j \le i. \end{cases}$$

Proof: There are three possibilities.

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

Case 2: $u \le j \le z < i$. In this case, obviously, $\bar{\mathcal{C}}_z = \langle x - 1 \rangle$. Then, by Lemma 2.2, $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 2$.

Case 3: $u \le z < j \le i$. In this case, we have,

$$\begin{aligned} \bar{g}_z(x) &= (x-1)(x^2 - (\epsilon + \epsilon^4)x + 1) \\ &= x^3 - (1 + \epsilon + \epsilon^4)x^2 + (1 + \epsilon + \epsilon^4)x + 1 \\ &= x^3 + (\epsilon^2 + \epsilon^3)x^2 - (\epsilon^2 + \epsilon^3)x + 1. \end{aligned}$$

Let $c(x)$ be an arbitrary nonzero codeword of $\bar{\mathcal{C}}_z$, by the Division Algorithm, then $c(x)$ can be expressed as $c(x) = (x^3 + (\epsilon^2 + \epsilon^3)x^2 - (\epsilon^2 + \epsilon^3)x + 1)(ax + b) = ax^4 + (b + a(\epsilon^2 + \epsilon^3))x^3 + (\epsilon^2 + \epsilon^3)(b - a)x^2 + (a - (\epsilon^2 + \epsilon^3)b)x + b$, where $(a, b) \ne (0, 0)$. There are two possibilities.

If $a = 0$, obviously, $\mathrm{wt_H}(c(x)) = 4$.

If $a \ne 0$, clearly, $b + a(\epsilon^2 + \epsilon^3) = 0$ if and only if $b = -a(\epsilon^2 + \epsilon^3)$; $(\epsilon^2 + \epsilon^3)(b - a) = 0$ if and only if $b = a$; $a - (\epsilon^2 + \epsilon^3)b = 0$ if and only if $b = \frac{a}{\epsilon^2 + \epsilon^3}$. Through simple calculations, it is easy to see that $a \ne -a(\epsilon^2 + \epsilon^3) \ne \frac{a}{\epsilon^2 + \epsilon^3}$, implying $c(x) \ge 4$. Hence, we have $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 4$.

Combining all the cases, the result follows. □

Proposition 5.3: Assume $0 \le u \le i \le j \le p^s$. *Let* $\bar{\mathcal{C}}_z = \langle \bar{g}_z(x) \rangle$ *be a* γ*-constacyclic code of length* 5 *over* $\mathbb{F}_{p^m}$, *where* $\bar{g}_z(x)$ *is defined in (7). Then*

$$\mathrm{d_H}(\bar{\mathcal{C}}_z) = \begin{cases} 1, & \text{if } u \le i \le j \le z, \\ 3, & \text{if } u \le i \le z < j, \\ 4, & \text{if } u \le z < i \le j. \end{cases}$$

Proof: We consider three cases.

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

Case 2: $u \le i \le z < j$. In this case, clearly, $\bar{g}_z(x) = x^2 - (\epsilon + \epsilon^4)x + 1$. Combining with Lemma 2.2, obviously, $2 \le \mathrm{d_H}(\bar{\mathcal{C}}_z) \le 3$. If $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 2$, then there exists a polynomial $x^t - a \in \mathbb{F}_{p^m}[x]$ such that $x^2 - (\epsilon + \epsilon^4)x + 1 \mid x^t - a$. By the Division Algorithm, we can assume that $t < 5$. From $x^2 - (\epsilon + \epsilon^4)x + 1 \mid x^t - a$, we obtain ϵ and ϵ^4 are solutions of $x^t - a$. It follows that $\epsilon^{3t} = 1$, which contradicts to $t < 5$. So, $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 3$.

Case 3: $u \le z < i \le j$. By the same way as **Case 3** of Proposition 5.2, we get $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 4$.

Combining all the cases, the result follows. □

Proposition 5.4: Assume $0 \le i \le u \le j \le p^s$. *Let* $\bar{\mathcal{C}}_z = \langle \bar{g}_z(x) \rangle$ *be a* γ*-constacyclic code of length* 5 *over* $\mathbb{F}_{p^m}$, *where* $\bar{g}_z(x)$ *is defined in (7). Then*

$$\mathrm{d_H}(\bar{\mathcal{C}}_z) = \begin{cases} 1, & \text{if } i \le u \le j \le z, \\ 3, & \text{if } i \le u \le z < j, \\ 5, & \text{if } i \le z < u \le j. \end{cases}$$

Proof: We consider three cases.

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

Case 2: $i \le u \le z < j$. By the same way as **Case 2** of Proposition 5.3, we get $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 3$.

Case 3: $i \le z < u \le j$. In this case, obviously, the elements of $\bar{\mathcal{C}}_z$ are precisely $r(x^4 + x^3 + x^2 + x + 1)$, where $r \in \mathbb{F}_{p^m}$. So, $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 5$.

Combining all the cases, the result follows. □

We now compute the Hamming distances of $\mathcal{C}$ for the case $0 \le u \le j \le i \le p^s$. Firstly, we consider the case for $u = 0$.

Lemma 5.5: Let $u = 0$ *and* $0 \le j \le i \le p^s$ *be integers. Then,*

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

Proof: By Theorem 3.2 and Proposition 5.2, we have

$$\begin{aligned} \mathrm{d_H}(\mathcal{C}) &= \min\{\mathrm{wt_H}((x^5 - \gamma)^z) \cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \mid 0 \le z \le p^s - 1\} \\ &\le \mathrm{wt_H}((x^5 - \gamma)^0) \cdot \mathrm{d_H}(\bar{\mathcal{C}}_0) \le 4. \end{aligned}$$

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

Case 1: $z = 0$. In this case, by Proposition 5.2, we have

$$\mathrm{wt_H}((x^5 - \gamma)^0) \cdot \mathrm{d_H}(\bar{\mathcal{C}}_0) = \begin{cases} 1, & \text{if } i = j = 0, \\ 2, & \text{if } j = 0 \text{ and } 0 < i \le p^s \end{cases} \quad (8)$$

and $\mathrm{wt_H}((x^5 - \gamma)^0) \cdot \mathrm{d_H}(\bar{\mathcal{C}}_0) = 4$ for the other values of i, j.

Case 2: $1 \le z \le p^s - 1$. There are three possibilities.

