Repeated-root constacyclic codes of length ℓp^s and their duals*

Bocong Chen[1,3], Hai Q. Dinh[2], Hongwei Liu[1]

1. School of Mathematics and Statistics, Central China Normal University
Wuhan, Hubei, 430079, China
2. Department of Mathematical Sciences, Kent State University,
4314 Mahoning Avenue, Warren, OH 44483, USA
3. Division of Mathematical Sciences, School of Physical & Mathematical Sciences,
Nanyang Technological University, Singapore, 637616, Singapore

Abstract

An equivalence relation is introduced on the nonzero elements of the finite field $\mathbb{F}_{p^m}$ to classify constacyclic codes of arbitrary length over $\mathbb{F}_{p^m}$. According to the equivalence classes, all constacyclic codes of length ℓp^s over $\mathbb{F}_{p^m}$ and their duals are characterized, where ℓ is a prime different from p and s is a positive integer. Self-dual cyclic codes of length ℓp^s over $\mathbb{F}_{p^m}$ exist precisely when p is equal to two; in this case, all self-dual cyclic codes of length $2^s\ell$ over $\mathbb{F}_{2^m}$ are presented.

Keywords: Finite field, constacyclic code, cyclic code, generator polynomial, dual code.

2010 Mathematics Subject Classification: 94B05; 94B15

1 Introduction

Constacyclic codes over finite fields form a remarkable class of linear codes, as they include the important family of cyclic codes. Constacyclic codes also have practical applications as they can be efficiently encoded using simple shift registers. They have rich algebraic structures for efficient error detection and correction, which explains their preferred role in engineering.

Let $\mathbb{F}_q$ be the finite field of order $q = p^m$, where p is the characteristic of the field. Given a nonzero element λ of $\mathbb{F}_q$, λ-constacyclic codes of length n over $\mathbb{F}_q$ are classified as the ideals $\langle g(X)\rangle$ of the quotient ring $\mathbb{F}_q[X]/\langle X^n - \lambda\rangle$, where the generator polynomial $g(X)$ is the unique monic polynimial of minimum degree

*E-Mail addresses: bocong_chen@yahoo.com (B. Chen), hdinh@kent.edu (H. Q. Dinh), hwliu@mail.ccnu.edu.cn (H. Liu).

in the code, which is a divisor of $x^n - \lambda$. In this paper, we first consider the following natural question.

Under what conditions on λ and μ such that λ-constacyclic codes of length n and μ-constacyclic codes of length n have the same structures?

Particular cases of this question have been considered by many authors, even for the more general alphabets of finite rings. Wolfmann [27] showed that cyclic and negacyclic codes over $\mathbb{Z}_4$, the ring of integers modulo 4, have the same structure for odd code lengths. Dinh and López-Permouth [6] generalized that to obtain that this fact holds true for cyclic and negacyclic codes of odd lengths over any finite chain ring. When the lengths are a prime power, say p^s, Dinh [8] showed that all constacyclic codes over the finite field $\mathbb{F}_{p^m}$ of p^m elements have the same structure; and over the chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, the author gave the classification that all $(\alpha + u\beta)$-constacyclic codes have the same structures, and all γ-constacyclic codes are equivalent, for arbitrary nonzero elements α, β, γ of the field $\mathbb{F}_{p^m}$.

In the previous work [5], Chen *et al.* introduced an equivalence relation " $\cong_n$ " called isometry for the nonzero elements of $\mathbb{F}_q$ to classify constacyclic codes of length n over $\mathbb{F}_q$ such that the constacyclic codes belonging to the same isometry class have the same distance structures and the same algebraic structures. Though $\lambda \cong_n \mu$ means there exists an isometry ψ between the rings $\mathbb{F}_q[X]/\langle X^n - \lambda\rangle$ and $\mathbb{F}_q[X]/\langle X^n - \mu\rangle$, it is not easy to connect the generator polynomial of the λ-constacyclic code C with that of $\psi(C)$, and as a result, it is not easy to describe the relation between $C^\perp$ and $\psi(C)^\perp$.

In this paper, we aim to overcome this problem by considering a more specified relation than the isometry " $\cong_n$ ", that allows us to obtain a much more explicit description of the generator polynomials of all constacyclic codes. This detailed description also enables us to establish the generator polynomials of the dual codes. A new equivalence relation " $\sim_n$ " is introduced on the nonzero elements of $\mathbb{F}_q$ to classify constacyclic codes of length n over $\mathbb{F}_q$. Some necessary and sufficient conditions for any two nonzero elements of $\mathbb{F}_q$ to be equivalent to each other are presented. We show that if $\lambda \sim_n \mu$ then there exists a very explicit $\mathbb{F}_q$-algebra isomorphism φ between $\mathbb{F}_q[X]/\langle X^n - \lambda\rangle$ and $\mathbb{F}_q[X]/\langle X^n - \mu\rangle$; moreover, the generator polynomial of the λ-constacyclic code C and the generator polynomial of the μ-constacyclic code $\varphi(C)$ are linked in a very simple way.

Since every ideal of $\mathbb{F}_q[X]/\langle X^n - \lambda\rangle$ can be generated by a monic divisor of $X^n - \lambda$, it follows that the irreducible factorization of $X^n - \lambda$ in $\mathbb{F}_q[X]$ determines all λ-constacyclic codes of length n over $\mathbb{F}_q$. Most of the authors assume from the outset that the code length n is coprime to q. This condition implies that every root of $X^n - \lambda$ is a simple root in an extension field of $\mathbb{F}_q$, which provides a description of all such roots, and hence, λ-constacyclic codes, by cyclotomic cosets modulo n. In contrast to simple-root codes, constacyclic codes with p dividing n are called repeated-root constacyclic codes, which were first studied in 1967 by Berman [2], and then by several authors such as Massey *et al.* [18], Falkner *et al.* [13], Roth, Seroussi [21] and Salagean [22]. Repeated-root codes

were first investigated in the most generality in the 1990s by Castagnoli *et al.* [4], and van Lint [26], where they showed that repeated-root cyclic codes have a concatenated construction, and are not asymptotically good. However, it turns out that optimal repeated-root constacyclic codes still exist. In particular, it has been proved that self-dual cyclic codes over a finite field exist precisely when the code length is even and the characteristic of the underlying field is two [16, 15]. These motivate researchers to further study this class of codes.

Using the discrete Fourier transforms, the generator polynomials, self-dual codes, as well as some results about the minimum Lee weights of cyclic codes of oddly even length over $\mathbf{Z}_4$ were obtained in [3]. The Hamming distances of all constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ were completely determined in [7, 8]. The generator polynomials of all constacyclic codes of length $2^t p^s$ over $\mathbb{F}_{p^m}$ were given in [1], where p is an odd prime. The generator polynomials of all constacyclic codes of length ℓp^s over $\mathbb{F}_{p^m}$ were characterized in [5], where ℓ is a prime different from p.

Dinh [9] determined the generator polynomials of all constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$, where p is an odd prime; self-dual cyclic and negacyclic codes of this length were also discussed. Recently, assuming that p is a prime different from 3, Dinh [10] obtained the duals of all constacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}$ and all self-dual cyclic codes of length $3 \cdot 2^\ell$ over $\mathbb{F}_{2^m}$.

