ON THE HAMMING DISTANCES OF CONSTACYCLIC CODES OF LENGTH $7p^s$ OVER $\mathbb{F}_{p^m}$

Hai Q. Dinh, Hieu V. Ha, Nghia T.H. Tran, and Thieu N. Vo

Abstract. In this paper, we study the algebraic structures of constacyclic codes of length $n = 7p^s$ over a finite field of characteristics p, where $p > 7$ is a prime number and s a positive integer. The Hamming distance of all codes of these types are determined. In addition, self-orthogonal, dual-containing, self-dual and MDS codes among them will also be characterized.

1. Introduction

Constacyclic codes of length n over a finite field $\mathbb{F}$ can be considered to be the ideals of the quotient ring $\mathbb{F}[x]/\langle x^n - \lambda\rangle$ where n is a positive integer and λ a nonzero element of $\mathbb{F}$. Cyclic codes are special cases of constacyclic codes when $\lambda = 1$. Cyclic codes were well studied in the late 1950s and they quickly became one of the most important linear codes because of their rich algebraic structures and easy implementation. As a direct generalization of cyclic codes, constacyclic codes play essential roles in the theory of error-correcting codes and applications in engineering.

A constacyclic code is generated by a monic polynomial $g(x)$ which is a divisor of $x^n - \lambda$. In case $g(x)$ has no repeated roots, it is called a simple-root constacyclic code. Otherwise, it is called a repeated-root constacyclic code. In 1991, the authors in [2] and [16] studied repeated-root cyclic codes from a systematic manner. They proved that repeated-root cyclic codes are asymptotically bad. However, the studies in [20, 23] showed that optimal repeated-root cyclic codes still exist. Since then, the problem of studying the algebraic structures and Hamming distances of repeated-root cyclic, and constacyclic codes in general, has received growing attention.

The problem of classifying linear codes in general, and constacyclic code in particular, is difficult. Several partial results of this problem have been investigated recently. In [6], Dinh described the algebraic structures of repeated-root cyclic codes of length p^s in terms of the generators. Repeated-root cyclic codes of length p^s and their duals were also studied in [3]. These results were developed for these types of codes of lengths $2p^s, 3p^s, 4p^s$ and $6p^s$ in a series of papers [7–10]. In a more general fashion, the authors in [4, 18, 22] derives the algebraic structures of repeated-root constacyclic codes of length $l^m p^n$ with $l = 2, 3, 4$, respectively.

Different from the problem of determining the algebraic structures of repeated-root constacyclic codes, the problem of computing Hamming distances is further difficult and receives less attention. Only Hamming distances of these codes with very precise lengths exist. In 2008, Dinh [6] determined the Hamming distance of repeated-root cyclic codes of length p^s over $\mathbb{F}_{p^m}$. A year later, based on the relationship of repeated-root cyclic codes and their radical described in [2], Ozadam and Ozbudak [21] successfully determined the Hamming distance of all repeated-root cyclic codes of length $2p^s$. These results were extended for these types of codes of lengths $3p^s$ in [13, 18], $4p^s$ in [11], $5p^s$ in [12], and $6p^s$ in [14] for the case $p^m \equiv 2 \mod 3$. The Hamming distances of certain constacyclic codes of length ηp^s where η and p are coprime were also determined in [19]. No work for computing the Hamming distances of these types of codes of length np^s with $n \geq 7$ was completed so far.

In this paper, we consider the class of repeated-root constacyclic codes of length $7p^s$. On the one hand, we classify the algebraic structures of these codes in terms of the generator polynomials. Among them, all self-dual, self-orthogonal and dual codes of these types are characterized. On the other hand, we determine the Hamming distances of such all codes. As a consequence, a necessary and sufficient condition for such a code to be an MDS code is given.

The paper is organized as follows. In Section 2, we recall necessary definitions and notations from algebraic coding theory. In Section 3, we determine the Hamming distance of a simple-root cyclic code of length 7 and prove that this Hamming distance is exactly equal to the degree of the generator polynomial plus one. The repeated-roots cyclic and constacyclic codes of length $7p^s$ are then considered in Section 4

Received by the editors September 5, 2022.

and 5, respectively. Finally, we characterize the MDS codes in Section 6 and the self-orthogonal, dual-containing, self-dual codes in Section 7.

2. Preliminaries

Throughout this paper, we denote $q = p^m$ to be a prime power with a prime number $p > 7$ and a positive integer m. By $\mathbb{F}_q$ we mean the finite field with q elements. A code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is defined to be a subset of $\mathbb{F}_q^n$. In case $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$, it is called a linear code. For a linear code, we use the indicators $[n, k, d]$ to denote the length, the dimension and the (minimum) Hamming distance, respectively. The code $\mathcal{C} = \{0\}$ has distance $d = +\infty$ and the code $\mathcal{C} = \mathbb{F}_q^n$ has distance $d = 1$. They are called trivial codes. Other linear codes are called nontrivial and they have the Hamming distance at least 2. It is well-known that $d \leq n - k + 1$ (the singleton bound). A linear $[n, k, d]$-code is called a maximal dimension separable (MDS) code if $d = n - k + 1$.

Definition (see [17])**.** A *generator matrix* G for a linear $[n, k, d]$-code $\mathcal{C}$ is a k by n matrix for which the rows form a linear basis for $\mathcal{C}$.

The following lemma is a dual version of [15, Theorem 8.4, page 85].

Lemma 1. *Let G be a generator matrix for a linear $[n, k, d]$-code $\mathcal{C}$ over $\mathbb{F}_q$. Then for a positive integer s, we have*

(1) *The Hamming distance $d \leq s$ if and only if after removing some s columns of G, the obtained matrix has linearly dependent rows.*
(2) *The Hamming distance $d \geq s$ if and only if after removing arbitrary $s - 1$ columns of G, the obtained matrix always has linearly independent rows.*

Next we recall the notions of constacyclic codes. Let λ be a nonzero element in $\mathbb{F}_q$. The λ-constacyclic shift of $\mathbb{F}_q^n$ is the linear map $\tau_\lambda : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that

$$\tau_\lambda((c_0, c_1, \ldots, c_{n-1})) := (\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2}),$$

for $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$. A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is called λ-constacyclic if $\tau_\lambda(\mathcal{C}) = \mathcal{C}$. If $\lambda = 1$, $\mathcal{C}$ is called a cyclic code. In case $\lambda = -1$, $\mathcal{C}$ is called a negacyclic code.

Each code word $c = (a_0, a_1, \ldots, a_{n-1})$ is identified with the polynomial $c(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$, and a code $\mathcal{C}$ is then identified with the set of all polynomial representations of its code words. In $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$, the product $xc(x)$ corresponds to $\tau_\lambda(c)$. Hence, a linear code $\mathcal{C}$ is λ-constacyclic if and only if $\mathcal{C}$ is an ideal of $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$. Since, $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$ is a principal ideal domain, $\mathcal{C}$ is generated by a polynomial, say $g(x)$. In case $\mathcal{C} \neq 0$, the generator $g(x)$ divides $x^n - \lambda$ and it can be chosen to be the unique monic polynomial in $\mathcal{C}$ of least degree.

3. Simple-root cyclic codes of length 7

A cyclic code of length 7 over $\mathbb{F}_q$ is an ideal of the ring $\mathbb{F}_q[x]/\langle x^7 - 1\rangle$. In this section, we prove that the minimum Hamming distance of this cyclic code is exactly equal to the degree of its generator polynomial plus one, thus provide a simple formula for computing the minimum Hamming distance for these codes.

For polynomials $f(x), g(x)$ in a polynomial ring $R[x]$ with coefficients in an integral domain R, we denote by $\mathrm{res}_x(f(x), g(x))$ the resultant of f and g with respect to x (see [5, Chapter 3, § 6] for a detailed definition). This resultant is an element in R. It is equal to zero if and only if f and g has a common factor (of degree at least one). In particular, in case $R = \mathbb{Z}$, this resultant is an integer. The following lemma gives a sufficient condition for a polynomial in $\mathbb{Z}[x]$ vanished at the primitive root α of $x^7 - 1$.

Lemma 2. *Let α be a primitive root of $x^7 - 1$ in an algebraic extension of $\mathbb{F}_q$. For a polynomial $f(x) \in \mathbb{Z}[x]$, if p does not divide $res_x(f(x), x^7 - 1)$, then $f(\alpha) \neq 0$.*

Proof. Since p does not divide $\mathrm{res}_x(f(x), x^7 - 1)$, we have $\mathrm{res}_x(f(x), x^7 - 1) \neq 0$ considered as polynomial over $\mathbb{F}_q$. Therefore, $f(x)$ and $x^7 - 1$ are coprime in $\mathbb{F}_q[x]$. There exist polynomials $g(x), h(x) \in \mathbb{F}_q[x]$ such that $f(x)g(x) + (x^7 - 1)h(x) = 1$. By substituting $x = \alpha$, we obtain $f(\alpha)g(\alpha) = 1$. Hence, $f(\alpha) \neq 0$. □

The following theorem characterizes the Hamming distance of all cyclic codes of length 7 over $\mathbb{F}_q$.

Theorem 3. *Let $q = p^m$ be a prime power with $p > 7$ and let $\mathcal{C} = \langle g(x)\rangle \subseteq \mathbb{F}_q[x]/\langle x^7 - 1\rangle$ be a cyclic code of length 7 over $\mathbb{F}_q$, where $g(x)$ divides $x^7 - 1$. Then*

$$d_H(\mathcal{C}) = \begin{cases} 1 + \deg g, & \text{if } g(x) \neq x^7 - 1, \\ +\infty, & \text{if } g(x) = x^7 - 1. \end{cases}$$

Proof. We consider the following cases based on the degree of $g(x)$.

Case 1: $\deg g = 0$. Then g is a nonzero constant polynomial and $\mathcal{C} = \mathbb{F}_q^7$. Therefore $d_H(\mathcal{C}) = 1 = 1 + \deg g$.

Case 2: $\deg g = 1$. Then $g = x - \alpha^i$ for some $i = 0, \ldots, 6$ and we have, $\alpha^i \in \mathbb{F}_q \setminus \{0\}$. In this case, $\mathcal{C}$ is a proper ideal of $\mathbb{F}_q[x]/\langle x^7 - 1\rangle$ and it contains the code word $(-\alpha^i, 1, 0, 0, 0, 0, 0)$ which is of Hamming weight 2. Therefore, $d_H(\mathcal{C}) = 2 = 1 + \deg g$.

Case 3: $\deg g = 2$. Then we have $g(x) = (x - \alpha^{i_1})(x - \alpha^{i_2}) = S_2(\alpha) - S_1(\alpha)x + x^2$ for some integers i_1, i_2 such that $0 \le i_1 < i_2 \le 6$ and

$$S_1(x) = x^{i_1} + x^{i_2}, \quad S_2(x) = x^{i_1+i_2}.$$

Note that in this case, α^{i_1} and α^{i_2} are not necessary in $\mathbb{F}_q$, but we always have $S_1(\alpha)$ and $S_2(\alpha)$ are in $\mathbb{F}_q^*$. Since $\mathcal{C} = \langle g(x)\rangle$, the code $\mathcal{C}$ contains the code word $(S_2(\alpha), -S_1(\alpha), 1, 0, 0, 0, 0)$ which is of Hamming weight 3. Therefore $d_H(\mathcal{C}) \le 3$.