Case 2.1: $j \le i \le z$. From Proposition 5.2, we get $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 1$. By Lemma 2.6, we obtain

$$\min\{\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \mid 0 < z \le p^{s-1}\} = 2,$$
$$\min\{\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \mid p^{s-1} < z \le 2p^{s-1}\} = 3,$$

and

$$\min\{\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \mid 3p^{s-1} < z \le p^s-1\} \ge 4.$$

Case 2.2: $j \le z < i$. From Proposition 5.2, clearly, $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 2$. By Lemma 2.6, we have $\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \ge 2\,\mathrm{wt_H}((x^5-\gamma)^z) \ge 4$ for any $1 \le z \le p^s-1$.

Case 2.3: $z < j \le i$. From Proposition 5.2, obviously, $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 4$. By Lemma 2.6, we have $\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \ge 4\,\mathrm{wt_H}((x^5-\gamma)^z) \ge 8$ for any $1 \le z \le p^s-1$.

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

$$\min\{\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \mid 1 \le z \le p^s-1\} = \begin{cases} 2, & \text{if } 0 \le j \le i \le p^{s-1}, \\ 3, & \text{if } 0 \le j \le 2p^{s-1} \text{ and } p^{s-1} < i \le 2p^{s-1} \end{cases} \tag{9}$$

and $\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \ge 4$ for the other values of i, j.

Combining with Theorem 3.2, (8) and (9), the result follows. □

In the following, we always assume that $0 \le \beta_0, \beta_1, \beta_2 \le p-2$, and $0 \le \tau_2 \le \tau_1 \le \tau_0 \le s-1$.

Lemma 5.6: Let $0 < k \le j \le i \le p^s-1$ *be integers such that* $p^s - p^{s-\tau_0} + \beta_0\, p^{s-\tau_0-1} + 1 \le i \le p^s - p^{s-\tau_0} + (\beta_0+1)p^{s-\tau_0-1}$, $p^s - p^{s-\tau_1} + \beta_1\, p^{s-\tau_1-1} + 1 \le j \le p^s - p^{s-\tau_1} + (\beta_1+1)p^{s-\tau_1-1}$ *and* $p^s - p^{s-\tau_2} + \beta_2\, p^{s-\tau_2-1} + 1 \le k \le p^s - p^{s-\tau_2} + (\beta_2+1)p^{s-\tau_2-1}$. *Then* $\mathrm{d_H}(\mathcal{C}) = \min\{(\beta_0+2)p^{\tau_0}, 2(\beta_1+2)p^{\tau_1}, 4(\beta_2+2)p^{\tau_2}\}$.

Proof: We consider three cases.

Case 1: $u \le j \le i \le z$. In this case, we get $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 1$. By Lemma 2.6, we have $\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \ge (\beta_0+2)p^{\tau_0}$ since $i \le z$. Moreover, when $z = p^s - p^{s-\tau_0} + (\beta_0+1)p^{s-\tau_0-1}$ the equality holds.

Case 2: $u \le j \le z < i$. In this case, we get $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 2$. By Lemma 2.6, we have $\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \ge 2(\beta_1+2)p^{\tau_1}$ since $j \le z$. Moreover, when $z = p^s - p^{s-\tau_1} + (\beta_1+1)p^{s-\tau_1-1}$ the equality holds.

Case 3: $u \le z < j \le i$. In this case, we get $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 3$. By Lemma 2.6, we have $\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \ge 4(\beta_2+2)p^{\tau_2}$ since $u \le z$. Moreover, when $z = p^s - p^{s-\tau_2} + (\beta_2+1)p^{s-\tau_2-1}$ the equality holds.

Therefore, by Theorem 3.2, $\mathrm{d_H}(\mathcal{C}) = \min\{(\beta_0+2)p^{\tau_0}, 2(\beta_1+2)p^{\tau_1}, 4(\beta_2+2)p^{\tau_2}\}$. □

By similar argument as Lemma 5.6, we obtain the following lemmas immediately.

Lemma 5.7: Let $u \le j \le i$ *be integers with* $i = p^s$, $p^s - p^{s-\tau_1} + \beta_1\, p^{s-\tau_1-1} + 1 \le j \le p^s - p^{s-\tau_1} + (\beta_1+1)p^{s-\tau_1-1}$, $p^s - p^{s-\tau_2} + \beta_2\, p^{s-\tau_2-1} + 1 \le u \le p^s - p^{s-\tau_2} + (\beta_2+1)p^{s-\tau_2-1}$. *Then* $\mathrm{d_H}(\mathcal{C}) = \min\{2(\beta_1+2)p^{\tau_1}, 4(\beta_2+2)p^{\tau_2}\}$.

Lemma 5.8: Let $u \le j \le i$ *be integers with* $i = j = p^s$, $p^s - p^{s-\tau_2} + \beta_2\, p^{s-\tau_2-1} + 1 \le u \le p^s - p^{s-\tau_2} + (\beta_2+1)p^{s-\tau_2-1}$. *Then* $\mathrm{d_H}(\mathcal{C}) = 4(\beta_2+2)p^{\tau_2}$.

Now, we summarize the Hamming distances $\mathrm{d_H}(\mathcal{C})$ for the case $0 \le u \le j \le i \le p^s$ as follows.

Theorem 5.9: Assume that $0 \le \beta_0, \beta_1, \beta_2 \le p-2$, *and* $0 \le \tau_2 \le \tau_1 \le \tau_0 \le s-1$. *Let* $0 \le u \le j \le i \le p^s$. *Then the codes* $\mathcal{C} = \langle (x-1)^i (x^2-(\epsilon+\epsilon^4)x+1)^j (x^2-(\epsilon^2+\epsilon^3)x+1)^u \rangle$ *have the following Hamming distances:*