In this paper, we extend the main results of [9] and [10] to a more general setting. According to the equivalence classes induced by " $\sim_{\ell p^s}$ ", all constacyclic codes of length ℓp^s over $\mathbb{F}_{p^m}$ and their duals are characterized in Sections 4 and 5 respectively, where ℓ is a prime different from p. Let $\mathbb{F}_{p^m}^* = \langle \xi \rangle$ denote the multiplicative group of nonzero elements of $\mathbb{F}_{p^m}$. It will be shown that there are exactly $\gcd(\ell, p^m - 1)$ ℓp^s-equivalence classes on $\mathbb{F}_{p^m}^*$, which are one-to-one correspondence to the cosets of $\langle \xi^\ell \rangle$ in $\mathbb{F}_{p^m}^*$. If $\gcd(\ell, p^m - 1) = 1$, all constacyclic codes have the same structures. Otherwise, for any $\lambda \in \mathbb{F}_{p^m}^*$, there exists a unique integer j with $0 \le j \le \ell - 1$ such that λ-constacyclic codes and ξ^{jp^s}-constacyclic codes have the same structures. As an application, in Section 5, all self-dual cyclic codes of length $2^s \ell$ over $\mathbb{F}_{2^\ell}$ are exhibited, and all linear complimentary dual constacylic codes of length ℓp^s are obtained.

2 Preliminaries

Throughout this paper, $\mathbb{F}_q$ denotes the finite field with $q = p^m$ elements, where p is the characteristic of the field and m is a positive integer. Let us denote by $\mathbb{F}_q^*$ the multiplicative group of nonzero elements of $\mathbb{F}_q$. For $\beta \in \mathbb{F}_q^*$, we denote by $\mathrm{ord}_q(\beta)$ the order of β in the group $\mathbb{F}_q^*$; then $\mathrm{ord}_q(\beta)$ is a divisor of $q - 1$, and β is called a *primitive* $\mathrm{ord}_q(\beta)$*-th root of unity*. It is well known that $\mathbb{F}_q^*$ is a cyclic group of order $q - 1$, i.e. $\mathbb{F}_q^*$ is generated by a primitive $(q - 1)$-th root ξ of unity, in symbols $\mathbb{F}_q^* = \langle \xi \rangle$.

Any λ-constacyclic code C of length n over $\mathbb{F}_q$ is identified with exactly one ideal of the quotient ring $\mathbb{F}_q[X]/\langle X^n - \lambda \rangle$, which is generated uniquely by

a monic divisor $g(X)$ of $X^n - \lambda$. In this case, $g(X)$ is called the *generator polynomial* of C. This implies that the irreducible factorization of $X^n - \lambda$ in $\mathbb{F}_q[X]$ determines all constacyclic codes of length n over $\mathbb{F}_q$.

Note that the 1-constacyclic codes (resp. -1-constacyclic codes) are just the usual *cyclic codes* (resp. *negacyclic codes*), and there has been a huge amount of literature on these topics. In particular, the irreducible decomposition of $X^n - 1$ (resp. $X^n + 1$) in $\mathbb{F}_q[X]$ determines all cyclic codes (resp. negacyclic codes) of length n over $\mathbb{F}_q$.

In this paper, ℓ denotes a prime integer different from p. For any integer r, the *q-cyclotomic coset of r modulo ℓ* is defined by

$$C_r = \Big\{ r \cdot q^j \pmod{\ell} \Big| \, j = 0, 1, \ldots \Big\}.$$

Let η be a primitive ℓ-th root of unity (maybe in some extension field of $\mathbb{F}_q$). We denote by $\mathrm{ord}_\ell(q) = f$, the multiplicative order of q in $\mathbf{Z}_\ell^*$. Let $e = \frac{\ell-1}{f}$ and g be a fixed generator of the cyclic group $\mathbf{Z}_\ell^*$. It follows from [24, Theorem 1] that for any integer k with $1 \le k \le e$, $C_0 = \{0\}$ and

$$C_k = \Big\{ g^k, g^k q, \cdots, g^k q^{f_k - 1} \Big\} \tag{2.1}$$

consist all the distinct q-cyclotomic cosets modulo ℓ, where f_k is the smallest positive integer such that $g^k \equiv g^k q^{f_k} \pmod{\ell}$. Here the elements in the brace are calculated modulo ℓ. The following gives the irreducible decomposition of $X^\ell - 1$ in $\mathbb{F}_q[X]$ (see [14, Theorem 4.1.1]):

$$X^\ell - 1 = M_0(X) M_1(X) M_2(X) \cdots M_e(X) \tag{2.2}$$

with

$$M_i(X) = \prod_{j \in C_i} (X - \eta^j), \qquad i = 0, 1, \cdots, e.$$

The next lemma contains a criterion on irreducible non-linear binomials over $\mathbb{F}_q$, which was given by Serret in 1866 (see [17, Theorem 3.75]).

Lemma 2.1. *Assume that $n \ge 2$. For any $a \in \mathbb{F}_q^*$ with $\mathrm{ord}(a) = k$, the binomial $X^n - a$ is irreducible over $\mathbb{F}_q$ if and only if both the following two conditions are satisfied:*

(i) *Every prime divisor of n divides k, but does not divide $(q-1)/k$;*

(ii) *If $4 \mid n$, then $4 \mid (q-1)$.*

3 Equivalence between constacyclic codes

Let $\mathbb{F}_q$ be the finite field of order $q = p^m$ and $\mathbb{F}_q^* = \langle \xi \rangle$ as before. Let ℓ denote a prime integer different from p. In [9], the elements of $\mathbb{F}_q^*$ are divided into two disjoint subsets

$$\mathbb{F}_q^* = A_{\mathrm{even}} \bigcup A_{\mathrm{odd}}, \tag{3.1}$$

where

$$A_{\text{even}} = \left\{ \xi^i \;\middle|\; 1 \leq i \leq (p^m - 1),\ i \text{ is even} \right\}$$

and

$$A_{\text{odd}} = \left\{ \xi^i \;\middle|\; 1 \leq i \leq (p^m - 1),\ i \text{ is odd} \right\}.$$

It was shown that if $\lambda \in A_{\text{even}}$, then λ-constacyclic codes of length $2p^s$ are equivalent to cyclic codes via an $\mathbb{F}_q$-algebra isomorphism; otherwise, λ-constacyclic codes of length $2p^s$ are equivalent to ξ-constacyclic codes via an $\mathbb{F}_q$-algebra isomorphism. Similar techniques were employed in [10] to classify constacyclic codes of length $3p^s$ over $\mathbb{F}_q$.

Observe that $A_{\text{even}} = \langle \xi^2 \rangle$ and $A_{\text{odd}} = \xi\langle \xi^2 \rangle$. That is, Equation (3.1) is exactly the cosets of $\langle \xi^2 \rangle$ partition $\langle \xi \rangle$. Generalizing these ideas, we introduce the following definition:

Definition 3.1. *Let n be a positive integer. For any elements λ, μ of $\mathbb{F}_q^*$, we say that λ and μ are* n-equivalent *in $\mathbb{F}_q^*$ and denote by $\lambda \sim_n \mu$ if the polynomial $\lambda X^n - \mu$ has a root in $\mathbb{F}_q$.*

It is routine to check that $\sim_n$ is an equivalence relation on $\mathbb{F}_q^*$. The next result shows that λ and μ are n-equivalent if and only if they belong to the same coset of $\langle \xi^n \rangle$ in $\langle \xi \rangle$. In other words, the distinct cosets of $\langle \xi^n \rangle$ in $\langle \xi \rangle$ give all the n-equivalence classes, thus each n-equivalence class contains the same number of elements.