It remains to prove that $d_H(\mathcal{C}) \ge 3$. By Lemma 1, we need to prove that the generator matrix of $\mathcal{C}$ satisfies the condition: after removing arbitrary two columns, the obtained matrix has independent rows. It is noted that, the generator matrix of $\mathcal{C}$ is a matrix of size 5×7 and it has the form $G(\alpha)$, where $G(x)$ is the following matrix:

$$G(x) = \begin{bmatrix} S_2(x) & -S_1(x) & 1 & 0 & 0 & 0 & 0 \\ 0 & S_2(x) & -S_1(x) & 1 & 0 & 0 & 0 \\ 0 & 0 & S_2(x) & -S_1(x) & 1 & 0 & 0 \\ 0 & 0 & 0 & S_2(x) & -S_1(x) & 1 & 0 \\ 0 & 0 & 0 & 0 & S_2(x) & -S_1(x) & 1 \end{bmatrix}. \tag{1}$$

For each integer i_1, i_2, r_1, r_2 with $0 \le i_1 < i_2 \le 6$ and $1 \le r_1 < r_2 \le 7$, we set

- $G_{i_1,i_2,r_1,r_2}(x)$ to be the 5×5 matrix obtained from $G(x)$ by deleting two columns r_1-th and r_2-th,
- $D_{i_1,i_2,r_1,r_2}(x)$ to be the determinant of the matrix $G_{i_1,i_2,r_1,r_2}(x)$, and
- $R_{i_1,i_2,r_1,r_2} := \mathrm{res}_x(D_{i_1,i_2,r_1,r_2}(x), x^7 - 1)$ which is the resultant of $D_{i_1,i_2,r_1,r_2}(x)$ and $x^7 - 1$ with respect to x.

The resultant R_{i_1,i_2,r_1,r_2} is an integer. We use a "for" loop in Maple to determine R_{i_1,i_2,r_1,r_2} for every integers i_1, i_2, r_1, r_2 such that $0 \le i_1 < i_2 \le 6$ and $1 \le r_1 < r_2 \le 7$. A direct computation from Maple shows that, for all such i_1, i_2, r_1, r_2, the resultant R_{i_1,i_2,r_1,r_2} is always an integer of the form $\pm 2^u 3^v 5^w$ for some nonnegative integers u, v and w (see Appendix A for the code and the results from Maple). Therefore by Lemma 2, $D_{i_1,i_2,r_1,r_2}(\alpha) \ne 0$. This means that all sub-matrices of size 5×5 of the generator matrix G are nonsingular. Equivalently, the rows of $G_{i_1,i_2,r_1,r_2}(\alpha)$ are linearly independent for arbitrary r_1 and r_2. Hence, by Lemma 1, we have $d_H(\mathcal{C}) \ge 3$. Thus, we must have $d_H(C) = 3$.

Case 4: $\deg g(x) = 3$. This case can be proved by using the same argument as in Case 3. Indeed, on the one hand, we have

$$g(x) = (x - \alpha^{i_1})(x - \alpha^{i_2})(x - \alpha^{i_3}) = -S_3(\alpha) + S_2(\alpha)x - S_1(\alpha)x^2 + x^3$$

for some integers i_1, i_2, i_3 such that $0 \le i_1, i_2, i_3 \le 6$, and

$$S_1(x) = x^{i_1} + x^{i_2} + x^{i_3}, \quad S_2(x) = x^{i_2+i_3} + x^{i_3+i_1} + x^{i_1+i_2}, \quad S_3(x) = x^{i_1+i_2+i_3}.$$

It is noted that, the elements $\alpha^{i_1}, \alpha^{i_2}$ and α^{i_3} are not necessarily in $\mathbb{F}_q$, but we always have $S_1(\alpha), S_2(\alpha), S_3(\alpha) \in \mathbb{F}_q^*$. Since $\mathcal{C} = \langle g(x)\rangle$, the code word

$$(-S_3(\alpha), S_2(\alpha), -S_1(\alpha), 1, 0, 0, 0) \in \mathbb{F}_q^7$$

is also in $\mathcal{C}$ and is of Hamming weight 4. Therefore $d_H(\mathcal{C}) \le 4$.

On the other hand, the generator matrix of $\mathcal{C}$ has the form $G(\alpha)$ where

$$G(x) = \begin{bmatrix} -S_3(x) & S_2(x) & -S_1(x) & 1 & 0 & 0 & 0 \\ 0 & -S_3(x) & S_2(x) & -S_1(x) & 1 & 0 & 0 \\ 0 & 0 & -S_3(x) & S_2(x) & -S_1(x) & 1 & 0 \\ 0 & 0 & 0 & -S_3(x) & S_2(x) & -S_1(x) & 1 \end{bmatrix}.$$

By using the same argument as in the previous case, we can check that, after removing arbitrary three columns of $G(\alpha)$, the obtained matrix has linearly independent rows. Thus, by Lemma 1, we have $d_H(\mathcal{C}) \geq 4$. Hence, we must have $d_H(\mathcal{C}) = 4$.

Case 5: $\deg g = 4$. This case is similar to Cases 3 and 4, so we omit it.

Case 6: $\deg g = 5$. This case is also similar to Cases 3 and 4, so we omit it.

Case 7: $\deg g(x) = 6$. Then $g(x) = 1 + x + \cdots + x^6$. In this case, the cyclic code $\mathcal{C}$ contains only the code words (a, a, a, a, a, a, a) for $a \in \mathbb{F}_q$. Thus $d_H(\mathcal{C}) = 7 = 1 + \deg g$.

In summary, we always have $d_H(\mathcal{C}) = 1 + \deg g$. The theorem is then proved. □

4. Repeated-root cyclic codes of length $7p^s$

Next, we will classify all of repeated-root cylic codes of length $7p^s$ over $\mathbb{F}_q$ in terms of their generator polynomials and determine their Hamming distances. Let $\mathcal{C} = \langle g(x) \rangle \subseteq \mathbb{F}_q[x]/\left\langle x^{7p^s} - 1 \right\rangle$ be such a code, where $g(x)$ is a factor of $x^{7p^s} - 1$. The structure of $\mathcal{C}$ depends much on the factorization of $g(x)$ over $\mathbb{F}_q$.

We start with a detail irreducible factorization of $x^7 - 1$ over $\mathbb{F}_q$. Let α be a primitive root of $x^7 - 1$ over some extension field of $\mathbb{F}_q$. For each $i = 0, 1, \ldots, 6$, the minimal polynomial of α^i over $\mathbb{F}_q$ is the polynomial $m_i(x) = \prod_{j \in C_{7,j}} (x - \alpha^j)$, where $C_{7,j}$ is the cyclotomic coset of j modulo 7 over $\mathbb{F}_q$. Let T_7 be the set of representatives of cyclotomic cosets of modulo 7. The factorization of $x^7 - 1$ over $\mathbb{F}_q$ is $x^7 - 1 = \prod_{i \in T_7} m_i(x)$. In detail, the irreducible factorization of $x^7 - 1$ is given in Table 1. In this table, and also in the rest of this article, the polynomials $f_i(x)$ are given by

$$
\begin{aligned}
f_1(x) &= (x - \alpha)(x - \alpha^6) = x^2 - ax + 1, \\
f_2(x) &= (x - \alpha^2)(x - \alpha^5) = x^2 - (a^2 - 2)x + 1, \\
f_3(x) &= (x - \alpha^3)(x - \alpha^4) = x^2 - (a^3 - 3a)x + 1, \\
f_4(x) &= (x - \alpha)(x - \alpha^2)(x - \alpha^4) = x^3 - bx^2 - (1 + b)x - 1, \\
f_5(x) &= (x - \alpha^3)(x - \alpha^5)(x - \alpha^6) = x^3 + (1 + b)x^2 + bx - 1, \quad \text{and} \\
f_6(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,
\end{aligned} \tag{2}
$$

where $a = \alpha + \alpha^6$ and $b = \alpha + \alpha^2 + \alpha^4$.

TABLE 1. The irreducible factorization of $x^7 - 1$ over $\mathbb{F}_q$.

	$q = p^m$	The factorization of $x^7 - 1$
Case 1	$q \equiv 1 \mod 7$	$\prod_{j=0}^{6} (x - \alpha^j)$
Case 2	$q \equiv 6 \mod 7$	$(x - 1)f_1(x)f_2(x)f_3(x)$
Case 3	$q \equiv 2 \text{ or } 4 \mod 7$	$(x - 1)f_4(x)f_5(x)$
Case 4	$q \equiv 3 \text{ or } 5 \mod 7$	$(x - 1)f_6(x)$

Since $x^{7p^s} - 1 = (x^7 - 1)^{p^s}$, the factorization of $g(x)$ over $\mathbb{F}_q$ has the form $g(x) = \prod_{i \in T_7} m_i(x)^{e_i}$ for some $0 \leq e_i \leq p^s$. The following definition will be in the central of our computations of the Hamming distance of the repeated-root cyclic codes.

Definition. Let $\mathcal{C} = \langle g(x) \rangle \subseteq \mathbb{F}_q[x]/\left\langle x^{7p^s} - 1 \right\rangle$ be a cyclic code of length $7p^s$ over $\mathbb{F}_q$. Assume that if $g \neq 0$ then $g(x) = \prod_{i \in T_7} m_i(x)^{e_i}$ for some $0 \leq e_i \leq p^s$. For each $t = 0, 1, \ldots, p^s$, we define

(1) the associated simple-root polynomial

$$
g_t(x) := \begin{cases} 0, & \text{if } g = 0, \\ 1, & \text{if } g \neq 0 \text{ and } t \geq e_i \text{ for every } i, \\ \prod\limits_{\substack{i \in T_7 \\ e_i > t}} m_i(x), & \text{if } g \neq 0 \text{ and } t < e_i \text{ for some } i, \end{cases}
$$

(2) the associated simple-root cyclic code $\mathcal{C}_t := \langle g_t(x) \rangle$ in $\mathbb{F}_q[x]/\left\langle x^7 - 1 \right\rangle$,

(3) the associated integer

$$P_t := \begin{cases} \prod_{k=0}^{s}(t_k+1), & \text{if } 0 \le t \le p^s-1 \text{ and } t = \overline{t_{s-1}t_{s-2}\ldots t_1t_0}_p, \\ +\infty, & \text{if } t = p^s. \end{cases}$$

Here, $\overline{t_{s-1}t_{s-2}\ldots t_1t_0}_p = t_{s-1}p^{s-1} + t_{s-2}p^{s-2} + \ldots + t_1p + t_0$, with $0 \le t_i \le p-1$, is the p-adic representation of t.

The following lemma shows that the minimum Hamming distances of the simple-root cyclic codes $\mathcal{C}_t$ carry important information about those of the repeated-root cyclic code $\mathcal{C}$.

Lemma 4 (See [2])**.** *Let $\mathcal{C}$ be a linear cyclic code of length $7p^s$ over $\mathbb{F}_q$ and $\mathcal{C}_t$ its associated simple-root cyclic codes for each $t = 0, 1, \ldots, p^s$. Then we have*

$$d_H(\mathcal{C}) = \min_{0 \le t \le p^s} P_t d_H(\mathcal{C}_t).$$

Lemma 5. *For each $l = 0, 1, \ldots, p^s$, we have $\min_{l \le t \le p^s} P_t = \mathcal{M}(l)$, where*

$$\mathcal{M}(l) := \begin{cases} \left(p+1-\left\lfloor p^{\{\log_p(p^s-l)\}}\right\rfloor\right) p^{s-1-\lfloor \log_p(p^s-l)\rfloor} & \text{if } 0 \le l < p^s, \\ +\infty, & \text{if } l = p^s. \end{cases}$$

Here, $\lfloor x \rfloor$ denotes the largest integer which is smaller or equal to x, and $\{x\} = x - \lfloor x \rfloor$.

Proof. We consider the following four cases.