$$\mathrm{d_H}(\mathcal{C}) = \begin{cases} 1, & \text{if } i=j=u=0, \\ 2, & \text{if } u=j=0 \text{ and } 0<i\le p^s, \\ & \text{or } u=0 \text{ and } 0<j\le i\le p^{s-1}, \\ 3, & \text{if } u=0,\ 0<j\le 2p^{s-1} \\ & \text{and } p^{s-1}<i\le 2p^{s-1}, \\ 4, & \text{if } u=0,\ 0<j\le p^s \text{ and } 2p^{s-1}<i\le p^s, \\ \min\{(\beta_0+2)p^{\tau_0}, & \text{if } p^s-p^{s-\tau_0}+\beta_0\, p^{s-\tau_0-1}+1\le i\le p^s \\ 2(\beta_1+2)p^{\tau_1}, & -p^{s-\tau_0}+(\beta_0+1)p^{s-\tau_0-1}, \\ 4(\beta_2+2)p^{\tau_2}\}, & p^s-p^{s-\tau_1}+\beta_1\, p^{s-\tau_1-1}+1\le j\le p^s \\ & -p^{s-\tau_1}+(\beta_1+1)p^{s-\tau_1-1}, \\ & p^s-p^{s-\tau_2}+\beta_2\, p^{s-\tau_2-1}+1\le u\le p^s \\ & -p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1}, \\ \min\{2(\beta_1+2)p^{\tau_1}, & \text{if } i=p^s, \\ 4(\beta_2+2)p^{\tau_2}\}, & p^s-p^{s-\tau_1}+\beta_1\, p^{s-\tau_1-1}+1\le j\le p^s \\ & -p^{s-\tau_1}+(\beta_1+1)p^{s-\tau_1-1}, \\ & p^s-p^{s-\tau_2}+\beta_2\, p^{s-\tau_2-1}+1\le u\le p^s \\ & -p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1}, \\ 4(\beta_2+2)p^{\tau_2}, & \text{if } i=j=p^s, \\ & p^s-p^{s-\tau_2}+\beta_2\, p^{s-\tau_2-1}+1\le u\le p^s \\ & -p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1}, \\ 0, & \text{if } i=j=u=p^s. \end{cases}$$

Example 5.10: Let $p = 7$, $i = 3$, $j = 1$ and $u = 0$, then $\mathcal{C}$ is a $[35, 30, 4]$ code by Theorem 5.9, which is optimal respect to the tables of best codes known maintained at http://www.codetables.de.

Remark 5.11: Using the above technique, it is easy to check that the corresponding case $0 \le j \le u \le i \le p^s$ *has the same Hamming distances as the case* $0 \le u \le j \le i \le p^s$. *For example, in case* $0 \le j \le u \le i \le p^s$, *if* $i = u = p^s$ *and* $p^s - p^{s-\tau_2} + \beta_2\, p^{s-\tau_2-1} + 1 \le j \le p^s - p^{s-\tau_2} + (\beta_2+1)p^{s-\tau_2-1}$, *the Hamming distance* $\mathrm{d_H}(\mathcal{C})$ *is* $4(\beta_2+2)p^{\tau_2}$.

We now state the Hamming distances of $\mathcal{C}$ for the case $0 \le u \le i \le j \le p^s$. Using the same argument as Lemmas 5.5 to 5.8, combining with Proposition 5.3, the Hamming distances

of $\mathcal{C}$ are easy to obtain for this case. We summarize the result here.

Theorem 5.12: Assume that $0 \le \beta_0, \beta_1, \beta_2 \le p-2$, *and* $0 \le \tau_2 \le \tau_1 \le \tau_0 \le s-1$. *Let* $0 \le u \le i \le j \le p^s$. *Then the codes* $\mathcal{C} = \langle (x-1)^i (x^2-(\epsilon+\epsilon^4)x+1)^j (x^2-(\epsilon^2+\epsilon^3)x+1)^u \rangle$ *have the following Hamming distances:*

$$
\mathrm{d_H}(\mathcal{C}) = \begin{cases}
1, & \text{if } i=j=u=0,\\
2, & \text{if } u=0 \text{ and } 0<i\le j\le p^{s-1},\\
3, & \text{if } u=i=0 \text{ and } p^{s-1}<j\le p^s, \text{ or } u=0,\\
 & 0<i\le 2p^{s-1} \text{ and } p^{s-1}<j\le 2p^{s-1},\\
4, & \text{if } u=0,\ 0<i\le p^s \text{ and } 2p^{s-1}<j\le p^s,\\
\min\{(\beta_0+2)p^{\tau_0}, & \text{if } p^s-p^{s-\tau_0}+\beta_0 p^{s-\tau_0-1}+1\le j\le p^s\\
3(\beta_1+2)p^{\tau_1}, & -p^{s-\tau_0}+(\beta_0+1)p^{s-\tau_0-1},\\
4(\beta_2+2)p^{\tau_2}\}, & p^s-p^{s-\tau_1}+\beta_1 p^{s-\tau_1-1}+1\le i\le p^s\\
 & -p^{s-\tau_1}+(\beta_1+1)p^{s-\tau_1-1},\\
 & p^s-p^{s-\tau_2}+\beta_2 p^{s-\tau_2-1}+1\le u\le p^s\\
 & -p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1},\\
\min\{3(\beta_1+2)p^{\tau_1}, & \text{if } j=p^s,\\
4(\beta_2+2)p^{\tau_2}\}, & p^s-p^{s-\tau_1}+\beta_1 p^{s-\tau_1-1}+1\le i\le p^s\\
 & -p^{s-\tau_1}+(\beta_1+1)p^{s-\tau_1-1},\\
 & p^s-p^{s-\tau_2}+\beta_2 p^{s-\tau_2-1}+1\le u\le p^s\\
 & -p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1},\\
4(\beta_2+2)p^{\tau_2}, & \text{if } i=j=p^s,\\
 & p^s-p^{s-\tau_2}+\beta_2 p^{s-\tau_2-1}+1\le u\le p^s\\
 & -p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1},\\
0, & \text{if } i=j=u=p^s.
\end{cases}
$$

Example 5.13: Let $p=7, j=2$ and $i=u=0$, then $\mathcal{C}$ is a $[35, 31, 3]$ code by Theorem 5.12, which is optimal respect to the tables of best codes known maintained at http://www.codetables.de.

Remark 5.14: Using the above technique, it is easy to check that the corresponding case $0 \le j \le i \le u \le p^s$ *has the same Hamming distances as the case* $0 \le u \le i \le j \le p^s$. *For example, in case* $0 \le j \le i \le u \le p^s$, *if* $i=u=p^s$ *and* $p^s-p^{s-\tau_2}+\beta_2 p^{s-\tau_2-1}+1 \le j \le p^s-p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1}$, *the Hamming distance* $\mathrm{d_H}(\mathcal{C})$ *is* $4(\beta_2+2)p^{\tau_2}$.

We here state the Hamming distances of $\mathcal{C}$ for the case $0 \le i \le j \le u \le p^s$. Using the same way as Lemmas 5.5 to 5.8, combining with Proposition 5.4, the Hamming distance of $\mathcal{C}$ for this case also can be obtained. We summarize the result in the following theorem.