Theorem 3.2. *For any $\lambda, \mu \in \mathbb{F}_q^*$, the following four statements are equivalent:*

(i) *There exists an $a \in \mathbb{F}_q^*$ such that*

$$\varphi :\ \mathbb{F}_q[X]/\langle X^n - \mu \rangle \ \to\ \mathbb{F}_q[X]/\langle X^n - \lambda \rangle$$

$$f(X) \mapsto f(aX),$$

is an $\mathbb{F}_q$-algebra isomorphism.

(ii) *λ and μ are n-equivalent in $\mathbb{F}_q^*$.*

(iii) *$\lambda^{-1}\mu \in \langle \xi^n \rangle$.*

(iv) *$(\lambda^{-1}\mu)^d = 1$, where $d = \frac{q-1}{\gcd(n, q-1)}$.*

In particular, the number of the n-equivalence classes in $\mathbb{F}_q^*$ is $\gcd(n, q-1)$.

Proof. (i) $\Rightarrow$ (ii). Assume that there exists an $a \in \mathbb{F}_q^*$ such that

$$\varphi :\ \mathbb{F}_q[X]/\langle X^n - \mu \rangle \ \to\ \mathbb{F}_q[X]/\langle X^n - \lambda \rangle,$$

$$f(X) \mapsto f(aX),$$

is an $\mathbb{F}_q$-algebra isomorphism. It follows that

$$\mu = \varphi(\mu) = \varphi(X^n) = \varphi(X)^n = (aX)^n = a^n X^n = a^n \lambda.$$

This gives that λ and μ are n-equivalent in $\mathbb{F}_q^*$.

(ii) $\Rightarrow$ (iii). By (ii), there is an element $a \in \mathbb{F}_q^*$ such that $\lambda a^n = \mu$. Let $a = \xi^i$ for some $0 \leq i \leq q-1$. Then $\lambda^{-1}\mu = a^n = \xi^{in} \in \langle \xi^n \rangle$.

(iii) $\Rightarrow$ (iv). Since $\mathrm{ord}(\xi^n) = \frac{q-1}{\gcd(n,q-1)} = d$, the cyclic subgroup $\langle \xi^n \rangle$ is of order d. So (iii) holds.

(iv) $\Rightarrow$ (i). Since $\mathbb{F}_q^* = \langle \xi \rangle$ is a cyclic group, $\langle \xi^n \rangle$ is the unique subgroup of order $d = \frac{q-1}{\gcd(n,q-1)}$ and any subgroup with order dividing d is contained in the subgroup $\langle \xi^n \rangle$. Thus, (iv) implies that $(\lambda\mu)^{-1} \in \langle \xi^n \rangle$; i.e. $\lambda^{-1}\mu = \xi^{nk}$ for an integer k. Set $a = \xi^k$, then $\lambda a^n = \mu$, and one can easily check that the following map is an isomorphism:

$$\varphi: \quad \mathbb{F}_q[X]/\langle X^n - \mu \rangle \longrightarrow \mathbb{F}_q[X]/\langle X^n - \lambda \rangle \tag{3.2}$$

which maps any $f(X) + \langle X^n - \mu \rangle \in \mathbb{F}_q[X]/\langle X^n - \mu \rangle$ to the following element of $\mathbb{F}_q[X]/\langle X^n - \lambda \rangle$:

$$\varphi\big(f(X) + \langle X^n - \mu \rangle\big) = f(aX) + \langle X^n - \lambda \rangle.$$

Finally, by the equivalence of (ii) and (iii), the number of the n-equivalence classes in $\mathbb{F}_q^*$ is equal to the number of cosets of the subgroup $\langle \xi^n \rangle$ in $\mathbb{F}_q^*$. The number of cosets of $\langle \xi^n \rangle$ in $\mathbb{F}_q^*$ is:

$$|\mathbb{F}_q^* : \langle \xi^n \rangle| = \frac{q-1}{|\langle \xi^n \rangle|} = \frac{q-1}{\frac{q-1}{\gcd(n,q-1)}} = \gcd(n, q-1).$$

This completes the proof. □

Remark 3.3. We say λ-constacyclic codes are n-equivalent to μ-constacyclic codes if $\lambda \sim_n \mu$. Comparing with the equivalence relation " $\cong_n$ " mentioned in Section 1, one can easily find that $\lambda \sim_n \mu$ implies $\lambda \cong_n \mu$. But the converse of this statement is not true in general. In fact, [5, Theorem 3.2] implies that if $\lambda \cong_n \mu$ then there exists a positive integer k with $\gcd(k, n) = 1$ such that $\lambda \sim_n \mu^k$. Hence, every isometry class is equal to some union of n-equivalence classes. We give the following illustrative example:

Example 3.4. Take $q = 2^4$ and $n = 6$ in Theorem 3.2. Clearly, $\gcd(6, 2^4 - 1) = 3$ and

$$\mathbb{F}_{2^4}^* = \langle \xi \rangle \bigcup \xi\langle \xi \rangle \bigcup \xi^2\langle \xi \rangle.$$

This implies that ξ and ξ^2 are not 6-equivalent. However, it has been shown that there are just two 6-isometry classes on $\mathbb{F}_{2^4}^*$ and $\xi \cong_n \xi^2$ (see [5, Table 3]).

Corollary 3.5. *If n is a positive integer coprime to $q-1$, then any two nonzero elements λ and μ of $\mathbb{F}_q^*$ are n-equivalent to each other, i.e. $\lambda a^n = \mu$ for an $a \in \mathbb{F}_q^*$, and the map $\varphi : \mathbb{F}_q[X]/\langle X^n - \mu \rangle \to \mathbb{F}_q[X]/\langle X^n - \lambda \rangle$ which maps $f(X)$ to $f(aX)$ is an $\mathbb{F}_q$-algebra isomorphism.*

Proof. Since $\gcd(n, q-1) = 1$, there is only one n-equivalence class in $\mathbb{F}_q^*$; in other words, $\lambda \sim_n \mu$. □

Note that Corollary 3.5 has been proved in [5, Corollary 3.5] according to the equivalence relation " $\cong_n$ ".

4 Constacyclic codes of length ℓp^s over $\mathbb{F}_q$

Suppose that $f(X)$ is a polynomial with leading coefficient $a_n \neq 0$. We denote by $\hat{f}(X)$, the monic polynomial such that $\hat{f}(X) = a_n^{-1} f(X)$. Denote by $f = \mathrm{ord}_\ell(q)$, the order of q in $\mathbf{Z}_\ell^*$. Let $e = \frac{\ell-1}{f}$. Then we pick a primitive ℓ-th root η of unity in the finite field $\mathbb{F}_{q^f}$ of order q^f; by Equation (2.2), we have the factorization of $X^{\ell p^s} - 1$ into irreducible factors over $\mathbb{F}_q$ as follows:

$$X^{\ell p^s} - 1 = (X^\ell - 1)^{p^s} = M_0(X)^{p^s} M_1(X)^{p^s} \cdots M_e(X)^{p^s}, \tag{4.1}$$

where $M_j(X) = \prod_{i \in C_j} (X - \eta^i)$ is the minimal polynomial of η^j over $\mathbb{F}_q$, $j = 0, \cdots, e$.