Case 1: $l = 0$. In this case, it is clear that $\min_{0 \le t \le p^s} P_t = P_0 = 1$. We also have $\lfloor \log_p(p^s - l) \rfloor = s$ and $\{\log_p(p^s - l)\} = 0$, thus $\mathcal{M}(0) = 1 = \min_{0 \le t \le p^s} P_t$.

Case 2: $1 \le l \le p^{s-1}$. We first claim that $\min_{l \le t \le p^s} P_t = 2$. Indeed, for every $l \le t \le p^s - 1$, there must be at least a positive integer digit in the p-adic expansion of t. Thus $P_t \ge 2$. We also have $P_{p^{s-1}} = 2$. The claim is proved.

For $1 \le l \le p^{s-1}$, we have $s - 1 \le \log_p(p^s - l) < s$. Thus, $\lfloor \log_p(p^s - l) \rfloor = s - 1$ and

$$\mathcal{M}(l) = p + 1 - \lfloor p^{\{\log_p(p^s-l)\}} \rfloor = p + 1 - \lfloor p^{\log_p(p^s-l)-(s-1)} \rfloor = p + 1 - \lfloor \frac{p^s - l}{p^{s-1}} \rfloor.$$

Since $1 \le l \le p^{s-1}$, we have $p - 1 \le \frac{p^s-l}{p^{s-1}} < p$. Hence, $\mathcal{M}(l) = p + 1 - (p-1) = 2 = \min_{l \le t \le p^s} P_t$.

Case 3: $p^{s-1} < l \le p^s - 1$. Following the lines in [19, Theorem 7.4], we have

$$\min_{l \le t \le p^s} P_t = (\beta + 2)p^\tau, \tag{3}$$

where (β, τ) is the unique pair of integers such that $0 \le \beta \le p-2$, $0 \le \tau \le s-1$ and

$$p^s - p^{s-\tau} + \beta p^{s-\tau-1} < l \le p^s - p^{s-\tau} + (\beta+1)p^{s-\tau-1}. \tag{4}$$

The above inequality is equivalent to

$$\frac{p^s - (\beta+1)p^{s-1}}{p^s - l} \le p^\tau < \frac{p^s - \beta p^{s-1}}{p^s - l}.$$

Since $0 \le \beta \le p-2$, we imply that

$$\frac{p^s - (p-1)p^{s-1}}{p^s - l} \le p^\tau < \frac{p^s}{p^s - l}.$$

Thus,

$$s - \log_p(p^s - l) - 1 \le \tau < s - \log_p(p^s - l).$$

Hence, $\tau = s - 1 - \lfloor \log_p(p^s - l) \rfloor$. To determine β, we equivalently transform the inequality (4) as

$$p - 1 - \frac{p^s - l}{p^{s-\tau-1}} \le \beta < p - \frac{p^s - l}{p^{s-\tau-1}}.$$

Thus,

$$\beta = p - 1 - \left\lfloor \frac{p^s - l}{p^{s-\tau-1}} \right\rfloor = p - 1 - \left\lfloor \frac{p^s - l}{p^{\lfloor \log_p(p^s-l) \rfloor}} \right\rfloor = p - 1 - \left\lfloor p^{\{\log_p(p^s-l)\}} \right\rfloor.$$

By substituting $\tau = s-1-\lfloor \log_p(p^s-l)\rfloor$ and $\beta = p-1-\left\lfloor p^{\{\log_p(p^s-l)\}}\right\rfloor$ to Eq. (3), we obtain

$$\min_{l\le t\le p^s} P_t = (\beta+2)p^\tau = \left(p+1-\left\lfloor p^{\{\log_p(p^s-l)\}}\right\rfloor\right)p^{s-1-\lfloor \log_p(p^s-l)\rfloor} = \mathcal{M}(l).$$

Case 4: $l = p^s$. Then it is clear that $P_{p^s} = +\infty = \mathcal{M}(p^s)$.

In summary, for $0 \le l \le p^s$, we always have $\min_{l\le t\le p^s} P_t = \mathcal{M}(l)$. The lemma is then proved. □

Remark 6. For the above proof, we can see that $\mathcal{M}(l)$ is a non-decreasing function and

$$\mathcal{M}(l) = \begin{cases} 1, & \text{if } l = 0, \\ 2, & \text{if } 1 \le l \le p^{s-1}, \\ \ge 3, & \text{if } p^{s-1}+1 \le l \le p^s-1, \\ p^s, & \text{if } l = p^s-1, \\ +\infty, & \text{if } l = p^s. \end{cases}$$

Now we are going to determine all repeated-cyclic codes of length $7p^s$ over $\mathbb{F}_q$ and their Hamming distances.

Theorem 7. *All nonzero repeated-root cyclic codes of length $7p^s$ over $\mathbb{F}_q$ are listed in Table 2. Let $\mathcal{C}$ be such a code. Then its Hamming distance is determined case by case as follows.*

***Case 1**: If $q \equiv 1 \mod 7$, then $\mathcal{C} = \left\langle \prod_{i=0}^{6}(x-\alpha^i)^{e_i} \right\rangle$ for some $e_i = 0,\dots,p^s$ and $i = 0,\dots,6$. Assume without loss of generality that $0 \le e_0 \le e_1 \le \dots \le e_6 \le p^s$, then*

$$d_H(\mathcal{C}) = \min\{7\mathcal{M}(e_0), 6\mathcal{M}(e_1), 5\mathcal{M}(e_2), 4\mathcal{M}(e_3), 3\mathcal{M}(e_4), 2\mathcal{M}(e_5), \mathcal{M}(e_6)\}.$$

***Case 2**: If $q \equiv 6 \mod 7$, then $\mathcal{C} = \langle (x-1)^{e_0} f_1(x)^{e_1} f_2(x)^{e_2} f_3(x)^{e_3}\rangle$ for some $e_i = 0,\dots,p^s$ and $i = 0,1,2,3$. Assume without loss of generality that $e_1 \le e_2 \le e_3$, then*

$$d_H(\mathcal{C}) = \begin{cases} \min\{7\mathcal{M}(e_0), 5\mathcal{M}(e_1), 3\mathcal{M}(e_2), \mathcal{M}(e_3)\}, & \text{if } e_0 \le e_1 \le e_2 \le e_3, \\ \min\{6\mathcal{M}(e_1), 5\mathcal{M}(e_0), 3\mathcal{M}(e_2), \mathcal{M}(e_3)\}, & \text{if } e_1 \le e_0 \le e_2 \le e_3, \\ \min\{6\mathcal{M}(e_1), 4\mathcal{M}(e_2), 3\mathcal{M}(e_0), \mathcal{M}(e_3)\}, & \text{if } e_1 \le e_2 \le e_0 \le e_3, \\ \min\{6\mathcal{M}(e_1), 4\mathcal{M}(e_2), 2\mathcal{M}(e_3), \mathcal{M}(e_0)\}, & \text{if } e_1 \le e_2 \le e_3 \le e_0. \end{cases}$$

***Case 3**: If $q \equiv 2$ or $4 \mod 7$, then $\mathcal{C} = \langle (x-1)^{e_0} f_4(x)^{e_1} f_5(x)^{e_2}\rangle$ for some $e_i = 0,\dots,p^s$ and $i = 0,1,2$. Assume without loss of generality that $e_1 \le e_2$, then*

$$d_H(\mathcal{C}) = \begin{cases} \min\{7\mathcal{M}(e_0), 4\mathcal{M}(e_1), \mathcal{M}(e_2)\}, & \text{if } e_0 \le e_1 \le e_2, \\ \min\{5\mathcal{M}(e_1), 4\mathcal{M}(e_0), \mathcal{M}(e_2)\}, & \text{if } e_1 \le e_0 \le e_2, \\ \min\{5\mathcal{M}(e_1), 2\mathcal{M}(e_2), \mathcal{M}(e_0)\}, & \text{if } e_1 \le e_2 \le e_0. \end{cases}$$

***Case 4**: If $q \equiv 3$ or $5 \mod 7$, then $\mathcal{C} = \langle (x-1)^{e_0} f_6(x)^{e_1}\rangle$ for some $e_i = 0,\dots,p^s$ and $i = 0,1$ and*

$$d_H(\mathcal{C}) = \begin{cases} \min\{7\mathcal{M}(e_0), \mathcal{M}(e_1)\}, & \text{if } e_0 \le e_1, \\ \min\{2\mathcal{M}(e_1), \mathcal{M}(e_0)\}, & \text{if } e_1 \le e_0. \end{cases}$$

Here, the function $\mathcal{M}$ is defined in Lemma 5.

Proof. We prove the theorem for the case when $q \equiv 1 \mod 7$. The other cases are proved similarly, so we omit it. In case $q \equiv 1 \mod 7$, according to Table 1, the polynomial x^7-1 is factored linearly over $\mathbb{F}_q$ as $x^7-1 = \prod_{i=0}^{6}(x-\alpha^i)$, where α is a primitive root of x^7-1 in $\mathbb{F}_q$. Therefore,

$$x^{7p^s}-1 = (x^7-1)^{p^s} = \prod_{i=0}^{6}(x-\alpha^i)^{p^s}.$$

Since $\mathcal{C}$ is a principal ideal generated by a divisor of $x^{7p^s}-1$, $\mathcal{C}$ must be of the form

$$\mathcal{C} = \left\langle \prod_{i=0}^{6}(x-\alpha^i)^{e_i} \right\rangle,$$

for some $e_i = 0,\dots,p^s$ and $i = 0,\dots,6$.

The Hamming distance of $\mathcal{C}$ will be determined by using Lemma 4 and 5 as follows. Without loss of generality, we assume that $0 \le e_0 \le \ldots \le e_6 \le p^s$. For each $t = 0, \ldots, p^s$, the associated simple-root polynomial g_t is given by

$$g_t(x) = \begin{cases} x^7 - 1, & \text{if } 0 \le t < e_0, \\ (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6), & \text{if } e_0 \le t < e_1, \\ (x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6), & \text{if } e_1 \le t < e_2, \\ (x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6), & \text{if } e_2 \le t < e_3, \\ (x-\alpha^4)(x-\alpha^5)(x-\alpha^6), & \text{if } e_3 \le t < e_4, \\ (x-\alpha^5)(x-\alpha^6), & \text{if } e_4 \le t < e_5, \\ x-\alpha^6, & \text{if } e_5 \le t < e_6, \\ 1, & \text{if } e_6 \le t \le p^s. \end{cases}$$

By applying Lemma 4, we have

$$\begin{aligned} d_H(\mathcal{C}) &= \min_{0 \le t \le p^s} P_t d_H(\mathcal{C}_t) \\ &= \min\left\{ \min_{e_0 \le t < e_1} 7P_t, \min_{e_1 \le t < e_2} 6P_t, \min_{e_2 \le t < e_3} 5P_t, \min_{e_3 \le t < e_4} 4P_t, \min_{e_4 \le t < e_5} 3P_t, \min_{e_5 \le t < e_6} 2P_t, \min_{e_6 \le t < p^s} P_t \right\} \\ &= \min\left\{ \min_{e_0 \le t \le p^s} 7P_t, \min_{e_1 \le t \le p^s} 6P_t, \min_{e_2 \le t \le p^s} 5P_t, \min_{e_3 \le t \le p^s} 4P_t, \min_{e_4 \le t \le p^s} 3P_t, \min_{e_5 \le t \le p^s} 2P_t, \min_{e_6 \le t \le p^s} P_t \right\}. \end{aligned}$$

Thus, by Lemma 5, we have

$$d_H(\mathcal{C}) = \min\left\{7\mathcal{M}(e_0),\, 6\mathcal{M}(e_1),\, 5\mathcal{M}(e_2),\, 4\mathcal{M}(e_3),\, 3\mathcal{M}(e_4),\, 2\mathcal{M}(e_5),\, \mathcal{M}(e_6)\right\}.$$

The theorem is then proved. □

TABLE 2. All nonzero repeated-root cyclic codes of length $7p^s$ over $\mathbb{F}_q$. Here, $0 \le e_j \le p^s$ with $j = 0, \ldots, 6$, and $f_i(x)$ are defined in Eq. (2).