Theorem 5.15: Assume that $0 \le \beta_0, \beta_1, \beta_2 \le p-2$, *and* $0 \le \tau_2 \le \tau_1 \le \tau_0 \le s-1$. *Let* $0 \le i \le j \le u \le p^s$. *Then the codes* $\mathcal{C} = \langle (x-1)^i (x^2-(\epsilon+\epsilon^4)x+1)^j (x^2-(\epsilon^2+\epsilon^3)x+1)^u \rangle$ *have the following Hamming distances:*

$$
\mathrm{d_H}(\mathcal{C}) = \begin{cases}
1, & \text{if } i=j=u=0,\\
2, & \text{if } i=0 \text{ and } 0<j\le u\le p^{s-1},\\
3, & \text{if } j=i=0 \text{ and } p^{s-1}<u\le 2p^{s-1},\\
 & \tilde{o}r\ i=0,\ 0\le j\le 2p^{s-1}\\
 & \text{and } p^{s-1}<u\le 2p^{s-1},\\
4, & \text{if } i=0,\ 0<j\le 3p^{s-1}\\
 & \text{and } 2p^{s-1}<u\le 3p^{s-1},\\
5, & \text{if } i=0,\ 0<j\le p^s \text{ and } 3p^{s-1}<u\le p^s,\\
\min\{(\beta_0+2)p^{\tau_0}, & \text{if } p^s-p^{s-\tau_0}+\beta_0 p^{s-\tau_0-1}+1\le u\le p^s\\
3(\beta_1+2)p^{\tau_1}, & -p^{s-\tau_0}+(\beta_0+1)p^{s-\tau_0-1},\\
5(\beta_2+2)p^{\tau_2}\}, & p^s-p^{s-\tau_1}+\beta_1 p^{s-\tau_1-1}+1\le j\le p^s\\
 & -p^{s-\tau_1}+(\beta_1+1)p^{s-\tau_1-1},\\
 & p^s-p^{s-\tau_2}+\beta_2 p^{s-\tau_2-1}+1\le i\le p^s\\
 & -p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1},\\
\min\{3(\beta_1+2)p^{\tau_1}, & \text{if } u=p^s,\\
5(\beta_2+2)p^{\tau_2}\}, & p^s-p^{s-\tau_1}+\beta_1 p^{s-\tau_1-1}+1\le j\le p^s\\
 & -p^{s-\tau_1}+(\beta_1+1)p^{s-\tau_1-1},\\
 & p^s-p^{s-\tau_2}+\beta_2 p^{s-\tau_2-1}+1\le i\le p^s\\
 & -p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1},\\
5(\beta_2+2)p^{\tau_2}, & \text{if } j=u=p^s,\\
 & p^s-p^{s-\tau_2}+\beta_2 p^{s-\tau_2-1}+1\le i\le p^s\\
 & -p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1},\\
0, & \text{if } i=j=u=p^s.
\end{cases}
$$

Example 5.16: Let $p=7, i=0\, j=1$ and $u=4$, then $\mathcal{C}$ is a $[35, 25, 5]$ code by Theorem 5.15.

Remark 5.17: Using the above technique, it is easy to check that the corresponding case $0 \le i \le u \le j \le p^s$ *has the same Hamming distances as the case* $0 \le i \le j \le u \le p^s$. *For example, in case* $0 \le i \le u \le j \le p^s$, *if* $j=u=p^s$ *and* $p^s-p^{s-\tau_2}+\beta_2 p^{s-\tau_2-1}+1 \le i \le p^s-p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1}$, *the Hamming distance* $\mathrm{d_H}(\mathcal{C})$ *is* $5(\beta_2+2)p^{\tau_2}$.

5.2 Case 2

Here, we consider the Hamming distances of $\mathcal{C} = \langle (x-1)^i (x^4+x^3+x^2+x+1)^j \rangle$. Let $e_{z,t}=1$ if $t>z$, otherwise, $e_{z,t}=0$, where $t=i,j$ and $1 \le z \le p^s-1$. Then the generator polynomial of simple-root γ-constacyclic code $\bar{\mathcal{C}}_z$ can be expressed as

$$\bar{g}_z(x) = (x-1)^{e_{i,z}} (x^4+x^3+x^2+x+1)^{e_{j,z}}.$$

Clearly, if $i \le z < j$, then $\bar{g}_z(x) = x^4+x^3+x^2+x+1$ and the elements of $\bar{\mathcal{C}}_z$ are precisely $r(x^4+x^3+x^2+x+1)$, where $r \in \mathbb{F}_{p^m}$. It follows that

$$\mathrm{d_H}(\bar{\mathcal{C}}_z) = \begin{cases} 1, & \text{if } i \le j \le z,\\ 4, & \text{if } i \le z < j. \end{cases} \tag{10}$$

Similarly, if $j \le z < i$, then $\bar{g}_z(x) = x - 1$. By Lemma 2.2, we have

$$\mathrm{d_H}(\bar{\mathcal{C}}_z) = \begin{cases} 1, & \text{if } j \le i \le z, \\ 2, & \text{if } j \le z < i. \end{cases} \tag{11}$$

Using the same technique for us to prove Theorem 5.15, combining with (10) and (11), the Hamming distances of $\mathcal{C} = \langle (x-1)^i (x^4+x^3+x^2+x+1)^j \rangle$ are given as follows.

Theorem 5.18: Assume that $0 \le \beta_0, \beta_1 \le p-2$, and $0 \le \tau_1 \le \tau_0 \le s-1$. Let $0 \le j \le i \le p^s$. Then the codes $\mathcal{C} = \langle (x-1)^i (x^4+x^3+x^2+x+1)^j \rangle$ have the following Hamming distances:

$$\mathrm{d_H}(\mathcal{C}) = \begin{cases} 1, & \text{if } i=j=0, \\ 2, & \text{if } j=0 \text{ and } 0 < i \le p^s, \\ \min\{(\beta_0+2)p^{\tau_0}, & \text{if } p^s - p^{s-\tau_0} + \beta_0 p^{s-\tau_0-1} + 1 \le i \le p^s \\ 2(\beta_1+2)p^{\tau_1}\}, & \quad -p^{s-\tau_0} + (\beta_0+1)p^{s-\tau_0-1}, \\ & p^s - p^{s-\tau_1} + \beta_1 p^{s-\tau_1-1} + 1 \le j \le p^s \\ & \quad -p^{s-\tau_1} + (\beta_1+1)p^{s-\tau_1-1}, \\ 2(\beta_1+2)p^{\tau_1}, & \text{if } j = p^s, \\ & p^s - p^{s-\tau_1} + \beta_1 p^{s-\tau_1-1} + 1 \le i \le p^s \\ & \quad -p^{s-\tau_1} + (\beta_1+1)p^{s-\tau_1-1}, \\ 0, & \text{if } i=j=p^s. \end{cases}$$

Example 5.19: Let $p = 7$, $i = 2$ and $j = 1$, then $\mathcal{C}$ is a [35, 29, 3] code by Theorem 5.18.