By Theorem 3.2, the number of ℓp^s-equivalence classes in $\mathbb{F}_q^*$ is equal to $\gcd(\ell p^s, q-1) = \gcd(\ell, q-1)$. Two cases may occur, namely $\gcd(\ell, q-1) = 1$ and $\gcd(\ell, q-1) = \ell$. We first consider the case $\gcd(\ell, q-1) = 1$.

The following result is straightforward by Corollary 3.5:

Theorem 4.1. *Let ℓ be a prime integer with $\gcd(\ell, q-1) = 1$. 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 $a \in \mathbb{F}_q^*$ such that $a^{\ell p^s} \lambda = 1$. Further, the map*

$$\varphi_a : \quad \mathbb{F}_q[X]/\langle X^{\ell p^s} - 1 \rangle \longrightarrow \mathbb{F}_q[X]/\langle X^{\ell p^s} - \lambda \rangle, \tag{4.2}$$

which maps $f(X)$ to $f(aX)$ is an $\mathbb{F}_q$-algebra isomorphism, and

$$X^{\ell p^s} - \lambda = \hat{M}_0(aX)^{p^s} \hat{M}_1(aX)^{p^s} \cdots \hat{M}_e(aX)^{p^s} \tag{4.3}$$

is the monic irreducible factorization of $X^{\ell p^s} - \lambda$ in $\mathbb{F}_q[X]$, where $M_j(X)$, $0 \leq j \leq e$, are defined in Equation (4.1). In particular, any λ-constacyclic code C has generator polynomial as follows:

$$\prod_{i=0}^{e} \hat{M}_i(aX)^{\varepsilon_i}, \qquad 0 \leq \varepsilon_i \leq p^s, \ i = 0, 1, \cdots, e. \tag{4.4}$$

Now we consider the other case, when $\gcd(\ell p^s, q-1) = \ell$, namely $\ell \mid (q-1)$.

Theorem 4.2. *Assume that ℓ is a prime divisor of $q-1$. Let $\zeta \in \mathbb{F}_q$ be a primitive ℓ-th root of unity in $\mathbb{F}_q$, and $\lambda \in \mathbb{F}_q^*$. Let C be a λ-constacyclic code of length ℓp^s over $\mathbb{F}_q$. Then one of the following two cases holds:*

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

$$C = \left\langle \prod_{i=0}^{\ell-1} \left(X - b^{-1}\zeta^i\right)^{\varepsilon_i} \right\rangle, \qquad 0 \le \varepsilon_i \le p^s, \quad \textit{for any} \;\; i = 0, 1, \cdots, \ell-1;$$

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

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

Proof. Consider the multiplicative group $\mathbb{F}_q^* = \langle \xi \rangle$ which is a cyclic group of order $q-1$ generated by ξ. It is easy to check that $\langle \xi^{\ell p^s} \rangle = \langle \xi^\ell \rangle$ and the index $|\mathbb{F}_q^* : \langle \xi^\ell \rangle| = \ell$. Thus the multiplicative group $\mathbb{F}_q^*$ is decomposed into disjoint union of cosets over the subgroup $\langle \xi^\ell \rangle$ as follows:

$$\mathbb{F}_q^* = \langle \xi \rangle = \langle \xi^\ell \rangle \cup \xi^{p^s}\langle \xi^\ell \rangle \cup \cdots \cup \xi^{p^s(\ell-1)}\langle \xi^\ell \rangle. \tag{4.5}$$

Therefore, the element λ of $\mathbb{F}_q^*$ belongs to exactly one of the cosets, i.e. there is a unique integer j with $0 \le j \le \ell - 1$ such that $\lambda \in \xi^{jp^s}\langle \xi^\ell \rangle$; in other words, $(\xi^{jp^s})^{-1}\lambda \in \langle \xi^\ell \rangle$. By Theorem 3.2, we get that λ is ℓp^s-equivalent to ξ^{jp^s}. There are two subcases:

Case (I): $j = 0$, i.e. λ and 1 are ℓp^s-equivalent. By Theorem 3.2(i), we have an element $b \in \mathbb{F}_q^*$ such that $\lambda b^{\ell p^s} = 1$ and an $\mathbb{F}_q$-algebra isomorphism:

$$\varphi : \mathbb{F}_q[X]/\langle X^{\ell p^s} - 1 \rangle \longrightarrow \mathbb{F}_q[X]/\langle X^{\ell p^s} - \lambda \rangle$$

defined by

$$\varphi\big(f(X) + \langle X^{\ell p^s} - 1 \rangle\big) = f(bX) + \langle X^{\ell p^s} - \lambda \rangle, \qquad \text{for any} \;\; f(X) \in \mathbb{F}_q[X].$$

As an ideal of $\mathbb{F}_q[X]/\langle X^{\ell p^s} - \lambda \rangle$, the λ-constacyclic code C of length ℓp^s over $\mathbb{F}_q$ is corresponding to an ideal of $\mathbb{F}_q[X]/\langle X^{\ell p^s} - 1 \rangle$, which is generated by a polynomial

$$(X-1)^{\varepsilon_0}(X-\zeta)^{\varepsilon_1}\cdots(X-\zeta^{\ell-1})^{\varepsilon_{\ell-1}}, \qquad 0 \le \varepsilon_0, \varepsilon_1, \cdots, \varepsilon_{\ell-1} \le p^s.$$

Therefore, the λ-constacyclic code C of length ℓp^s over $\mathbb{F}_q$ is generated by the polynomial

$$\prod_{i=0}^{\ell-1} \left(X - b^{-1}\zeta^i\right)^{\varepsilon_i}, \qquad 0 \le \varepsilon_0, \varepsilon_1, \cdots, \varepsilon_{\ell-1} \le p^s.$$

We are done for the statement (I).

Case (II): $1 \leq j \leq \ell - 1$. Then there is an element $d \in \mathbb{F}_q^*$ such that $\lambda d^{\ell p^s} = \xi^{jp^s}$ and an $\mathbb{F}_q$-algebra isomorphism:

$$\varphi : \mathbb{F}_q[X]/\langle X^{\ell p^s} - \xi^{jp^s} \rangle \longrightarrow \mathbb{F}_q[X]/\langle X^{\ell p^s} - \lambda \rangle$$

defined by

$$\varphi\big(f(X) + \langle X^{\ell p^s} - \xi^{jp^s} \rangle\big) = f(dX) + \langle X^{\ell p^s} - \lambda \rangle, \qquad \text{for any} \quad f(X) \in \mathbb{F}_q[X].$$

Recall that $1 \leq j \leq \ell - 1$ and $\ell \mid (q-1)$. By Lemma 2.1, it is routine to check that

$$X^{\ell p^s} - \xi^{jp^s} = (X^\ell - \xi^j)^{p^s},$$

is an irreducible decomposition of $X^{\ell p^s} - \xi^{jp^s}$ in $\mathbb{F}_q[X]$. Thus, any ξ^{jp^s}-constacyclic code C' can be generated as follows:

$$C' = \left\langle \left(X^\ell - \xi^j\right)^\varepsilon \right\rangle, \quad 0 \leq \varepsilon \leq p^s. \tag{4.6}$$

We deduce that

$$C = \left\langle \left(X^\ell - d^{-\ell}\xi^j\right)^\varepsilon \right\rangle, \qquad 0 \leq \varepsilon \leq p^s.$$

□

Remark 4.3. Note that the generator polynomials of all constacyclic codes of length ℓp^s with $\ell \mid (q-1)$ have been determined in [5, Corollary 3.5]. We remark that Theorem 4.2 and [5, Corollary 3.5] are different, and the generator polynomials given by Theorem 4.2 are more specific, which makes it easier to get their dual codes.