	$q = p^m$	The cyclic code $\mathcal{C}$
Case 1	$q \equiv 1 \mod 7$	$\left\langle \prod_{j=0}^{6} (x-\alpha^j)^{e_j} \right\rangle$
Case 2	$q \equiv 6 \mod 7$	$\langle (x-1)^{e_0} f_1(x)^{e_1} f_2(x)^{e_2} f_3(x)^{e_3} \rangle$
Case 3	$q \equiv 2 \text{ or } 4 \mod 7$	$\langle (x-1)^{e_0} f_4(x)^{e_1} f_5(x)^{e_2} \rangle$
Case 4	$q \equiv 3 \text{ or } 5 \mod 7$	$\langle (x-1)^{e_0} f_6(x)^{e_1} \rangle$

5. Repeated-root λ-constacyclic codes of length $7p^s$

In this section, we will classify all of repeated-root constacylic codes of length $7p^s$ over $\mathbb{F}_q$ in terms of their generator polynomials and determine their Hamming distances. The following proposition shows that almost all of these constacylic codes indeed have the same structure as a cyclic codes of the same length via an appropriate ring isomorphism.

Proposition 8. *Assume that β is the generator of the multiplicative group $\mathbb{F}_q^*$ and l is a prime number such that $l \ne p$.*

1. *If $(q \equiv 1 \mod l$ and $\lambda \notin \langle \beta^l \rangle)$, then $\lambda = \gamma^{p^s}$ for some $\gamma \in \mathbb{F}_q^*$ and the polynomial $x^l - \gamma$ is irreducible over $\mathbb{F}_q$. As a consequence, any λ-constacyclic code in $\mathbb{F}_q[x]/\langle x^{lp^s} - \lambda \rangle$ has the form $\mathcal{C} = \langle (x^l - \gamma)^e \rangle$ for some $e = 0, 1, \ldots, p^s$.*
2. *If $(q \equiv 1 \mod l$ and $\lambda \in \langle \beta^l \rangle)$ or $(q \not\equiv 1 \mod l)$, then $\lambda = \zeta^{lp^s}$ for some $\zeta \in \mathbb{F}_q^*$ and the ring homomorphism $\phi : \mathbb{F}_q[x]/\langle x^{lp^s} - \lambda \rangle \to \mathbb{F}_q[x]/\langle x^{lp^s} - 1 \rangle$ defined by $f(x) \mapsto f(\zeta x)$ is an isomorphism. As a consequence, any λ-constacyclic code in $\mathbb{F}_q[x]/\langle x^{lp^s} - \lambda \rangle$ has the form $\mathcal{C}(\zeta^{-1}x)$, where $\mathcal{C} = \mathcal{C}(x)$ is a cyclic code in $\mathbb{F}_q[x]/\langle x^{lp^s} - 1 \rangle$.*

Proof. See Theorems 4.1 and 4.2 in [3]. □

Based on the above proposition and Theorem 7, we can classify all repeated-root λ-constacyclic codes of length $7p^s$ and determine their Hamming distances as in the following theorem.

Theorem 9. *Let β be the generator of the multiplicative group $\mathbb{F}_q^*$ and $\gamma \in \mathbb{F}_q^*$. All nonzero repeated-root λ-constacyclic codes of length $7p^s$ over $\mathbb{F}_q$ are listed in Table 3.*

Let $\mathcal{C}$ be such a code. Then its Hamming distance is determined case by case as follows.

***Case 1a**: If $q \equiv 1 \mod 7$ and $\lambda \notin \langle \beta^7 \rangle$, then $\mathcal{C} = \langle (x^7 - \gamma)^{e_0} \rangle$ for some $e_0 = 0, 1, \ldots, p^s$ and for $\gamma \in \mathbb{F}_q^*$ such that $\lambda = \gamma^{p^s}$. In this case, $d_H(\mathcal{C}) = \mathcal{M}(e_0)$.*

***Case 1b**: If $q \equiv 1 \mod 7$ and $\lambda \in \langle \beta^7 \rangle$, then $\mathcal{C} = \left\langle \prod_{i=0}^{6} (x - \zeta\alpha^i)^{e_i} \right\rangle$ for some $e_i = 0, 1, \ldots, p^s$ and $\zeta \in \mathbb{F}_q^*$ such that $\lambda = \zeta^{7p^s}$. Furthermore, assume without loss of generality that $0 \le e_0 \le e_1 \le \ldots \le e_6 \le p^s$, then*

$$d_H(\mathcal{C}) = \min\{7\mathcal{M}(e_0), 6\mathcal{M}(e_1), 5\mathcal{M}(e_2), 4\mathcal{M}(e_3), 3\mathcal{M}(e_4), 2\mathcal{M}(e_5), \mathcal{M}(e_6)\}.$$

***Case 2**: If $q \equiv 6 \mod 7$, then $\mathcal{C} = \langle (x-\zeta)^{e_0} f_1(\zeta^{-1}x)^{e_1} f_2(\zeta^{-1}x)^{e_2} f_3(\zeta^{-1}x)^{e_3} \rangle$ for some $e_i = 0, 1, \ldots, p^s$ and $\zeta \in \mathbb{F}_q^*$ such that $\lambda = \zeta^{7p^s}$. Furthermore, assume without loss of generality that $e_1 \le e_2 \le e_3$, then*

$$d_H(\mathcal{C}) = \begin{cases} \min\{7\mathcal{M}(e_0), 5\mathcal{M}(e_1), 3\mathcal{M}(e_2), \mathcal{M}(e_3)\}, & \text{if } e_0 \le e_1 \le e_2 \le e_3, \\ \min\{6\mathcal{M}(e_1), 5\mathcal{M}(e_0), 3\mathcal{M}(e_2), \mathcal{M}(e_3)\}, & \text{if } e_1 \le e_0 \le e_2 \le e_3, \\ \min\{6\mathcal{M}(e_1), 4\mathcal{M}(e_2), 3\mathcal{M}(e_0), \mathcal{M}(e_3)\}, & \text{if } e_1 \le e_2 \le e_0 \le e_3, \\ \min\{6\mathcal{M}(e_1), 4\mathcal{M}(e_2), 2\mathcal{M}(e_3), \mathcal{M}(e_0)\}, & \text{if } e_1 \le e_2 \le e_3 \le e_0. \end{cases}$$

***Case 3**: If $q \equiv 2$ or $4 \mod 7$, then $\mathcal{C} = \langle (x-\zeta)^{e_0} f_4(\zeta^{-1}x)^{e_1} f_5(\zeta^{-1}x)^{e_2} \rangle$ for some $e_i = 0, 1, \ldots, p^s$ and $\zeta \in \mathbb{F}_q^*$ such that $\lambda = \zeta^{7p^s}$. Furthermore, assume without loss of generality that $e_1 \le e_2$, then*

$$d_H(\mathcal{C}) = \begin{cases} \min\{7\mathcal{M}(e_0), 4\mathcal{M}(e_1), \mathcal{M}(e_2)\}, & \text{if } e_0 \le e_1 \le e_2, \\ \min\{5\mathcal{M}(e_1), 4\mathcal{M}(e_0), \mathcal{M}(e_2)\}, & \text{if } e_1 \le e_0 \le e_2, \\ \min\{5\mathcal{M}(e_1), 2\mathcal{M}(e_2), \mathcal{M}(e_0)\}, & \text{if } e_1 \le e_2 \le e_0. \end{cases}$$

***Case 4**: If $q \equiv 3$ or $5 \mod 7$, then $\mathcal{C} = \langle (x-\zeta)^{e_0} f_6(\zeta x)^{e_1} \rangle$ for some $e_i = 0, 1, \ldots, p^s$ and $\zeta \in \mathbb{F}_q^*$ such that $\lambda = \zeta^{7p^s}$. In this case, we have*

$$d_H(\mathcal{C}) = \begin{cases} \min\{7\mathcal{M}(e_0), \mathcal{M}(e_1)\}, & \text{if } e_0 \le e_1, \\ \min\{2\mathcal{M}(e_1), \mathcal{M}(e_0)\}, & \text{if } e_1 \le e_0. \end{cases}$$

Here, the function $\mathcal{M}$ is defined in Lemma 5.

Proof. Assume that $\mathcal{C}$ is a nonzero repeated-root λ-constacyclic code of length $7p^s$ over $\mathbb{F}_q$. According to Proposition 8, $\mathcal{C}$ has only one of the following two forms:

(1) $\mathcal{C} = \langle (x^7 - \gamma)^{e_0} \rangle$, for some $\gamma \in \mathbb{F}_q^*$ such that $\lambda = \gamma^{p^s}$. This form occurs when $q \equiv 1 \mod 7$ and $\lambda \in \langle \beta^7 \rangle$ which is ***Case 1a***.
(2) $\mathcal{C} = \overline{\mathcal{C}}(\zeta^{-1}x)$, where $\overline{\mathcal{C}}$ is a repeated-root cyclic code of length $7p^s$ over $\mathbb{F}_q$, and $\zeta \in \mathbb{F}_q^*$ such that $\lambda = \zeta^{7p^s}$. This form occurs in ***Cases 1b*** and ***2-4***.

In combination with the list of all possibilities for $\overline{\mathcal{C}}$ in Table 2, we obtain the list of all possibilities for $\mathcal{C}$ in Table 3.

Next, we determine the Hamming distance of $\mathcal{C}$. ***Cases 1b*** and ***2-4*** follows directly from the fact that $d_H(\mathcal{C}) = d_H(\overline{\mathcal{C}})$ and Theorem 2. We only need to consider ***Case 1a*** when ($q \equiv 1 \mod 7$ and $\lambda \notin \langle \beta^7 \rangle$). In this case, $\mathcal{C}$ must be of the form $\mathcal{C} = \langle (x^7 - \gamma)^{e_0} \rangle$ for some $e_0 = 0, 1, \ldots, p^s$. By [19, Theorem 7.5], we known that

$$d_H(\mathcal{C}) = \begin{cases} 1, & \text{if } e_0 = 0, \\ (\beta+2)p^\tau, & \text{if } p^s - p^{s-\tau} + \beta p^{s-\tau-1} + 1 \le e_0 \le p^s - p^{s-\tau} + (\beta+1)p^{s-\tau-1}, \\ +\infty, & \text{if } e_0 = p^s. \end{cases}$$

By using the same argument as in the proof of Lemma 5, we can verify that the right hand side is exactly equal to $\mathcal{M}(e_0)$. Thus, $d_H(\mathcal{C}) = \mathcal{M}(e_0)$. The theorem is then proved. □

TABLE 3. All nonzero repeated-root λ-constacyclic codes of length $7p^s$ over $\mathbb{F}_q$. Here, $0 \le e_j \le p^s$, β is the generator of $\mathbb{F}_q^*$, and $f_i(x)$ are defined in Eq. (2).