Theorem 5.20: Assume that $0 \le \beta_0, \beta_1 \le p-2$, and $0 \le \tau_1 \le \tau_0 \le s-1$. Let $0 \le i \le j \le p^s$. Then the codes $\mathcal{C} = \langle (x-1)^i (x^4+x^3+x^2+x+1)^j \rangle$ have the following Hamming distances:

$$\mathrm{d_H}(\mathcal{C}) = \begin{cases} 1, & \text{if } i=j=0, \\ 2, & \text{if } i=0 \text{ and } 0 < j \le p^{s-1}, \\ 3, & \text{if } i=0 \text{ and } p^{s-1} < j \le 2p^{s-1}, \\ 4, & \text{if } i=0 \text{ and } 2p^{s-1} < j \le 3p^{s-1}, \\ 5, & \text{if } i=0 \text{ and } 3p^{s-1} < j \le p^s, \\ \min\{(\beta_0+2)p^{\tau_0}, & \text{if } p^s - p^{s-\tau_0} + \beta_0 p^{s-\tau_0-1} + 1 \le i \le p^s \\ 5(\beta_1+2)p^{\tau_1}\}, & \quad -p^{s-\tau_0} + (\beta_0+1)p^{s-\tau_0-1}, \\ & p^s - p^{s-\tau_1} + \beta_1 p^{s-\tau_1-1} + 1 \le j \le p^s \\ & \quad -p^{s-\tau_1} + (\beta_1+1)p^{s-\tau_1-1}, \\ 5(\beta_1+2)p^{\tau_1}, & \text{if } j = p^s, \\ & p^s - p^{s-\tau_1} + \beta_1 p^{s-\tau_1-1} + 1 \le i \le p^s \\ & \quad -p^{s-\tau_1} + (\beta_1+1)p^{s-\tau_1-1}, \\ 0, & \text{if } i=j=p^s. \end{cases}$$

Example 5.21: Let $p = 7$, $i = 0$ and $j = 4$, then $\mathcal{C}$ is a [35, 19, 5] code by Theorem 5.20.

5.3 Case 3

We now consider the Hamming distances of $\mathcal{C} = \langle (x-1)^i (x-\varepsilon)^j (x-\varepsilon^2)^y (x-\varepsilon^3)^u (x-\varepsilon^4)^v \rangle$, where $\varepsilon \in \mathbb{F}_{p^m}$ is a 5th root of unity. Recall that $e_{z,t} = 1$ if $t > z$, otherwise, $e_{z,t} = 0$, where $t = i, j, y, u$, or v and $1 \le z \le p^s - 1$. Then the generator polynomial of simple-root γ-constacyclic code $\bar{\mathcal{C}}_z$ can be expressed as

$$\bar{g}_z(x) = (x-1)^{e_{i,t}} (x-\varepsilon)^{e_{j,t}} (x-\varepsilon^2)^{e_{y,t}} (x-\varepsilon^3)^{e_{u,t}} (x-\varepsilon^4)^{e_{v,t}}, \tag{12}$$

where $\bar{\mathcal{C}}_z$ is defined in Theorem 3.2. In order to determine the Hamming distances of $\mathcal{C}$, we first consider the Hamming distances of $\bar{\mathcal{C}}_z$ for the case $0 \le v \le u \le y \le j \le i \le p^s$.

Proposition 5.22: Assume $0 \le v \le u \le y \le j \le i \le p^s$. Let $\bar{\mathcal{C}}_z = \langle \bar{g}_z(x) \rangle$ be a γ-constacyclic code of length 5 over $\mathbb{F}_{p^m}$, where $\bar{g}_z(x)$ is defined in (12). Then

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

Proof: We consider five cases.

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

Case 2: $v \le u \le y \le j \le z < i$. In this case, obviously, $\bar{\mathcal{C}}_z = \langle x-1 \rangle$. Then, by Lemma 2.2, $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 2$.

Case 3: $v \le u \le y \le z < j \le i$. In this case, we have $\bar{\mathcal{C}}_z = \langle (x-1)(x-\varepsilon) \rangle$. By the same way as **Case 2** of Proposition 5.3, we get $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 3$.

Case 4: $v \le u \le z < y \le j \le i$. In this case, we get $\bar{\mathcal{C}}_z = \langle (x-1)(x-\varepsilon)(x-\varepsilon^2) \rangle$. By the same argument as **Case 3** of Proposition 5.2, we have $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 4$.

Case 5: $v \le z < u \le y \le j \le i$. In this case, we obtain $\bar{\mathcal{C}}_z = \langle (x-1)(x-\varepsilon)(x-\varepsilon^2)(x-\varepsilon^3) \rangle$. In this case, obviously, the elements of $\bar{\mathcal{C}}_z$ are precisely $r(x-1)(x-\varepsilon)(x-\varepsilon^2)(x-\varepsilon^3)$, where $r \in \mathbb{F}_{p^m}$. So, $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 5$.

Combining all the cases, the result follows. □

We now compute the Hamming distances of $\mathcal{C}$ for the case $0 \le v \le u \le k \le j \le i \le p^s$. Firstly, we consider the case for $v = 0$.