5 Dual codes

In this section, the duals of all constacyclic codes of length ℓp^s over $\mathbb{F}_q$ are obtained, where ℓ is a prime different from p. As an application, all linear complementary-dual (LCD) cyclic and negacylic codes of length ℓp^s are provided, and all self-dual cyclic codes of length $2^s\ell$ over $\mathbb{F}_{2^m}$ are also determined at the same time.

The concept of the reciprocal polynomial is closely related to these issues. Assume that $g(X)$ is the generator polynomial of a λ-constacyclic code C of length ℓp^s over $\mathbb{F}_q$. Let $h(X) = \frac{X^{\ell p^s} - \lambda}{g(X)}$. The dual code $C^\perp$ is a λ^{-1}-constacyclic code and has generator polynomial $h^*(X)$, where $h^*(X) = h(0)^{-1} X^{\deg h} h(\frac{1}{X})$ is the *reciprocal polynomial* of $h(X)$. Note that $h^*(X)$ is a monic polynomial and it divides $X^{\ell p^s} - \lambda^{-1}$. If a polynomial is equal to its reciprocal polynomial, then it is called *self-reciprocal*.

We first deal with the case $\ell \neq 2$. The following lemma characterizes the irreducible factorization of $X^\ell - 1$ over $\mathbb{F}_q$ concretely, when $\mathrm{ord}_\ell(q)$ is odd. In this case, it turns out that the irreducible factors of $X^\ell - 1$ except $X - 1$ are not self-reciprocal.

Lemma 5.1. *Assume that ℓ is an odd prime different from p and g is a fixed generator of the cyclic group $\mathbf{Z}_\ell^*$. Let $\mathrm{ord}_\ell(q) = f$ and $e = \frac{\ell-1}{f}$. If f is odd, then all the distinct q-cyclotomic cosets modulo ℓ are given by $C_0 = \{0\}$,*

$$C_k = \left\{g^k, g^k q, \cdots, g^k q^{f-1}\right\} \text{ and } C_{-k} = \left\{-g^k, -g^k q, \cdots, -g^k q^{f-1}\right\}, \quad 1 \leq k \leq \tfrac{e}{2}.$$

Proof. We first claim that the cyclotomic cosets C_{k_1} and C_{-k_2}, $1 \leq k_1, k_2 \leq \frac{e}{2}$, are distinct from each other. Suppose otherwise that $C_{k_1} = C_{-k_2}$ for some $1 \leq k_1, k_2 \leq \frac{e}{2}$. Then there exists some integer j such that

$$g^{k_1} \equiv -g^{k_2} q^j \pmod{\ell}. \tag{5.1}$$

Therefore, $g^{2fk_1} \equiv g^{2fk_2} q^{2fj} \pmod{\ell}$, which gives $g^{2fk_1} \equiv g^{2fk_2} \pmod{\ell}$. We get $2f(k_1 - k_2) \equiv 0 \pmod{\ell - 1}$ since g is of order $\ell - 1$ in $\mathbf{Z}_\ell^*$, which implies $k_1 = k_2$. Then (5.1) gives

$$-1 \equiv q^j \pmod{\ell}.$$

Using $\mathrm{ord}_\ell(q) = f$ again, we have f divides $2j$. Since f is odd, hence f divides j. This leads to

$$1 \equiv q^j \pmod{\ell},$$

a contradiction. This proves the claim. Taking similar arguments, we obtain that $C_{k_1} = C_{k_1'}$ if and only if $k_1 = k_1'$, and that $C_{-k_2} = C_{-k_2'}$ if and only if $k_2 = k_2'$, $1 \leq k_1, k_1', k_2, k_2' \leq \frac{e}{2}$. Finally, C_0, C_k and C_{-k}, $1 \leq k \leq \frac{e}{2}$, are all the q-cyclotomic cosets modulo ℓ. To this end,

$$|C_0| + \sum_{i=1}^{\frac{e}{2}} (|C_i| + |C_{-i}|) = 1 + \sum_{i=1}^{\frac{e}{2}} 2f = 1 + ef = \ell.$$

□

Assuming that $\mathrm{ord}_\ell(q)$ is odd, by Lemma 5.1,

$$X^\ell - 1 = M_0(X) M_1(X) M_{-1}(X) \cdots M_{\frac{e}{2}}(X) M_{-\frac{e}{2}}(X) \tag{5.2}$$

gives the irreducible factorization of $X^\ell - 1$ over $\mathbb{F}_q$. Clearly, in this case, $M_0^*(X) = (X-1)^* = X - 1$ and $M_k^*(X) = M_{-k}(X)$ for each $1 \leq k \leq \frac{e}{2}$.

On the other hand, if $\mathrm{ord}_\ell(q)$ is even, then the monic irreducible factors of $X^\ell - 1$ are self-reciprocal. Indeed, this is simply because $q^{\frac{\mathrm{ord}_\ell(q)}{2}} \equiv -1 \pmod{\ell}$.

Now assuming that ℓ is an odd prime, we give the duals of all constacyclic codes of length ℓp^s over $\mathbb{F}_q$.

Theorem 5.2. *Let ℓ be an odd prime with $\gcd(\ell, q-1) = 1$. Given $\lambda \in \mathbb{F}_q^*$, there exists a unique $a \in \mathbb{F}_q^*$ such that $a^{\ell p^s}\lambda = 1$. One of the following two cases holds:*

(I) *$\mathrm{ord}_\ell(q) = f$ is odd. Any λ-constacyclic code C of length ℓp^s over $\mathbb{F}_q$ has generator polynomial*

$$(X - a^{-1})^{\varepsilon} \prod_{i=1}^{\frac{e}{2}} \hat{M}_i(aX)^{\varepsilon_i} \hat{M}_{-i}(aX)^{\delta_i}, \qquad 0 \le \varepsilon, \varepsilon_i, \delta_i \le p^s, \quad 1 \le i \le \tfrac{e}{2}.$$

Its dual code $C^\perp$ is the λ^{-1}-constacyclic code, which has generator polynomial

$$(X - a)^{p^s - \varepsilon} \prod_{i=1}^{\frac{e}{2}} \hat{M}_i(a^{-1}X)^{p^s - \delta_i} \hat{M}_{-i}(a^{-1}X)^{p^s - \varepsilon_i}.$$

(II) *$\mathrm{ord}_\ell(q) = f$ is even. Any λ-constacyclic code C of length ℓp^s over $\mathbb{F}_q$ has generator polynomial*

$$\prod_{i=0}^{e} \hat{M}_i(aX)^{\varepsilon_i}, \qquad 0 \le \varepsilon_i \le p^s.$$