	$q = p^m$	λ	The λ-constacyclic codes $\mathcal{C}$
Case 1a	$q \equiv 1 \mod 7$ and $\lambda \notin \langle \beta^7 \rangle$	$\lambda = \gamma^{p^s}$	$\langle (x^7 - \gamma)^{e_0} \rangle$
Case 1b	$q \equiv 1 \mod 7$ and $\lambda \in \langle \beta^7 \rangle$	$\lambda = \zeta^{7p^s}$	$\left\langle \prod_{j=0}^{6} (x - \zeta\alpha^j)^{e_j} \right\rangle$
Case 2	$q \equiv 6 \mod 7$	$\lambda = \zeta^{7p^s}$	$\langle (x-\zeta)^{e_0} f_1(\zeta^{-1}x)^{e_1} f_2(\zeta^{-1}x)^{e_2} f_3(\zeta^{-1}x)^{e_3} \rangle$
Case 3	$q \equiv 2$ or $4 \mod 7$	$\lambda = \zeta^{7p^s}$	$\langle (x-\zeta)^{e_0} f_4(\zeta^{-1}x)^{e_1} f_5(\zeta^{-1}x)^{e_2} \rangle$
Case 4	$q \equiv 3$ or $5 \mod 7$	$\lambda = \zeta^{7p^s}$	$\langle (x-\zeta)^{e_0} f_6(\zeta^{-1}x)^{e_1} \rangle$

6. MDS repeated-root constacyclic codes of length $7p^s$

In this section, we characterize all MDS codes among the class of repeated-root constacyclic codes of length $7p^s$ over $\mathbb{F}_q$. Because the Hamming distance of these codes is calculated via the function $\mathcal{M}$, we first begin with a bound for $\mathcal{M}$.

Lemma 10. *For every integer l such that $0 \le l \le p^s - 1$, we have $\mathcal{M}(l) \le l + 1$. The equality holds if and only if either $s = 1$ or $l = 0, 1, p^s - 1$.*

Proof. From Remark 6, we see that if $0 \le l \le p^{s-1}$ then $\mathcal{M}(l) \le l + 1$. We only need to consider the case when $p^{s-1} + 1 \le l \le p^s - 1$. Following the lines in [19, Theorem 7.4], we have

$$\mathcal{M}(l) = \min_{l \le t \le p^s} P_t = (\beta + 2)p^\tau,$$

where (β, τ) is the unique pair of integers such that $0 \le \beta \le p - 2$, $0 \le \tau \le s - 1$ and

$$p^s - p^{s-\tau} + \beta p^{s-\tau-1} + 1 \le l \le p^s - p^{s-\tau} + (\beta + 1)p^{s-\tau-1}.$$

Hence, it suffices to prove that

$$(\beta + 2)p^\tau \le p^s - p^{s-\tau} + \beta p^{s-\tau-1} + 2,$$

or equivalently,

$$\beta(p^\tau - p^{s-\tau-1)} \le (p^{s-\tau} - 2)(p^\tau - 1).$$

The later inequality is true because $\beta \le p-2 \le p^{s-\tau} - 2$ and $p^\tau - p^{s-\tau-1} \le p^\tau - 1$. Hence, $\mathcal{M}(l) \le l+1$. The equality occurs if and only if either

$$\begin{cases} p^\tau - 1 = p^\tau - p^{s-\tau-1} = 0 \\ l = p^s - p^{s-\tau} + \beta p^{s-\tau-1} + 1 \end{cases} \tag{5}$$

or

$$\begin{cases} l = p^s - p^{s-\tau} + \beta p^{s-\tau-1} + 1 \\ \beta = p - 2 \\ \tau = s - 1 \end{cases} \tag{6}$$

Eq. (5) is equivalent to $(\tau = 0, s = 1, l = \beta + 1)$. While Eq. (6) is equivalent to $l = p^s - 1$. The lemma is then proved. □

Theorem 11. *Let $\mathcal{C} = \langle g(x) \rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^{7p^s} - \lambda \rangle$ be a non-trivial λ-constacyclic code of length $7p^s$ over $\mathbb{F}_{p^m}$, where $g(x)$ is a monic divisor of $x^{7p^s} - \lambda$. Then $\mathcal{C}$ is an MDS code if and only if either $s = 0$ or $\deg g = 1$ or $\deg g = 7p^s - 1$.*

Proof. We observe that $\mathcal{C}$ is an MDS code if and only if $d_H(\mathcal{C}) = 1 + \deg g$. By Theorem 3, this condition holds when $s = 0$. Therefore, we only need to consider the case when $s \ge 1$. Furthermore, if $\deg g = 1$ then $g(x) = x - \alpha^i$ for some integer $0 \le i \le 6$ such that $\alpha^i \in \mathbb{F}_{p^m}$, and then $d_H(\mathcal{C}) = 2 = 1 + \deg g$ (by Theorem 9). Similarly, if $\deg g = 7p^s - 1$ then g has exactly one irreducible factor of degree strictly smaller than p^s, namely $(x - \alpha^i)^{p^s - 1}$, and then $d_H(\mathcal{C}) = 7\mathcal{M}(p^s - 1) = 7p^s = \deg g + 1$. This proves the "if" part of the theorem.

Suppose now that $\mathcal{C}$ is a non-trivial MDS code, i.e., $\mathcal{C} \ne \{0\}, \mathcal{C} \ne \mathbb{F}_{p^m}^{7p^s}$ and $d_H(\mathcal{C}) = \deg g + 1$. We will prove that $\deg g = 1$ or $\deg g = 7p^s - 1$ holds. It is noted that $\mathcal{C}$ must be one of the forms listed in the five cases in Theorem 9.

- **Case 1a**: $7 \mid p^m - 1$ and $\lambda \notin \langle \beta^7 \rangle$. Then $g(x) = (x^7 - \gamma)^{e_0}$ for some integers $1 \le e_0 \le p^s - 1$ and $\gamma \in \mathbb{F}_q^*$ such that $x^7 - \gamma$ is irreducible. By Theorem 9 and Lemma 10, we have
$$d_H(\mathcal{C}) = \mathcal{M}(e_0) \le e_0 + 1 < 7e_0 + 1 = \deg g + 1.$$
Therefore, there is no MDS code in this case. This case is excluded.
- **Case 1b**: $7 \mid p^m - 1$ and $\lambda \in \langle \beta^7 \rangle$. Then $g(x) = \prod_{i=0}^{6}(x - \zeta\alpha^i)^{e_i}$ for some integers $0 \le e_i \le p^s$ and $0 \le i \le 6$. Thus $\deg g = \sum_{j=0}^{6} e_j$. Without loss of generality, we can assume that $0 \le e_0 \le e_1 \le \cdots \le e_6 \le p^s$. By Theorem 7, we have

$$d_H(\mathcal{C}) = \min\{7\mathcal{M}(e_0), 6\mathcal{M}(e_1), 5\mathcal{M}(e_2), 4\mathcal{M}(e_3), 3\mathcal{M}(e_4), 2\mathcal{M}(e_5), \mathcal{M}(e_6)\} \tag{7}$$

Let k be the largest index such that $e_k < p^s$, i.e.,
$$0 \le e_0 \le \ldots \le e_k < e_{k+1} = p^s.$$
It is noted that such k exists because $\mathcal{C}$ is nontrivial. Since $\mathcal{M}(p^s) = \infty$ and $\mathcal{M}(e) \le e + 1$ for every $0 \le e \le p^s - 1$ (see Lemma 10), we have
$$\begin{aligned} d_H(\mathcal{C}) &\le (7-k)\mathcal{M}(e_k) \le (7-k)(e_k+1) \\ &\le e_k + 1 + (6-k)p^s = e_k + 1 + (e_{k+1} + \cdots + e_6) \\ &\le 1 + \deg g. \end{aligned}$$

  - **Case 1b.1:** $0 < k < 6$ and $e_0 > 0$. Then $e_k + 1 + (e_{k+1} + \cdots + e_6) < 1 + \deg g$, and hence, $d_H(\mathcal{C}) \le \deg g$. There is no MDS code in this case. This case is excluded.
  - **Case 1b.2:** $0 < k < 6$ and $e_0 = 0$. Then $d_H(\mathcal{C}) \le 7\mathcal{M}(e_0) = 7 < p^s = e_6 \le \deg g$. There is no MDS code in this case. This case is excluded.
  - **Case 1b.3:** $k = 0$. If so, $d_H(\mathcal{C}) = \deg g + 1$ only if the equality $(7-k)(e_k+1) = e_k + 1 + (6-k)p^s$ holds. Hence, $e_0 = p^s - 1, e_1 = \ldots = e_6 = p^s$.
  - **Case 1b.4:** $k = 6$. In this case, the equality $e_k + 1 + (e_{k+1} + \cdots + e_6) = 1 + \deg g$ holds only if $e_0 = e_1 = \cdots = e_5 = 0$. If so, $d_H(\mathcal{C}) = 2\mathcal{M}(e_5) = 2$. Hence, $d_H(\mathcal{C}) = \deg g + 1$ only if $e_6 = 1$.

  In summary, $\mathcal{C}$ is an MDS code only if either ($k = 0$, $e_0 = p^s - 1$ and $e_1 = \cdots = e_6 = p^s$) or ($k = 6$, $e_0 = e_1 = e_2 = e_3 = e_4 = e_5 = 0$) and $e_6 = 1$. This is exactly the case when $\deg g = 1$ and $7p^s - 1$.
- **Case 2**: $p^m \equiv 6 \mod 7$. Then $g(x) = \left\langle (x-\zeta)^{e_0} f_1(\zeta^{-1}x)^{e_1} f_2(\zeta^{-1}x)^{e_2} f_3(\zeta^{-1}x)^{e_3} \right\rangle$ for some $0 \le e_0, e_1, e_2, e_3 \le p^s$. In this case $\deg g = e_0 + 2e_1 + 2e_2 + 2e_3$. Without loss of generality, we can assume that $e_1 \le e_2 \le e_3$. By Theorem 9, we have

$$d_H(\mathcal{C}) = \begin{cases} \min\{7\mathcal{M}(e_0), 5\mathcal{M}(e_1), 3\mathcal{M}(e_2), \mathcal{M}(e_3)\}, & \text{if } e_0 \le e_1 \le e_2 \le e_3, \\ \min\{6\mathcal{M}(e_1), 5\mathcal{M}(e_0), 3\mathcal{M}(e_2), \mathcal{M}(e_3)\}, & \text{if } e_1 \le e_0 \le e_2 \le e_3, \\ \min\{6\mathcal{M}(e_1), 4\mathcal{M}(e_2), 3\mathcal{M}(e_0), \mathcal{M}(e_3)\}, & \text{if } e_1 \le e_2 \le e_0 \le e_3, \\ \min\{6\mathcal{M}(e_1), 4\mathcal{M}(e_2), 2\mathcal{M}(e_3), \mathcal{M}(e_0)\}, & \text{if } e_1 \le e_2 \le e_3 \le e_0. \end{cases} \tag{8}$$

  We split this case into the following subcases as follows:
  - **Case 2.1:** $e_3 < p^s$ and $e_0 \le e_3$. Then $d_H(\mathcal{C}) \le \mathcal{M}(e_3) \le e_3 + 1 = 1 + \deg g - (e_0 + 2e_1 + 2e_2 + e_3)$. Hence, $\mathcal{C}$ is an MDS code only if $e_0 = e_1 = e_2 = e_3 = 0$, a trivial code.
  - **Case 2.2:** $e_3 < e_0$. Then $d_H(\mathcal{C}) \le 2\mathcal{M}(e_3) \le 2e_3 + 2 = 1 + \deg g + (1 - e_0 - 2e_1 - 2e_2) \le 1 + \deg g$. It can be verified that
  $$1 - e_0 - 2e_1 - 2e_2 = 0 \Leftrightarrow e_0 = 1, e_1 = e_2 = 0.$$
  Since $e_3 < e_0 = 1$, we obtain $e_3 = 0$. Hence, $\deg g = 1$, as required.
  - **Case 2.3:** $e_3 = p^s, e_2 < p^s$. Then $d_H(\mathcal{C}) \le 4\mathcal{M}(e_2) \le 4e_2 + 4 \le \deg g + 1 + (3 - e_0 - 2e_1 + 2e_2 - 2p^s)$. Since $e_2 \le p^s - 1$, we have $3 - e_0 - 2e_1 + 2e_2 - 2p^s \le 1 - e_0 - 2e_1 \le 1$. It can be verified easily that
  $$\begin{cases} 3 - e_0 - 2e_1 + 2e_2 - 2p^s = 0 \Leftrightarrow e_0 = 1, e_1 = 0, e_2 = p^s - 1, \\ 3 - e_0 - 2e_1 + 2e_2 - 2p^s = 1 \Leftrightarrow e_0 = 0, e_1 = 0, e_2 = p^s - 1. \end{cases}$$

However, if $e_0 = 0, 1$ then $d_H(\mathcal{C}) \leq 14 < 2p^s \leq \deg g$. Hence, there is no MDS code in this case.