Lemma 5.23: Let $v = 0$ and $0 \le u \le y \le j \le i \le p^s$ be integers. Then,

$$\mathrm{d_H}(\mathcal{C}) = \begin{cases} 1, & \text{if } i=j=y=u=0, \\ 2, & \text{if } j=y=u=0 \text{ and } 0 < i \le p^s, \text{ or} \\ & \quad 0 \le u \le y \le j \le i \le p^{s-1} \\ & \quad \text{(but not } i=j=y=u=0), \\ 3, & \text{if } y=u=0,\ 0 < j \le p^s \text{ and } p^{s-1} < i \le p^s, \text{ or} \\ & \quad 0 \le u \le y \le 2p^{s-1},\ 0 < j \le 2p^{s-1} \\ & \quad \text{and } p^{s-1} < i \le 2p^{s-1}, \\ 4, & \text{if } u=0,\ 0 < y \le j \le p^s \text{ and } 2p^{s-1} < i \le p^s, \text{ or} \\ & \quad 0 < u \le y \le j \le 3p^{s-1} \text{ and } 2p^{s-1} < i \le 3p^{s-1}, \\ & \quad \text{or } 0 < u \le y \le j \le p^{s-1} \text{ and } 2p^{s-1} < i \le p^s, \\ 5, & \text{if } 0 < u \le y \le p^s,\ p^{s-1} < j \le p^s \\ & \quad \text{and } 3p^{s-1} < i \le p^s. \end{cases}$$

Proof: By Theorem 3.2 and Proposition 5.22, we have

$$\begin{aligned}\mathrm{d_H}(\mathcal{C}) &= \min\{\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\,|\,0\le z\le p^s-1\}\\ &\le \mathrm{wt_H}((x^5-\gamma)^0)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_0)\\ &\le 5.\end{aligned}$$

So, $\mathrm{d_H}(\mathcal{C}) = 1, 2, 3, 4$ or 5. Thus, we only need to find out what values of i, j, y, u such that $\mathrm{d_H}(\mathcal{C}) = 1, 2, 3$ or 4 (the remaining values of i, j, y, u will give $\mathrm{d_H}(\mathcal{C}) = 4$.) We consider two cases.

Case 1: $z = 0$. In this case, by Proposition 5.22, we have

$$\mathrm{wt_H}((x^5-\gamma)^0)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_0) = \begin{cases}1, & \text{if } i=j=y=u=0,\\ 2, & \text{if } j=y=u=0 \text{ and } 0<i\le p^s,\\ 3, & \text{if } y=u=0 \text{ and } 0<j\le i\le p^s,\\ 4, & \text{if } u=0 \text{ and } 0<y\le j\le i\le p^s\end{cases} \tag{13}$$

and $\mathrm{wt_H}((x^5-\gamma)^0)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_0) = 5$ for the other values of i, j, y, u.

Case 2: $1 \le z \le p^s - 1$. There are five possibilities.

Case 2.1: $u \le y \le j \le i \le z$. From Proposition 5.22, we get $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 1$. By Lemma 2.6, we obtain

$$\begin{aligned}&\min\{\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\mid 0<z\le p^{s-1}\} = 2,\\ &\min\{\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\mid p^{s-1}<z\le 2p^{s-1}\} = 3,\\ &\min\{\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\mid 2p^{s-1}<z\le 3p^{s-1}\} = 4,\end{aligned}$$

and

$$\min\{\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\mid 3p^{s-1}<z\le p^s-1\}\ge 5.$$

Case 2.2: $u \le y \le j \le z < i$. From Proposition 5.22, clearly, $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 2$. By Lemma 2.6, we have

$$\min\{\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\mid 0<z\le p^{s-1}\} = 4,$$

and

$$\min\{\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\mid 3p^{s-1}<z\le p^s-1\}\ge 6.$$

Case 2.3: $u \le y \le z < j \le i$. From Proposition 5.22, obviously, $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 3$. By Lemma 2.6, we obtain $\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \ge 3\,\mathrm{wt_H}((x^5-\gamma)^z) \ge 6$ for any $1 \le z \le p^s - 1$.

Case 2.4: $u \le z < y \le j \le i$. From Proposition 5.22, clearly, $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 4$. By Lemma 2.6, we have $\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \ge 4\,\mathrm{wt_H}((x^5-\gamma)^z) \ge 8$ for any $1 \le z \le p^s - 1$.

Case 2.5: $u \le z < y \le j \le i$. From Proposition 5.22, we get $\mathrm{d_H}(\bar{\mathcal{C}}_z) = 5$. By Lemma 2.6, we obtain $\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \ge 5\,\mathrm{wt_H}((x^5-\gamma)^z) \ge 10$ for any $1 \le z \le p^s - 1$.

Therefore, combining with **Cases 2.1-2.5**, we get

$$\min\{\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z)\,|\,1\le z\le p^s-1\} = \begin{cases}2, & \text{if } 0\le u\le y\le j\le i\le p^{s-1},\\ 3, & \text{if } 0\le u\le y\le j\le 2p^{s-1}\\ & \quad \text{and } p^{s-1}<i\le 2p^{s-1},\\ 4, & \text{if } 0\le u\le y\le j\le 3p^{s-1}\\ & \quad \text{and } 2p^{s-1}<i\le 3p^{s-1},\\ & \text{õr } 0\le u\le y\le j\le p^{s-1}\\ & \quad \text{and } 3p^{s-1}<i\le p^s\end{cases} \tag{14}$$