Its dual code $C^\perp$ is the λ^{-1}-constacyclic code, which has generator polynomial

$$\prod_{i=0}^{e} \hat{M}_i(a^{-1}X)^{p^s - \varepsilon_i}.$$

Proof. The first statement of (I) follows directly from Theorem 4.1 and Lemma 5.1. Now suppose we have $C = \langle g(X) \rangle$,

$$g(X) = (X - a^{-1})^{\varepsilon} \prod_{i=1}^{\frac{e}{2}} \hat{M}_i(aX)^{\varepsilon_i} \hat{M}_{-i}(aX)^{\delta_i}.$$

To give the generator polynomial of $C^\perp$, we need to compute $h^*(X)$, where $h(X)$ is equal to $\frac{X^{\ell p^s} - \lambda}{g(X)}$. Since $X^{\ell p^s} - \lambda = (X - a^{-1})^{p^s} \prod_{i=1}^{\frac{e}{2}} \hat{M}_i(aX)^{p^s} \hat{M}_{-i}(aX)^{p^s}$, it follows that

$$h(X) = \frac{X^{\ell p^s} - \lambda}{g(X)} = (X - a^{-1})^{p^s - \varepsilon} \prod_{i=1}^{\frac{e}{2}} \hat{M}_i(aX)^{p^s - \varepsilon_i} \hat{M}_{-i}(aX)^{p^s - \delta_i}.$$

Thus,

$$\begin{aligned} h^*(X) &= \big((X - a^{-1})^*\big)^{p^s - \varepsilon} \prod_{i=1}^{\frac{e}{2}} \Big(\big(\hat{M}_i^*(aX)\big)^{p^s - \varepsilon_i} \big(\hat{M}_{-i}^*(aX)\big)^{p^s - \delta_i} \Big) \\ &= (X - a)^{p^s - \varepsilon} \prod_{i=1}^{\frac{e}{2}} \hat{M}_{-i}(a^{-1}X)^{p^s - \varepsilon_i} \hat{M}_i(a^{-1}X)^{p^s - \delta_i}. \end{aligned}$$

This gives the desired result. Taking arguments similar to the proof of (I), we can obtain statement (II).

□

The next result determines the dual codes of all constacyclic codes of length ℓp^s over $\mathbb{F}_q$, when the prime ℓ is an odd divisor of $q-1$. We shall omit its proof, since taking similar arguments in Thoerem 5.2 is enough.

Theorem 5.3. *Assume that ℓ is an odd prime divisor of $q-1$. Let $\lambda \in \mathbb{F}_q^*$. Then one of the following two cases holds:*

(I) *$\lambda \in \langle \xi^\ell \rangle$. Any λ-constacyclic code C of length ℓp^s over $\mathbb{F}_q$ has generator polynomial*

$$(X-b^{-1})^\varepsilon \prod_{i=1}^{\frac{\ell-1}{2}} \left(X-b^{-1}\zeta^i\right)^{\varepsilon_i} (X-b^{-1}\zeta^{-i})^{\delta_i}, \quad 0 \le \varepsilon, \varepsilon_i, \delta_i \le p^s, \quad i = 1, \cdots, \frac{\ell-1}{2},$$

where $b \in \mathbb{F}_q^*$ satisfies $b^{\ell p^s}\lambda = 1$. Its dual code $C^\perp$ is the λ^{-1}-constacyclic code, which has generator polynomial

$$(X-b)^{p^s-\varepsilon} \prod_{i=1}^{\frac{\ell-1}{2}} (X-b\zeta^i)^{p^s-\delta_i} (X-b\zeta^{-i})^{p^s-\varepsilon_i}.$$

(II) *$\lambda \notin \langle \xi^\ell \rangle$. A unique integer j with $1 \le j \le \ell-1$ and an element $d \in \mathbb{F}_q^*$ can be found such that $d^{\ell p^s}\lambda = \xi^{jp^s}$. Any λ-constacyclic code C of length ℓp^s over $\mathbb{F}_q$ has generator polynomial*

$$\left(X^\ell - d^{-\ell}\xi^j\right)^\varepsilon, \qquad 0 \le \varepsilon \le p^s.$$

Its dual code $C^\perp$ is the λ^{-1}-constacyclic code, which has generator polynomial

$$\left(X^\ell - d^\ell \xi^{-j}\right)^{p^s-\varepsilon}.$$

We are left with the case $\ell = 2$. At this point $q = p^m$ must be an odd, thus $2 \mid (q-1)$. Using Theorem 4.2, the following corollary gives the duals of all constacyclic codes of length $2p^s$ over $\mathbb{F}_q$.

Corollary 5.4. *Let $q = p^m$, where p is an odd prime. Let $\lambda \in \mathbb{F}_q^*$. Then one of the following two statements holds:*

(i) $\lambda \in \langle \xi^2 \rangle$. There exists $b \in \mathbb{F}_q^*$ such that $b^{2p^s}\lambda = 1$. Any λ-constacyclic code C of length $2p^s$ over $\mathbb{F}_q$ has generator polynomial

$$\left(X-b^{-1}\right)^\varepsilon \left(X+b^{-1}\right)^\delta, \quad 0 \le \varepsilon, \delta \le p^s.$$

Its dual code $C^\perp$ is the λ^{-1}-constacyclic code, which has generator polynomial

$$\left(X-b\right)^{p^s-\varepsilon} \left(X+b\right)^{p^s-\delta}.$$

(ii) $\lambda \in \xi^{p^s}\langle \xi^2 \rangle$. *There exists* $d \in \mathbb{F}_q^*$ *such that* $d^{2p^s}\lambda = \xi^{p^s}$. *Any* λ*-constacyclic code* C *of length* $2p^s$ *over* $\mathbb{F}_q$ *has generator polynomial*

$$\Big(X^2 - d^{-2}\xi\Big)^{\varepsilon}, \qquad 0 \leq \varepsilon \leq p^s.$$

Its dual code $C^{\perp}$ *is the* λ^{-1}*-constacyclic code, which has generator polynomial*

$$\Big(X^2 - d^2\xi^{-1}\Big)^{p^s-\varepsilon}.$$

Proof. As in Theorem 4.2, take $\ell = 2$, then $\ell \mid (q-1)$, and -1 is a primitive second root of unity in $\mathbb{F}_q$. In this special case,

$$\mathbb{F}_q^* = \Big\langle \xi \Big\rangle = \Big\langle \xi^2 \Big\rangle \bigcup \xi^{p^s} \Big\langle \xi^2 \Big\rangle.$$

There only two cases may occur: $\lambda \in \langle \xi^2 \rangle$ or $\lambda \in \xi^{p^s}\langle \xi^2 \rangle$.

(i) If $\lambda \in \langle \xi^2 \rangle$, it follows from Theorem 4.2 (I) that any λ-constacyclic code C of length $2p^s$ over $\mathbb{F}_q$ has generator polynomial $g(X) = (X-b^{-1})^{\varepsilon}(X+b^{-1})^{\delta}$, where $0 \leq \varepsilon, \delta \leq p^s$. Note that $X^{2p^s} - \lambda = (X-b^{-1})^{p^s}(X+b^{-1})^{p^s}$. Thus, $h(X) = \frac{X^{2p^s}-1}{g(X)} = (X-b^{-1})^{p^s-\varepsilon}(X+b^{-1})^{p^s-\delta}$, implying that $C^{\perp}$ has generator polynomial

$$h^*(X) = \Big(X-b\Big)^{p^s-\varepsilon}\Big(X+b\Big)^{p^s-\delta}.$$

(ii) Using similar arguments and Theorem 4.2 (II), we obtain the desired result.