– **Case 2.4:** $e_2 = e_3 = p^s$ and $e_1 < p^s$. Then

$$d_H(\mathcal{C}) \leq 6\mathcal{M}(e_1) \leq 6e_1 + 6 = \deg g + 1 + (5 + 4e_1 - e_0 - 4p^s).$$

Since $e_1 \leq p^s - 1$, we have $5 + 4e_1 - e_0 - 4p^s \leq 1 - e_0$. It can be verified easily that

$$\begin{cases} 5 + 4e_1 - e_0 - 4p^s = 0 \Leftrightarrow e_0 = 1 \text{ and } e_1 = p^s - 1, \\ 5 + 4e_1 - e_0 - 4p^s = 1 \Leftrightarrow e_0 = 0 \text{ and } e_1 = p^s - 1. \end{cases}$$

However, if $e_0 \leq 1$ then $d_H(\mathcal{C}) \leq 14 < 2p^s \leq \deg g$. Hence, there is no MDS code in this case.

– **Case 2.5:** $e_1 = e_2 = e_3 = p^s$. Then $e_0 < p^s$ and

$$d_H(\mathcal{C}) = 7\mathcal{M}(e_0) \leq 7e_0 + 7 \leq \deg g + 1.$$

The equality $d_H(\mathcal{C}) = \deg g + 1$ holds only if $7e_0 + 7 = e_0 + 6p^s + 1$ or $e_0 = p^s - 1$. Hence, $\deg g = 7p^s - 1$ as required.

- **Case 3**: $p^m \equiv 2, 4 \mod 7$. Then $g(x) = (x - \zeta)^{e_0} f_4(x)^{e_1} f_5(x)^{e_2}$ for some $0 \leq e_0, e_1, e_2 \leq p^s$. In this case, $\deg g = e_0 + 3e_1 + 3e_2$. Without loss of generality, we can assume that $e_1 \leq e_2$. By Theorem 9, we have

$$d_H(\mathcal{C}) = \begin{cases} \min\{7\mathcal{M}(e_0), 4\mathcal{M}(e_1), \mathcal{M}(e_2)\}, & \text{if } e_0 \leq e_1 \leq e_2, \\ \min\{5\mathcal{M}(e_1), 4\mathcal{M}(e_0), \mathcal{M}(e_2)\}, & \text{if } e_1 \leq e_0 \leq e_2, \\ \min\{5\mathcal{M}(e_1), 2\mathcal{M}(e_2), \mathcal{M}(e_0)\}, & \text{if } e_1 \leq e_2 \leq e_0. \end{cases}$$

We split this case to three subcases as follows:

– **Case 3.1:** $e_2 < p^s$. By Lemma 10, we have $d_H(\mathcal{C}) \leq 2\mathcal{M}(e_2) \leq 2e_2 + 2 = \deg g + (2 - e_0 - 3e_1 - e_2) \leq \deg g + 1$ (since $\mathcal{C}$ is non-trivial). Now, we can verify that

$$2 - e_0 - 3e_1 - e_2 = 1 \Leftrightarrow (e_0 = 1, e_1 = 0, e_2 = 0) \vee (e_0 = 0, e_1 = 0, e_2 = 1).$$

Hence, $\mathcal{C}$ is an MDS code, i.e., $d_H(\mathcal{C}) = \deg g + 1$, if and only if $e_0 = 0, e_1 = 0, e_2 = 1$. This is exactly when $\deg g = 1$, as required.

– **Case 3.2:** $e_1 < p^s, e_2 = p^s$. Then $d_H(\mathcal{C}) \leq 5\mathcal{M}(e_1) \leq 5e_1 + 5 \leq \deg g + (5 - 2p^s) \leq \deg g$. Hence, there is no MDS code in this case.

– **Case 3.3:** $e_1 = e_2 = p^s$. Then $d_H(\mathcal{C}) = 7\mathcal{M}(e_0) \leq 7e_0 + 7 \leq \deg g + 1$. The equality $d_H(\mathcal{C}) = \deg g + 1$ holds if and only if $e_0 = p^s - 1$. Hence, $\mathcal{C}$ is an MDS code if and only if $\deg g = 7p^s - 1$

- **Case 4:** $p^m \equiv 3, 5 \mod 7$. Then $g(x) = (x - \zeta)^{e_0} f_6(\zeta^{-1}x)^{e_1}$ for some $e_i = 0, 1, \ldots, p^s$ and $i = 0, 1$. In this case, $\deg g = e_0 + 6e_1$. By Theorem 9 again, we have

$$d_H(\mathcal{C}) = \begin{cases} \min\{7\mathcal{M}(e_0), \mathcal{M}(e_1)\}, & \text{if } e_0 \leq e_1, \\ \min\{2\mathcal{M}(e_1), \mathcal{M}(e_0)\}, & \text{if } e_1 \leq e_0. \end{cases}$$

– **Case 4.1:** $e_1 \leq p^s - 1$. Since $\mathcal{C}$ is non-trivial, we have

$$d_H(\mathcal{C}) \leq 2\mathcal{M}(e_1) \leq 2e_1 + 2 = \deg g + 1 + (1 - e_0 - 4e_1) \leq \deg g + 1.$$

Hence, $d_H(\mathcal{C}) = 1 + \deg g$ holds only if $e_0 = 1, e_1 = 0$ or $\deg g = 1$.

– **Case 4.2:** $e_1 = p^s$. In this case, $e_0 < p^s$ because $\mathcal{C}$ is non-trivial. It follows that

$$d_H(\mathcal{C}) = 7\mathcal{M}(e_0) \leq 7e_0 + 7 \leq 1 + e_0 + 6(1 + e_0) \leq 1 + \deg g.$$

If $d_H(C) = 1 + \deg g$ then $1 + e_0 = p^s$ or $e_0 = p^s - 1$ or $\deg g = 7p^s - 1$, as required.

□

7. Self-orthogonal, dual-containing, and self-dual repeated-root constacyclic codes of length $7p^s$

For a linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$, its *dual* $\mathcal{C}^\perp$ is defined as

$$\mathcal{C}^\perp := \{x \in \mathbb{F}_q \text{ such that } x \cdot y = 0, \forall y \in \mathcal{C}\}.$$

The code $\mathcal{C}$ is said to be *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^\perp$, *dual-containing* if $\mathcal{C}^\perp \subseteq \mathcal{C}$, and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. If $\mathcal{C}$ is a cyclic code of length n over $\mathbb{F}_q$, then so is $\mathcal{C}^\perp$. In this case, the generator polynomial of $\mathcal{C}^\perp$ can be determined directly from the generator polynomial of $\mathcal{C}$ via the following well-known result.

Proposition 12. *Let $\mathcal{C} = \langle g(x) \rangle$ be a λ-constacyclic code in $\mathbb{F}_q[x]/\langle x^n - \lambda \rangle$ generated by a monic factor $g(x)$ of $x^n - \lambda$. Then the dual code $C^\perp$ is a λ^{-1}-constacyclic code in $\mathbb{F}_q[x]/\langle x^n - \lambda \rangle$ generated by the polynomial $h^*(x) := h(0)^{-1} x^{\deg h} h(1/x)$, where $h(x) = \frac{x^n - \lambda}{g(x)}$.*

We are now going to characterize all self-orthogonal, dual-containing, and self-dual codes among the class of repeated-root λ-constacyclic codes of length $7p^s$ over $\mathbb{F}_q$.

Theorem 13. *Let $p \neq 7$ be a prime number. Then all self-orthogonal/dual-containing/self-dual repeated-root λ-constacyclic codes of length $7p^s$ over $\mathbb{F}_q$ are either negacyclic or cyclic codes and are listed in Table 4.*

Proof. The set of all repeated-root λ-constacyclic codes of length $7p^s$ over $\mathbb{F}_q$ are classified in Theorem 9 and they are listed in Table 3. We determine self-orthogonal/dual-containing/self-dual constacyclic codes from this table case by case.

- **Case 1a:** $7 \mid p^m - 1$ and $\lambda \notin \langle \beta^7 \rangle$. Then there is $\gamma \in \mathbb{F}_q^*$ such that $\lambda = \gamma^{p^s}$, $x^7 - \gamma$ is irreducible over $\mathbb{F}_q$ and $\mathcal{C} = \langle (x^7 - \gamma)^{e_0} \rangle$. In this case, the generator polynomial of $\mathcal{C}^\perp$ is
$$h^*(x) := h(0)^{-1} x^{\deg h} h(1/x)$$
where $h(x) = \dfrac{x^{7p^s} - \lambda}{(x^7 - \gamma)^{e_0}} = (x^7 - \gamma)^{p^s - e_0}$. Hence,
$$h^*(x) = (-\gamma)^{e_0 - p^s} x^{7p^s - 7e_0} \left(\frac{1}{x^7} - \gamma \right)^{p^s - e_0} = (x^7 - \gamma^{-1})^{p^s - e_0}.$$
Therefore, $\mathcal{C}$ is self-orthogonal if and only if $(x^7 - \gamma^{-1})^{p^s - e_0}$ is a divisor of $(x^7 - \gamma)^{e_0}$. Equivalently, $\gamma^2 = 1$ and $p^s - e_0 \leq e_0$. Since $x^7 - \gamma$ is irreducible, $\gamma = -1$. Hence, $\mathcal{C}$ is self-orthogonal if and only if $\lambda = -1$ and $e_0 \geq p^s/2$. Similarly, $\mathcal{C}$ is dual-containing if and only if $\lambda = -1$ and $e_0 \leq p^s/2$. Besides, if $p = 2$ and $\lambda = -1$ then $x^7 - \gamma = x^7 - 1$ is not irreducible. Therefore, there is no self-dual code in this case.
- **Case 1b:** $7 \mid p^m - 1$ and $\lambda \in \langle \beta^7 \rangle$. Then there is $\zeta \in \mathbb{F}_q$: $\lambda = \zeta^{7p^s}$ and $\mathcal{C} = \langle \prod_{i=0}^{6} (x - \zeta \alpha^i)^{e_i} \rangle$. In this case, the generator polynomial of $\mathcal{C}^\perp$ is
$$h^*(x) = \prod_{i=0}^{6} (-\zeta^{-1} \alpha^{-i})^{p^s - e_i} (1 - \zeta \alpha^i x)^{p^s - e_i} = \prod_{i=0}^{6} (x - \zeta^{-1} \alpha^{7-i})^{p^s - e_i}$$
By the same argument as in Case 1a, $\mathcal{C}$ is self-orthogonal if and only if $\lambda^2 = 1$, $e_0 \geq p^s/2$, and $e_1 + e_{7-i} \geq p^s$ for $1 \leq i \leq 3$. Similarly, $\mathcal{C}$ is dual-containing if and only if $e_0 \leq p^s/2$, and $e_i + e_{7-i} \leq p^s$ for $1 \leq i \leq 3$. Finally, $\mathcal{C}$ is self-dual if and only if $p = 2$ and $e_0 = e_1 + e_6 = e_2 + e_5 = e_3 + e_4 = p^s/2 = 2^{s-1}$.
- **Case 2, Case 3**, and **Case 4** are similar. So we omit them.