$$\mathrm{d_H}(\mathcal{C}) = \begin{cases}1, & \text{if } i=j=y=u=v=0,\\ 2, & \text{if } j=y=u=v=0 \text{ and } 0<i\le p^s,\\ & \text{or } 0\le v\le u\le y\le j\le i\le p^{s-1}\\ & \text{(but not } i=j=y=u=v=0),\\ 3, & \text{if } y=u=v=0,\ 0<j\le p^s\\ & \text{and } p^{s-1}<i\le p^s, \text{ or } v=0,\\ & 0\le u\le y\le 2p^{s-1},\ 0<j\le 2p^{s-1}\\ & \text{and } p^{s-1}<i\le 2p^{s-1},\\ 4, & \text{if } u=v=0,\ 0<y\le j\le p^s \text{ and}\\ & 2p^{s-1}<i\le p^s, \text{ or } v=0,\\ & 0<u\le y\le j\le 3p^{s-1} \text{ and}\\ & 2p^{s-1}<i\le 3p^{s-1}, \text{ or } v=0,\ 0<u\le\\ & y\le j\le p^{s-1} \text{ and } 2p^{s-1}<i\le p^s,\\ 5, & \text{if } v=0,\ 0<u\le y\le p^s,\ p^{s-1}<j\le p^s\\ & \text{and } 3p^{s-1}<i\le p^s,\\ & \min\{(\beta_0+2)p^{\tau_0},\\ & \quad \text{if } p^s-p^{s-\tau_0}+\beta_0\,p^{s-\tau_0-1}+1\le i\le p^s\\ & 2(\beta_1+2)p^{\tau_1}, \quad -p^{s-\tau_0}+(\beta_0+1)p^{s-\tau_0-1},\\ & 3(\beta_2+2)p^{\tau_2}, \quad p^s-p^{s-\tau_1}+\beta_1\,p^{s-\tau_1-1}+1\le j\le p^s\\ & 4(\beta_3+2)p^{\tau_3}, \quad -p^{s-\tau_1}+(\beta_1+1)p^{s-\tau_1-1},\\ & 5(\beta_4+2)p^{\tau_4}\}, \quad p^s-p^{s-\tau_2}+\beta_2\,p^{s-\tau_2-1}+1\le y\le p^s\\ & \quad -p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1},\\ & \quad p^s-p^{s-\tau_3}+\beta_3\,p^{s-\tau_3-1}+1\le u\le p^s\\ & \quad -p^{s-\tau_3}+(\beta_3+1)p^{s-\tau_3-1},\\ & \quad p^s-p^{s-\tau_4}+\beta_4\,p^{s-\tau_4-1}+1\le v\le p^s\\ & \quad -p^{s-\tau_4}+(\beta_4+1)p^{s-\tau_4-1},\\ & \min\{2(\beta_1+2)p^{\tau_1}, \quad \text{if } i=p^s,\\ & 3(\beta_2+2)p^{\tau_2}, \quad p^s-p^{s-\tau_1}+\beta_1\,p^{s-\tau_1-1}+1\le j\le p^s\\ & 4(\beta_3+2)p^{\tau_3}, \quad -p^{s-\tau_1}+(\beta_1+1)p^{s-\tau_1-1},\\ & 5(\beta_4+2)p^{\tau_4}\}, \quad p^s-p^{s-\tau_2}+\beta_2\,p^{s-\tau_2-1}+1\le y\le p^s\\ & \quad -p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1},\\ & \quad p^s-p^{s-\tau_3}+\beta_3\,p^{s-\tau_3-1}+1\le u\le p^s\\ & \quad -p^{s-\tau_3}+(\beta_3+1)p^{s-\tau_3-1},\\ & \quad p^s-p^{s-\tau_4}+\beta_4\,p^{s-\tau_4-1}+1\le v\le p^s\\ & \quad -p^{s-\tau_4}+(\beta_4+1)p^{s-\tau_4-1},\\ & \min\{3(\beta_1+2)p^{\tau_1}, \quad \text{if } i=j=p^s,\\ & 4(\beta_2+2)p^{\tau_2}, \quad p^s-p^{s-\tau_2}+\beta_2\,p^{s-\tau_2-1}+1\le y\le p^s\\ & 5(\beta_4+2)p^{\tau_4}\}, \quad -p^{s-\tau_2}+(\beta_2+1)p^{s-\tau_2-1},\\ & \quad p^s-p^{s-\tau_3}+\beta_3\,p^{s-\tau_3-1}+1\le u\le p^s\\ & \quad -p^{s-\tau_3}+(\beta_3+1)p^{s-\tau_3-1},\\ & \quad p^s-p^{s-\tau_4}+\beta_4\,p^{s-\tau_4-1}+1\le v\le p^s\\ & \quad -p^{s-\tau_4}+(\beta_4+1)p^{s-\tau_4-1},\\ & \min\{4(\beta_2+2)p^{\tau_2}, \quad \text{if } i=j=y=p^s,\\ & 5(\beta_4+2)p^{\tau_4}\}, \quad p^s-p^{s-\tau_3}+\beta_3\,p^{s-\tau_3-1}+1\le u\le p^s\\ & \quad -p^{s-\tau_3}+(\beta_3+1)p^{s-\tau_3-1},\\ & \quad p^s-p^{s-\tau_4}+\beta_4\,p^{s-\tau_4-1}+1\le v\le p^s\\ & \quad -p^{s-\tau_4}+(\beta_4+1)p^{s-\tau_4-1},\\ & 5(\beta_4+2)p^{\tau_4}, \quad \text{if } i=j=y=u=p^s,\\ & \quad p^s-p^{s-\tau_4}+\beta_4\,p^{s-\tau_4-1}+1\le v\le p^s\\ & \quad -p^{s-\tau_4}+(\beta_4+1)p^{s-\tau_4-1},\\ 0, & \text{if } i=j=y=u=v=p^s\end{cases}$$

and $\mathrm{wt_H}((x^5-\gamma)^z)\cdot \mathrm{d_H}(\bar{\mathcal{C}}_z) \geq 5$ for the other values of i, j, y, u.

Combining with Theorem 3.2, (13) and (14), the result follows. □

Using the same technique as Lemma 5.6, we can obtain the Hamming distances of

$$\mathcal{C} = \left\langle (x-1)^i(x-\varepsilon)^j(x-\varepsilon^2)^y(x-\varepsilon^3)^u(x-\varepsilon^4)^v \right\rangle$$

for the case $0 < v \leq u \leq y \leq j \leq i \leq p^s$, immediately. So, we omit the proof.

Combining Lemma 5.23, we now summary the Hamming distances of $\mathcal{C}$ for the case $0 \leq v \leq u \leq k \leq j \leq i \leq p^s$ as follows.

Theorem 5.24: Assume that $0 \leq \beta_0, \beta_1, \beta_2, \beta_3, \beta_4 \leq p-2$, *and* $0 \leq \tau_4 \leq \tau_3 \leq \tau_2 \leq \tau_1 \leq \tau_0 \leq s-1$. *Let* $0 \leq v \leq u \leq y \leq j \leq i \leq p^s$. *Then the codes* $\mathcal{C} = \left\langle (x-1)^i(x-\varepsilon)^j(x-\varepsilon^2)^k(x-\varepsilon^3)^u(x-\varepsilon^4)^v \right\rangle$ *have the following Hamming distances* $\mathrm{d_H}(\mathcal{C})$, *as shown at the previous page.*

Example 5.25: Let $p = 7$, $i = 4$, $j = 2$ $y = u = 1$ and $v = 0$, then $\mathcal{C}$ is a $[35, 27, 5]$ code by Theorem 5.24, which is almost optimal respect to the tables of best codes known maintained at http://www.codetables.de.