□

We devote the rest of this section to apply our results on duals codes to investigate the situations of self-dual codes and linear complimentary-dual (LCD) codes. These are the two extreme connections between C and $C^{\perp}$, where $C = C^{\perp}$ (for self-dual codes) and $C \bigcap C^{\perp} = \{0\}$ (for LCD codes). The concept of LCD codes was introduced by Massey [19] in 1992. In the same paper, he showed that asymptotically good LCD codes exist, and provided applications of LCD codes such as they provide an optimum linear coding solution for the two-user binary adder channel. It was proven by Sendrier [23] that LCD codes meet the Gilbert-Varshamov bound. Necessary and sufficient conditions for cyclic codes [28] and certain classes of quasi-cyclic codes [12] to be LCD codes were obtained.

It is known that self-dual λ-constacyclic codes can only occur among the classes of cyclic and negacyclic codes, i.e., $\lambda = 1$ or -1 (e.g. [11]). It was also shown that self-dual cyclic codes of length n over $\mathbb{F}_q$ exist if and only if n is even and the characteristic of the underlying field is two ([16, 15]). The following corollary gives all self-dual cyclic codes of length $2^s\ell$ over $\mathbb{F}_{2^m}$.

Corollary 5.5. *Let* ℓ *be an odd prime. Self-dual cyclic codes of length* $2^s\ell$ *over* $\mathbb{F}_{2^m}$ *exist.*

(I) *If* $\gcd(\ell, q-1) = 1$ *and* f *is odd, then there are exactly* $(2^s+1)^{\frac{e}{2}}$ *self-dual cyclic codes of length* $2^s\ell$ *over* $\mathbb{F}_{2^m}$ *given by*

$$\Big\langle (X-1)^{2^{s-1}} \prod_{i=1}^{\frac{e}{2}} M_i(X)^{\varepsilon_i} M_{-i}(X)^{2^s-\varepsilon_i} \Big\rangle, \quad 0 \le \varepsilon_i \le 2^s.$$

(II) *If* $\gcd(\ell, q-1) = 1$ *and* f *is even, then there is only one self-dual cyclic code of length* $2^s\ell$ *over* $\mathbb{F}_{2^m}$ *given by*

$$\Big\langle \prod_{i=0}^{e} M_i(X)^{2^{s-1}} \Big\rangle.$$

(III) *If* $\ell \mid (q-1)$*, then there are exactly* $(2^s+1)^{\frac{\ell-1}{2}}$ *self-dual cyclic codes of length* $2^s\ell$ *over* $\mathbb{F}_{2^m}$ *given by*

$$\Big\langle (X-1)^{2^{s-1}} \prod_{i=1}^{\frac{\ell-1}{2}} \big(X-\zeta^i\big)^{\varepsilon_i} \big(X-\zeta^{-i}\big)^{2^s-\varepsilon_i} \Big\rangle, \quad 0 \le \varepsilon_i \le 2^s, \quad i = 1, \cdots, \tfrac{\ell-1}{2},$$

where $\zeta \in \mathbb{F}_q$ *is a primitive* ℓ*-th root of unity.*

Proof. We just give a proof for (I), since the proofs for (II) and (III) are similar. Let C be a cyclic code of length $2^s\ell$ over $\mathbb{F}_{2^m}$ with generator polynomial $g(X)$. According to (5.2), we can assume that

$$g(X) = (X-1)^{\varepsilon} \prod_{i=1}^{\frac{e}{2}} M_i(X)^{\varepsilon_i} M_{-i}(X)^{\delta_i}, \quad 0 \le \varepsilon, \varepsilon_i, \delta_i \le 2^s \ .$$

Therefore, its check polynomial $h(X)$ is given by

$$h(X) = (X-1)^{2^s-\varepsilon} \prod_{i=1}^{\frac{e}{2}} M_i(X)^{2^s-\varepsilon_i} M_{-i}(X)^{2^s-\delta_i}.$$

It follows that

$$h^*(X) = (X-1)^{2^s-\varepsilon} \prod_{i=1}^{\frac{e}{2}} M_{-i}(X)^{2^s-\varepsilon_i} M_i(X)^{2^s-\delta_i}.$$

From the fact that $C = C^{\perp}$ if and only if $g(X) = h(X)^*$, we deduce that

$$\varepsilon = 2^{s-1}, \varepsilon_i + \delta_i = 2^s, \quad \text{for each } 1 \le i \le \tfrac{e}{2}.$$

□

Remark 5.6. It is true that a necessary condition for the existence of self-dual codes over finite fields is that the code length must be even. Regarding self-dual negacyclic codes of length ℓp^s over $\mathbb{F}_{p^m}$, we have to assume that p is even or ℓ is even.

When $p = 2$, cyclic codes over $\mathbb{F}_{2^m}$ are the same with negacyclic codes over $\mathbb{F}_{2^m}$. Corollary 5.5 actually gives all self-dual negayclic codes of length $2^s\ell$ over $\mathbb{F}_{2^m}$. When $\ell = 2$, we note that all self-dual negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ have been determined in [9].

For the case of LCD codes, it was shown that any λ-constacyclic code with $\lambda \notin \{-1, 1\}$ is a LCD code ([11]). So in order to obtain all λ-constacyclic codes, we only need to work on cyclic and negacyclic codes.

Corollary 5.7. *Let ℓ be an odd prime not equal to the field characteristic p.*

(i) If f is odd, then there are $2^{\frac{e}{2}+1}$ LCD cyclic codes given by

$$\Big\langle (X-1)^{i_0} \prod_{j=1}^{\frac{e}{2}} M_j(X)^{i_j} M_{-j}(X)^{i_j} \Big\rangle, \quad i_j \in \{0, p^s\}, \quad 0 \le j \le \frac{e}{2}.$$

(ii) If f is even, then there are 2^{e+1} LCD cyclic codes given by

$$\Big\langle \prod_{j=0}^{e} M_j(X)^{i_j} \Big\rangle, \quad i_j \in \{0, p^s\}, \quad 0 \le j \le e.$$

Proof. We just give a proof for (i), since the proof for (ii) is similar. We get the result by computing the intersection of C and $C^\perp$. From Theorem 5.2, we can assume that C is a cyclic code of length ℓp^s with generator polynomial

$$(X-1)^{\varepsilon} \prod_{i=1}^{\frac{e}{2}} M_i(X)^{\varepsilon_i} M_{-i}(X)^{\delta_i}, \qquad 0 \le \varepsilon, \varepsilon_i, \delta_i \le p^s, \quad 1 \le i \le \tfrac{e}{2}.$$

Then its dual code $C^\perp$ has generator polynomial

$$(X-1)^{p^s-\varepsilon} \prod_{i=1}^{\frac{e}{2}} M_i(X)^{p^s-\delta_i} M_{-i}(X)^{p^s-\varepsilon_i}.$$

Therefore $C \bigcap C^\perp$ has generator polynomial as follows

$$(X-1)^{\max\{\varepsilon, p^s-\varepsilon\}} \prod_{i=1}^{\frac{e}{2}} M_i(X)^{\max\{\varepsilon_i, p^s-\delta_i\}} M_{-i}(X)^{\max\{\delta_i, p^s-\varepsilon_i\}}.$$

Thus, $C \bigcap C^\perp = \{0\}$ if and only if

$$p^s = \max\{\varepsilon, p^s-\varepsilon\} = \max\{\varepsilon_i, p^s-\delta_i\} = \max\{\delta_i, p^s-\varepsilon_i\}, \text{ for each } 1 \le i \le \tfrac{e}{2},$$

which is equivalent to

$$\varepsilon \in \{0, p^s\}, \quad \varepsilon_i = \delta_i \in \{0, p^s\}, \text{ for each } 1 \leq i \leq \tfrac{e}{2}.$$

We complete the proof of statement (i). □

Also we can give the LCD cyclic codes of length $2p^s$ over $\mathbb{F}_q$, which is easier to obtain than the previous case.