□

TABLE 4. Self-orthogonal/dual-containing/self-dual λ-constacyclic codes of length $7p^s$ over $\mathbb{F}_q$. Here, $\zeta = \pm 1$.

	The λ-constacyclic code $\mathcal{C}$	Self-orthogonal	Dual-containing	Self-dual
Case 1a	$\langle (x^7 + \gamma)^{e_0} \rangle$	$e_0 \geq p^s/2$	$e_0 \leq p^s/2$	-
Case 1b	$\langle \prod_{i=0}^{6} (x - \alpha^i)^{e_i} \rangle$	$e_0 \geq p^s/2$, $e_i + e_{7-i} \geq p^s$	$e_0 \leq p^s/2$, $e_i + e_{7-i} \leq p^s$	$p = 2, e_0 = 2^{s-1}$, $e_i + e_{7-i} = 2^{s-1}$
Case 2	$\langle (x - \zeta)^{e_0} f_1(\zeta^{-1}x)^{e_1} f_2(\zeta^{-1}x)^{e_2} f_3(\zeta^{-1}x)^{e_3} \rangle$	$e_i \geq p^s/2$	$e_i \leq p^s/2$	-
Case 3	$\langle (x - \zeta)^{e_0} f_4(\zeta^{-1}x)^{e_1} f_5(\zeta^{-1}x)^{e_2} \rangle$	$e_0 \geq p^s/2$, $e_1 + e_2 \geq p^s$	$e_0 \leq p^s/2$, $e_1 + e_2 \leq p^s$	$p = 2, e_0 = 2^{s-1}$, $e_1 + e_2 = 2^{s-1}$
Case 4	$\langle (x - \zeta)^{e_0} f_6(\zeta^{-1}x)^{e_1} \rangle$	$e_0, e_1 \geq p^s/2$	$e_0, e_1 \leq p^s/2$	-

Acknowledgements

This paper was completed when the authors were working at Vietnam Institute for Advance Study in Mathematics (VIASM). The authors would like to thank the VIASM for providing a fruitful research environment and extending support and hospitality during their visit.

References

[1] G. K. Bakshi and M. Raka, A class of constacyclic codes over a finite field, Finite Fields Appl. 18 (2) (2012) 362–377.
[2] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seemann, On repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (2) (1991) 337–342.
[3] B. Chen, H. Q. Dinh, H. Lie, Repeated-root constacyclic codes of length lp^s and their duals, Discrete Appl. Math. 177 (2014), 60–70.
[4] B. Chen, H. Q. Dinh, H. Liu, Repeated-root constacyclic codes of length $2^m p^n$, Finite Fields Appl. 33 (2015) 137–159.
[5] D. Cox, J. Little, D. OShea, Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra. Springer Science & Business Media (2015).
[6] H. Q. Dinh, On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions, Finite Fields Appl. 14 (1) (2008) 22–40.
[7] H. Q. Dinh, Repeated-root constacyclic codes of length $2p^s$, Finite Fields Appl. 18 (2012) 133–143.
[8] H. Q. Dinh, Structure of repeated-root constacyclic codes of length $3p^s$ and their duals, Discrete Math. 313 (9) (2013) 983–991.
[9] H. Q. Dinh, On repeated-root constacyclic codes of length 4ps, Asian Eur. J. Math. 6 (2013) 1–25.
[10] H. Q. Dinh, Structure of repeated-root cyclic codes and negacyclic codes of length $6p^s$ and their duals, Contemp. Math. 609 (2014) 69–87.
[11] H. Q. Dinh, X. Wang, H. Liu, S. Sriboonchitta, On the Hamming distances of repeated-root constacyclic codes of length $4p^s$, Discrete Math. 342 (2019) 1456–1470.
[12] H. Q. Dinh, X. Wang, J. Sirisrisakulchai, On the Hamming Distances of Constacyclic Codes of Length $5p^s$, IEEE Access 8 (2020) 46242–46254.
[13] H. Q. Dinh, X. Wang, H. Liu, W. Yamaka, Hamming distances of constacyclic codes of length $3p^s$ and optimal codes with respect to the Griesmer and Singleton bounds. Finite Fields Appl. 70 (2021) 101794.
[14] H. Q. Dinh, X. Wang, P. Maneejuk, On the Hamming Distance of Repeated-Root Cyclic Codes of Length $6p^s$. IEEE Access 8 (2020) 39946–39958.
[15] R. Hill, A first course in coding theory, Clarendon Press (1997).
[16] J. H. van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (2) (1991) 343–345.
[17] J.H. van Lint, Introduction to Coding Theory, 3rd edition, Springer (1998).
[18] L. Liu, L. Q. Li, X. S. Kai, S. X. Zhu, Repeated-root constacyclic codes of length $3^l p^n$ and their dual codes, Finite Fields Appl. 42 (2016) 269–295.
[19] S. R. Lopez-Permouth, H. Ozadam, F. Ozbudak, S. Szabo, Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes, Finite Fields Appl. 19 (1) (2013) 16–38.
[20] C.-S. Nedeloaia, Weight distributions of cyclic self-dual codes, IEEE Trans. Inform. Theory 49 (6) (2003) 1582–1591.
[21] H. Ozadam, F. Ozbudak, The minimum Hamming distance of cyclic codes of length $2p^s$, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Lecture Notes in Computer Science), Springer 5527 (2009) 92–100.
[22] A. Sharma, S. Rani, Repeated-root constacyclic codes of length $4^m p^n$, Finite Fields Appl. 40 (C) (2016) 163–200.
[23] L. Z. Tang, C. B. Soh, E. Gunawan, A note on the q-ary image of a q^m-ary repeated-root cyclic code, IEEE Trans. Inform. Theory 43 (2) (1997) 732–737.

Appendix A. Maple code for the proof of Theorem 3

In this section, we provide the Maple code for the completeness of the proof of Theorem 3. The code and the results are given below case by case.

A.1. Case 3: when $\deg g = 2$ and $g(x) = (x - \alpha^{i_1})(x - \alpha^{i_2})$

In this case, we need to show that for all integers i_1, i_2, r_1, r_2 such that $0 \le i_1 < i_2 \le 6$ and $0 \le r_1 < r_2 \le 7$, the resultant $R_{i_1,i_2,r_1,r_2} := \mathrm{res}_x(D_{i_1,i_2,r_1,r_2}(x), x^7 - 1)$ is always an integer of the form $\pm 2^u 3^v 5^w$ for some nonnegative integers u, v and w, or equivalently, their prime factors are just 2, 3 or 5. The following codes are to determine the set of prime factors for the resultants R_{i_1,i_2,r_1,r_2} (which is "*Rir*" in the codes). The results are indeed $\{2, 3, 5\}$.

```
> restart;
> with(LinearAlgebra): with(NumberTheory):
> S1 := x^i1 + x^i2:
  S2 := x^i1+i2:
> seq(v[i], i = 1 .. 7):
> v[1] := Vector([S2, 0, 0, 0, 0]):
  v[2] := Vector([-S1, S2, 0, 0, 0]):
  v[3] := Vector([1, -S1, S2, 0, 0]):
  v[4] := Vector([0, 1, -S1, S2, 0]):
  v[5] := Vector([0, 0, 1, -S1, S2]):
  v[6] := Vector([0, 0, 0, 1, -S1]):
  v[7] := Vector([0, 0, 0, 0, 1]):
  G := <<v[1]> | <v[2]> | <v[3]> | <v[4]> | <v[5]> | <v[6]> | <v[7]>>;
```

$$G := \begin{bmatrix} x^{i1+i2} & -x^{i1}-x^{i2} & 1 & 0 & 0 & 0 & 0 \\ 0 & x^{i1+i2} & -x^{i1}-x^{i2} & 1 & 0 & 0 & 0 \\ 0 & 0 & x^{i1+i2} & -x^{i1}-x^{i2} & 1 & 0 & 0 \\ 0 & 0 & 0 & x^{i1+i2} & -x^{i1}-x^{i2} & 1 & 0 \\ 0 & 0 & 0 & 0 & x^{i1+i2} & -x^{i1}-x^{i2} & 1 \end{bmatrix}$$

```
> ListPrimeFactors := { }:
  for i1 from 0 to 5 do
      for i2 from i1 + 1 to 6 do
          for r1 from 1 to 6 do
              for r2 from r1 + 1 to 7 do
                  Gir := DeleteColumn(G, [r1, r2]);
                  Dir := Determinant(Gir);
                  Rir := resultant(Dir, x^7 - 1, x);
                  Rir := PrimeFactors(Rir);
                  ListPrimeFactors := {op(ListPrimeFactors), Rir}
              end do
          end do
      end do
  end do:
  ListPrimeFactors;
```

$$\{2, 3, 5\}$$

A.2. Case 4: when $\deg g = 3$ and $g(x) = (x - \alpha^{i_1})(x - \alpha^{i_2})(x - \alpha^{i_3})$

In this case, we need to show that for all integers $i_1, i_2, i_3, r_1, r_2, r_3$ such that $0 \le i_1 < i_2 < i_3 \le 6$ and $0 \le r_1 < r_2 < r_3 \le 7$, the resultant $R_{i_1,i_2,i_3,r_1,r_2,r_3} := \mathrm{res}_x(D_{i_1,i_2,i_3,r_1,r_2,r_3}(x), x^7 - 1)$ has only prime factors 2, 3 or 5. The following codes are to determine the set of prime factors for the resultants $R_{i_1,i_2,i_3,r_1,r_2,r_3}$ (which is "*Rir*" in the codes). The results are indeed $\{2, 3, 5\}$.

```
> restart;
> with(LinearAlgebra): with(NumberTheory):
> S1 := x^(i1+i2+i3):
  S2 := x^(i2+i3) + x^(i3+i1) + x^(i1+i2):
  S3 := x^(i1+i2+i3):
> seq(v[i], i = 1 .. 7):
> v[1] := Vector([-S3, 0, 0, 0]):
  v[2] := Vector([S2, -S3, 0, 0]):
  v[3] := Vector([-S1,S2,-S3, 0]):
  v[4] := Vector([1, -S1, S2, -S3]):
  v[5] := Vector([0, 1, -S1, S2]):
  v[6] := Vector([0, 0, 1, -S1]):
  v[7] := Vector([0, 0, 0, 1]):
  G := <<v[1]> | <v[2]> | <v[3]> | <v[4]> | <v[5]> | <v[6]> | <v[7]>>;
```

$$G := [[-x^{i1+i2+i3}, x^{i1+i2} + x^{i1+i3} + x^{i2+i3}, -x^{i1} - x^{i2} - x^{i3}, 1, 0, 0, 0],$$
$$[0, -x^{i1+i2+i3}, x^{i1+i2} + x^{i1+i3} + x^{i2+i3}, -x^{i1} - x^{i2} - x^{i3}, 1, 0, 0],$$
$$[0, 0, -x^{i1+i2+i3}, x^{i1+i2} + x^{i1+i3} + x^{i2+i3}, -x^{i1} - x^{i2} - x^{i3}, 1, 0],$$
$$[0, 0, 0, -x^{i1+i2+i3}, x^{i1+i2} + x^{i1+i3} + x^{i2+i3}, -x^{i1} - x^{i2} - x^{i3}, 1]]$$

```
> ListPrimeFactors := { }:
  for i1 from 0 to 5 do
      for i2 from i1 + 1 to 6 do
          for i3 from i2 + 1 to 7 do
              for r1 from 1 to 5 do
                  for r2 from r1 + 1 to 6 do
                      for r3 from r2 + 1 to 7 do
                          Gir := DeleteColumn(G, [r1, r2, r3]);
```

```
                    Dir := Determinant(Gir);
                    Rir := resultant(Dir, x^7 - 1, x);
                    Rir := PrimeFactors(Rir);
                    ListPrimeFactors := {op(ListPrimeFactors), op(Rir)}
                end do
            end do
        end do
    end do
end do:
ListPrimeFactors;
```

$$\{2, 3, 5\}$$

A.3. Case 5: when $\deg g = 4$ and $g(x) = (x - \alpha^{i_1})(x - \alpha^{i_2})(x - \alpha^{i_3})(x - \alpha^{i_4})$