Remark 5.26: Using the above technique, it is easy to check that the other corresponding cases for the codes $\mathcal{C} = \left\langle (x-1)^i(x-\varepsilon)^j(x-\varepsilon^2)^y(x-\varepsilon^3)^u(x-\varepsilon^4)^v \right\rangle$ *have the same Hamming distances as the case* $0 \leq v \leq u \leq y \leq j \leq i \leq p^s$. *For example, in case* $0 \leq i \leq j \leq y \leq u \leq v \leq p^s$, *if* $j = y = u = v = p^s$ *and* $p^s - p^{s-\tau_4} + \beta_4\, p^{s-\tau_4-1} + 1 \leq i \leq p^s - p^{s-\tau_4} + (\beta_4+1)p^{s-\tau_4-1}$, *the Hamming distance* $\mathrm{d_H}(\mathcal{C})$ *is* $5(\beta_4+2)p^{\tau_4}$.

VI. CONCLUSION

Determining the Hamming distances of constacyclic codes and obtaining MDS constacyclic codes are very important in error-correcting coding theory. However, not much work has been done on them as they are very difficult tasks in general. In this paper, based on the relationships about the Hamming distances between simple-root constacyclic codes and repeated-root constacyclic codes, and the algebraic structures of repeated-root constacyclic codes of length ℓp^s, where ℓ is a prime, the algebraic structures of constacyclic codes of length $5\ p^s$ are provided explicitly. Among other result, the necessary and sufficient conditions for the existence of self-dual, self-orthogonal and dual containing code and the Hamming distances of all such constacyclic codes are given. Moreover, we obtained that a repeated-root constacyclic code of length lp^s is an MDS code if and only if the degree i of the generator polynomial of this code is $0 \leq i \leq p-1$ for the case $l = s = 1$, and the degree of the generator polynomial of this code is 0, 1 or $lp^s - 1$ for the case $l \geq 2$. As a future work, taking quantum synchronizable codes from repeated-root constacyclic codes of length $5p^s$ is interesting.

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 paper.

REFERENCES

[1] G. K. Bakshi and M. Raka, "A class of constacyclic codes over a finite field," *Finite Fields Their Appl.*, vol. 18, no. 2, pp. 362–377, Mar. 2012.

[2] 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.

[3] B. Chen, H. Q. Dinh, and H. Liu, "Repeated-root constacyclic codes of length ℓps and their duals," *Discrete Appl. Math.*, vol. 177, pp. 60–70, Nov. 2014.

[4] B. Chen, H. Q. Dinh, and H. Liu, "Repeated-root constacyclic codes of length $2\ell^m p^n$," *Finite Fields Appl.*, vol. 33, pp. 137–159, May 2015.

[5] B. Chen and H. Q. Dinh, "Equivalence classes and structures of constacyclic codes over finite fields," *AMS Contemp. Math.*, vol. 642, pp. 181–223, Jun. 2015.

[6] 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.

[7] H. Q. Dinh, "Repeated-root constacyclic codes of length $2p^s$," *Finite Fields Appl.*, vol. 18, pp. 133–143, Jan. 2012.

[8] H. Q. Dinh, "Structure of repeated-root constacyclic codes of length $3p^s$ and their duals," *Discrete Math.*, vol. 313, no. 9, pp. 983–991, May 2013.

[9] H. Q. Dinh, "On repeated-root constacyclic codes of length $4p^s$," *Asian Eur. J. Math*, vol. 6, Jun. 2013, Art. no. 1350020.

[10] 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.

[11] H. Q. Dinh, "Repeated-root constacyclic codes of prime power length," *AMS Contemp. Math.*, vol. 480, pp. 87–100, Jun. 2009.

[12] H. Q. Dinh, X. Wang, H. Liu, and W. Yamaka, "Hamming distances of constacyclic codes of length $3p^s$ and optimal codes with respect to the Griesmer and Singleton bounds," to be published.

[13] H. Q. Dinh, X. Wang, H. Liu, and S. Sriboonchitta, "On the Hamming distances of repeated-root constacyclic codes of length $4p^s$," *Discrete Math.*, vol. 342, no. 5, pp. 1456–1470, May 2019.

[14] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[15] L. Liu, L. Q. Li, X. S. Kai, and S. X. Zhu, "Repeated-root constacyclic codes of length $3lp^n$ and their dual codes," *Finite Fields Appl.*, vol. 42, pp. 269–295, Nov. 2016.

[16] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[17] S. R. López-Permouth, H. Özadam, F. Özbudak, and S. Szabo, "Polycyclic codes over galois rings with applications to repeated-root constacyclic codes," *Finite Fields Their Appl.*, vol. 19, no. 1, pp. 16–38, Jan. 2013.

[18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 10th ed. Amsterdam, The Netherlands: North Holland, 1998.

[19] 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.

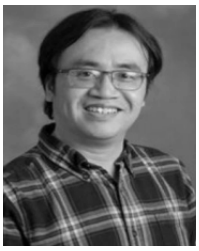
[20] H. Özadam and F. Özbudak, "The minimum Hamming distance of cyclic codes of length $2p^s$," *Appl. Algebra Engrg. Commun. Comput.*, vol. 5527, pp. 92–100, Jun. 2009.

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

[22] A. Sharma and S. Rani, "Repeated-root constacyclic codes of length $4\ell^m p^n$," *Finite Fields Appl.*, vol. 40, pp. 163–200, Jul. 2016.

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

[24] 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 as a Visiting Professor at North Dakota State University, USA, for one year. Since 2004, he has been working as the tenure Professor of mathematics at Kent State University, USA. He is currently a Professor of applied mathematics with the Department of Mathematical Sciences, Kent State University. Since 2004, he has 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 on INFORMATION THEORY, the IEEE COMMUNICATIONS 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 been a well-known invited/keynote speaker at numerous international conferences and mathematics colloquium. Other than universities in the U.S., 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 10 articles in high ranked peer review journals, such as *Designs, Codes and Cryptography*, *Discrete Mathematics*, and *Finite Fields and Their Applications*.

JIRAKOM SIRISRISAKULCHAI has a solid knowledge on econometrics and economics, specifically information and entropy econometrics. He started his research career by doing research on National Road Safety Policy Analysis. After he finished three road safety research projects, he has enhanced his research experience to Thailand Demand Response Initiative Projects (demand-side management for electricity systems). He is currently working on impact assessment for several (innovative) research projects funded by the Thailand Research Fund. As a member of the Center of Excellence in Econometrics, he aims to use the power of econometrics in economic applications and policies in the hope of promoting Thailand to be developed country.