Corollary 5.8. *There are* 4 *LCD cyclic codes of length* $2p^s$ *over* $\mathbb{F}_q$*, given by*

$$\left\langle (X-1)^{i_0}(X+1)^{i_1} \right\rangle, \quad i_0, i_1 \in \{0, p^s\}.$$

Finally, we are left to give all LCD negacyclic codes of length ℓp^s over $\mathbb{F}_q$.

Corollary 5.9. *Let* ℓ *be a prime not equal to* p *and* $\mathrm{ord}_\ell(q) = f$*.*

(i) If ℓ *is odd and* f *is odd, then there are* $2^{\frac{e}{2}+1}$ *LCD negacyclic codes given by*

$$\left\langle (X+1)^{i_0} \prod_{j=1}^{\frac{e}{2}} \hat{M}_j(-X)^{i_j} \hat{M}_{-j}(-X)^{i_j} \right\rangle, \quad i_j \in \{0, p^s\}, \quad 0 \leq j \leq \frac{e}{2}.$$

(ii) If ℓ *is odd and* f *is even, then there are* 2^{e+1} *LCD negacyclic codes given by*

$$\left\langle \prod_{j=0}^{e} \hat{M}_j(-X)^{i_j} \right\rangle, \quad i_j \in \{0, p^s\}, \quad 0 \leq j \leq e.$$

(iii) If $q \equiv 1 \pmod 4$*, then there are* 4 *LCD negacyclic codes of length* $2p^s$ *over* $\mathbb{F}_q$ *given by*

$$\left\langle (X-\alpha)^{i_0}(X+\alpha)^{i_1} \right\rangle, \quad i_0, i_1 \in \{0, p^s\},$$

where α *is a primitive* 4*-th root of unity in* $\mathbb{F}_q$*.*

(iv) If $q \equiv 3 \pmod 4$*, then there are only two LCD negacyclic codes of length* $2p^s$ *over* $\mathbb{F}_q$*, namely only the trivial negacyclic codes satisfy the condition* $C \bigcap C^\perp = \{0\}$*.*

Proof. We just remark that, (i) and (ii) hold true simply because ℓ is odd. That is to say, if f is odd

$$X^\ell + 1 = \hat{M}_0(-X)\hat{M}_1(-X)\hat{M}_{-1}(-X)\cdots\hat{M}_{\frac{e}{2}}(-X)\hat{M}_{-\frac{e}{2}}(-X)$$

actually gives the monic irreducible factorization of $X^\ell + 1$ over $\mathbb{F}_q$. While f is even,

$$X^\ell + 1 = \prod_{j=0}^{e} \hat{M}_j(-X),$$

is the irreducible factorization of $X^\ell + 1$ over $\mathbb{F}_q$. □

Acknowledgements The authors would like to thank the referees for a very meticulous reading of this manuscript, and for many valuable suggestions which help to create an improved version. The first and the third authors thank NSFC for the supporting Grant No. 11171370. The research of the first author is also partially supported by NSFC (Grant No. 11271005) and Nanyang Technological University's research grant number M4080456.

References

[1] G. K. Bakshi, M. Raka, A class of constacyclic codes over a finite field, Finite Fields Appl., **18**(2012), 362-377.

[2] S. D. Berman, Semisimple cyclic and abelian codes II, English translation: Cybernetics, **3**(1967) 17-23.

[3] T. Blackford, Cyclic codes over $\mathbf{Z}_4$ of oddly even length, Discrete Appl. Math., **128**(2003), 27-46.

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

[5] B. Chen, Y. Fan, L. Lin, H. Liu, Constacyclic codes over finite fields, Finite Fields Appl., **18**(2012), 1217-1231.

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

[7] H. Q. Dinh, On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions, Finite Fields Appl., **14**(2008), 22-40.

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

[9] H. Q. Dinh, Repeated-root constacyclic codes of length $2p^s$, Finite Fields Appl., **18**(2012), 133-143.

[10] H. Q. Dinh, Structure of repeated-root constacyclic codes of length $3p^s$ and their duals, Discrete Math., **313**(2013), 983-991.

[11] H. Q. Dinh, Structure of repeated-root cyclic and negacyclic codes of length $6p^s$ and their duals, AMS Contemporary Mathematics (2013), to appear.

[12] M. Esmaeili, S. Yari, On complementary-dual quasi-cyclic codes, Finite Fields Appl., **15**(2009), 375-386.

[13] G. Falkner, B. Kowol, W. Heise, E. Zehendner, On the existence of cyclic optimal codes, Atti Sem. Mat. Fis. Univ. Modena **28**(1979), 326-341.

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

[15] Y. Jia, S. Ling, C. Xing, On self-dual cyclic codes over finite fields, IEEE Trans. Inform. Theory **57**(2011), 2243-2251.

[16] X. Kai, S. Zhu, On cyclic self-dual codes, Appl. Algebra Engrg. Comm. Comput., **19**(2008), 509-525.

[17] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 2008.

[18] J. L. Massey, D. J. Costello, J. Justesen, Polynomial weights and code constructions, IEEE Trans. Inform. Theory **19**(1973), 101-110.

[19] J. L. Massey, Linear codes with complementary duals, Discrete Math., **106/107**(1992), 337-342.

[20] C. -S. Nedeloaia, Weight distributions of cyclic self-dual codes, IEEE Trans. Inform. Theory **49**(2003), 1582-1591.

[21] R. M. Roth, G. Seroussi, On cyclic MDS codes of length q over $GF(q)$, IEEE Trans. Inform. Theory **32**(1986), 284-285.

[22] A. Sălăgean, Repeated-root cyclic and negacyclic codes over a finite chain ring, Discrete Appl. Math., **154**(2006), 413-419.

[23] N. Sendrier, Linear codes with complementary duals meet the Gilbert-Varshamov bound, Discrete Math., **285**(2004), 345-347.

[24] A. Sharma, G. K. Bakshi, V. C. Dumir, M. Raka, Cyclotomic numbers and primitive idempotents in the ring $GF(q)[X]/\langle X^{p^n}-1\rangle$, Finite Fields Appl., **10**(2004), 653-673.

[25] 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**(1997), 732-737.

[26] J. H. van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory **37**(1991), 343-345.

[27] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory **45**(1999), 2527-2532.

[28] X. Yang, J. L. Massey, The condition for a cyclic code to have a complementary dual, Discrete Math., **126**(1994), 391-393.

[29] K. -H. Zimmermann, On generalizations of repeated-root cyclic codes, IEEE Trans. Inform. Theory **42**(1996), 641-649.