In this case, we need to show that for all integers $i_1, i_2, i_3, i_4, r_1, r_2, r_3, r_4$ such that $0 \le i_1 < i_2 < i_3 < i_4 \le 6$ and $0 \le r_1 < r_2 < r_3 < r_4 \le 7$, the resultant $R_{i_1,i_2,i_3,i_4,r_1,r_2,r_3,r_4} := \mathrm{res}_x(D_{i_1,i_2,i_3,i_4,r_1,r_2,r_3,r_4}(x), x^7 - 1)$ has only prime factors 2, 3 or 5. The following codes are to determine the set of prime factors for the resultants $R_{i_1,i_2,i_3,i_4,r_1,r_2,r_3,r_4}$ (which is "*Rir*" in the codes). The results are again $\{2, 3, 5\}$.

```
> restart;
> with(LinearAlgebra): with(NumberTheory):
> S1 := x^i1 + x^i2 + x^i3 + x^i4:
  S2 := x^(i1+i2) + x^(i1+i3) + x^(i1+i4) + x^(i2+i3) + x^(i2+i4) + x^(i3+i4):
  S3 := x^(i1+i2+i3) + x^(i1+i2+i4) + x^(i1+i3+i4) + x^(i2+i3+i4):
  S4 := x^(i1+i2+i3+i4):
> seq(v[i], i = 1 .. 7):
> v[1] :=Vector([S4, 0, 0]):
  v[2] := Vector([-S3, S4, 0]):
  v[3] := Vector([S2, -S3, S4]):
  v[4] := Vector([-S1, S2, -S3]):
  v[5] := Vector([1, -S1, S2]):
  v[6] := Vector([0, 1, -S1]):
  v[7] := Vector([0, 0, 1]):
  G := <<v[1]> | <v[2]> | <v[3]> | <v[4]> | <v[5]> | <v[6]> | <v[7]>>;
```

$$G := [[x^{i1+i2+i3+i4}, -x^{i1+i2+i3} - x^{i1+i2+i4} - x^{i1+i3+i4} - x^{i2+i3+i4},$$
$$x^{i1+i2} + x^{i1+i3} + x^{i1+i4} + x^{i2+i3} + x^{i2+i4} + x^{i3+i4}, -x^{i1} - x^{i2} - x^{i3} - x^{i4}, 1, 0, 0],$$
$$[0, x^{i1+i2+i3+i4}, -x^{i1+i2+i3} - x^{i1+i2+i4} - x^{i1+i3+i4} - x^{i2+i3+i4},$$
$$x^{i1+i2} + x^{i1+i3} + x^{i1+i4} + x^{i2+i3} + x^{i2+i4} + x^{i3+i4}, -x^{i1} - x^{i2} - x^{i3} - x^{i4}, 1, 0],$$
$$[0, 0, x^{i1+i2+i3+i4}, -x^{i1+i2+i3} - x^{i1+i2+i4} - x^{i1+i3+i4} - x^{i2+i3+i4},$$
$$x^{i1+i2} + x^{i1+i3} + x^{i1+i4} + x^{i2+i3} + x^{i2+i4} + x^{i3+i4}, -x^{i1} - x^{i2} - x^{i3} - x^{i4}, 1]]$$

```
> ListPrimeFactors := { }:
  for i1 from 1 to 4 do
      for i2 from i1 + 1 to 5 do
          for i3 from i2 + 1 to 6 do
              for i4 from i3 + 1 to 7 do
                  for r1 from 1 to 4 do
                      for r2 from r1 + 1 to 5 do
                          for r3 from r2 + 1 to 6 do
                              for r4 from r3 + 1 to 7 do
                                  Gir := DeleteColumn(G, [r1, r2, r3, r4]);
                                  Dir := Determinant(Gir);
                                  Rir := resultant(Dir, x^7 - 1, x);
                                  Rir := PrimeFactors(Rir);
                                  ListPrimeFactors := {op(ListPrimeFactors), op(Rir)}
```

```
                    end do
                end do
            end do
        end do
    end do
end do
end do:
ListPrimeFactors;
```

$$\{2, 3, 5\}$$

A.4. Case 6: when $\deg g = 5$ and $g(x) = (x-\alpha^{i_1})(x-\alpha^{i_2})(x-\alpha^{i_3})(x-\alpha^{i_4})(x-\alpha^{i_5})$

In this case, we need to show that for all integers $i_1, i_2, i_3, i_4, i_5, r_1, r_2, r_3, r_4, r_5$ such that $0 \le i_1 < i_2 < i_3 < i_4 < i_5 \le 6$ and $0 \le r_1 < r_2 < r_3 < r_4 < r_5 \le 7$, the resultant $R_{i_1,i_2,i_3,i_4,i_5,r_1,r_2,r_3,r_4,r_5} := \mathrm{res}_x(D_{i_1,i_2,i_3,i_4,i_5,r_1,r_2,r_3,r_4,r_5}(x), x^7-1)$ has only prime factors 2, 3 or 5. The following codes are to determine the set of prime factors for the resultants $R_{i_1,i_2,i_3,i_4,i_5,r_1,r_2,r_3,r_4,r_5}$ (which is "*Rir*" in the codes). The results are still $\{2, 3, 5\}$.

```
> restart;
> with(LinearAlgebra): with(NumberTheory):
> S1 := x^i1 + x^i2 + x^i3 + x^i4 + x^i5:
  S2 := x^(i1+i2) + x^(i1+i3) + x^(i1+i4) + x^(i1+i5) + x^(i2+i3) + x^(i2+i4) + x^(i2+i5) + x^(i3+i4) + x^(i3+i5) + x^(i4+i5):
  S3 := x^(i1+i2+i3) + x^(i1+i2+i4) + x^(i1+i2+i5) + x^(i1+i3+i4) + x^(i1+i3+i5) + x^(i1+i4+i5) + x^(i2+i3+i4) + x^(i2+i3+i5) +
  x^(i2+i4+i5) + x^(i3+i4+i5):
  S4 := x^(i1+i2+i3+i4) + x^(i1+i2+i3+i5) + x^(i1+i2+i4+i5) + x^(i1+i3+i4+i5) + x^(i2+i3+i4+i5):
  S5 := x^(i1+i2+i3+i4+i5):
> seq(v[i], i = 1 .. 7):
> v[1]:=Vector([-S5, 0]):
  v[2]:=Vector([S4, -S5]):
  v[3]:=Vector([-S3, S4]):
  v[4]:=Vector([S2, -S3]):
  v[5]:=Vector([-S1, S2]):
  v[6]:=Vector([1, -S1]):
  v[7]:=Vector([0,1]):
  G := <<v[1]> | <v[2]> | <v[3]> | <v[4]> | <v[5]> | <v[6]> | <v[7]>>;
```

$$G := [[-x^{i1+i2+i3+i4+i5}, x^{i1+i2+i3+i4} + x^{i1+i2+i3+i5} + x^{i1+i2+i4+i5} + x^{i1+i3+i4+i5} + x^{i2+i3+i4+i5}, -x^{i1+i2+i3} - x^{i1+i2+i4} - x^{i1+i2+i5} - x^{i1+i3+i4} + x^{i2+i3+i5} - x^{i1+i4+i5} - x^{i2+i3+i4} - x^{i2+i3+i5} - x^{i2+i4+i5} - x^{i3+i4+i5}, x^{i1+i2} + x^{i1+i3} + x^{i1+i4} + x^{i1+i5} + x^{i2+i3} + x^{i2+i4} + x^{i2+i5} + x^{i3+i4} + x^{i3+i5} + x^{i4+i5}, -x^{i1} - x^{i2} - x^{i3} - x^{i4} - x^{i5}, 1, 0], [0, -x^{i1+i2+i3+i4+i5}, x^{i1+i2+i3+i4} + x^{i1+i2+i3+i5} + x^{i1+i2+i4+i5} + x^{i1+i3+i4+i5} + x^{i2+i3+i4+i5}, -x^{i1+i2+i3} - x^{i1+i2+i4} - x^{i1+i2+i5} - x^{i1+i3+i4} - x^{i1+i3+i5} - x^{i1+i4+i5} - x^{i2+i3+i4} - x^{i2+i3+i5} - x^{i2+i4+i5} - x^{i3+i4+i5}, x^{i1+i2} + x^{i1+i3} + x^{i1+i4} + x^{i1+i5} + x^{i2+i3} + x^{i2+i4} + x^{i2+i5} + x^{i3+i4} + x^{i3+i5} + x^{i4+i5}, -x^{i1} - x^{i2} - x^{i3} - x^{i4} - x^{i5}, 1]]$$

```
> ListPrimeFactors := { }:
  for i1 from 0 to 3 do
      for i2 from i1 + 1 to 4 do
          for i3 from i2 + 1 to 5 do
              for i4 from i3 + 1 to 6 do
                  for i5 from i4 + 1 to 7 do
                      for r1 from 1 to 3 do
                          for r2 from r1 + 1 to 4 do
                              for r3 from r2 + 1 to 5 do
                                  for r4 from r3 + 1 to 6 do
```

```
                    for r5 from r4 + 1 to 7 do
                        Gir := DeleteColumn(G, [r1, r2, r3, r4, r5]);
                        Dir := Determinant(G1);
                        Rir := resultant(Dir, x^7 − 1, x);
                        Rir := PrimeFactors(Rir);
                        ListPrimeFactors := {op(Rir), op(ListPrimeFactors)}
                    end do
                end do
            end do
        end do
    end do
end do
end do
end do
end do:
ListPrimeFactors;
```

$$\{2, 3, 5\}$$

Hai Q. Dinh
Department of Mathematical Sciences
Kent State University
4314, Mahoning Avenue, Warren, OH, 44483, USA
E-mail address: hdinh@kent.edu

Hieu V. Ha
Faculty of Economic Mathematics
University of Economics and Law, Ho Chi Minh City, Vietnam
Vietnam National University, Ho Chi Minh City, Vietnam
Ho Chi Minh City, Vietnam
E-mail address: hieuhv@uel.edu.vn

Nghia T.H. Tran
Department of Mathematics
University of Pedagogy and Education
Ho Chi Minh City, Vietnam
E-mail address: nghiatth@hcmue.edu.vn

Thieu N. Vo
Faculty of Mathematics
Ton Duc Thang University, Ho Chi Minh City, Vietnam
Ho Chi Minh City, Vietnam
E-mail address: vongocthieu@tdtu.edu.vn