Repeated-root constacyclic codes of length $2\ell mpn$

Chen, Bocong; Dinh, Hai Q.; Liu, Hongwei

2014

Chen, B., Dinh, H. Q., & Liu, H. (2015). Repeated-root constacyclic codes of length $2\ell mpn$. Finite fields and their applications, 33, 137-159.

https://hdl.handle.net/10356/106836

https://doi.org/10.1016/j.ffa.2014.11.006

Repeated-root constacyclic codes of length $2\ell^m p^n$*

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]School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637616, Singapore

Abstract

For any different odd primes ℓ and p, structure of constacyclic codes of length $2\ell^m p^n$ over the finite field $\mathbb{F}_q$ of characteritic p and their duals is established in term of their generator polynomials. Among other results, the characterization and enumeration of all linear complimentary dual and self-dual constacylic codes of length $2\ell^m p^n$ are obtained.

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

2010 Mathematics Subject Classification: 11T71; 94B05

1 Introduction

Constacyclic codes over finite fields form a remarkable class of linear codes, as they include the important family of cyclic codes. In fact, the class of cyclic codes is one of the most significant and well studied of all codes. Many well known codes, such as BCH, Kerdock, Golay, Reed-Muller, Preparata, Justesen and binary Hamming codes, are either cyclic codes or can be constructed from 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, where q is a power of a prime p. 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 in the code, which is a divisor of $X^n-\lambda$.

Obviously, there are $q-1$ classes constacyclic codes of length n over $\mathbb{F}_q$. However, it turned out that many of them are equivalent in the sense that they have the same structures. Thus, the natural question, that 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 algebraic structures, has been studied by many authors. Particular cases of this question have been considered since the late 1990s, even for the more general alphabets of finite rings. Wolfmann [33] 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 [10] generalized this result and obtained 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 [13] showed that all constacyclic codes over the finite field $\mathbb{F}_q$ have the same structure; and over the chain ring $\mathbb{F}_q+u\mathbb{F}_q$, 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 $\mathbb{F}_q$.

Recently, we introduced an equivalence relation " $\sim_n$ " called n-equivalence 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 equivalence class have the same distance structures and the same algebraic structures [9].

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

Definition 1.1. *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 $\mathbb{F}_q^*$ (denoted by $\lambda \sim_n \mu$) if the polynomial $\lambda X^n - \mu$ has a root in $\mathbb{F}_q$.*

We obtained that λ and μ are n-equivalent if and only if they belong to the same coset of $\langle \xi^n \rangle$ in $\langle \xi \rangle$. That means 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. Moreover, we showed that, for any $\lambda, \mu \in \mathbb{F}_q^*$, $\lambda \sim_n \mu$ if and only if 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 a ring isomorphism, and hence, the generator polynomial of the μ-constacyclic code C and the generator polynomial of the λ-constacyclic code $\varphi(C)$ are linked in a very simple way.

For any nonzero $\lambda \in \mathbb{F}_q$, $\mathbb{F}_q[X]/\langle X^n - \lambda \rangle$ is a principal ideal ring, i.e., 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 using cyclotomic cosets. 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 [5], and then by several authors such as Massey *et al.* [26], Falkner *et al.* [18], Roth, Seroussi [27] and Salagean [28]. Repeated-root codes were first investigated in the most generality in the 1990s by Castagnoli *et al.* [6], and van Lint [31], 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 [12, 13, 22]. 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 [21, 20]. These motivate researchers to further study this class of codes.

Recently, Dinh, in a series of papers [14, 15, 16], determined the generator polynomials of all constacyclic codes over $\mathbb{F}_q$, of lengths $2p^s$, $3p^s$ and $6p^s$. Dual constacyclic codes of these lengths were also discussed. These results have been extended to more general code lengths. The generator polynomials of all constacyclic codes of length $2^t p^s$ over $\mathbb{F}_q$ were given in [1], where q is a power of an odd prime p. The generator polynomials of all constacyclic codes of length ℓp^s over $\mathbb{F}_q$ were characterized in [7] and [9], where ℓ is a prime different from p. Moreover, [9] identified the duals of all such conctacyclic codes, and provided all self-dual and all linear complimentary dual constacylic codes.

In this paper, we continue to extend the main results of [14, 16] to a more general code length of $2\ell^m p^n$, for any different odd primes ℓ and p. According to the equivalence classes induced by " $\sim_{2\ell^m p^n}$ ", all constacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$ and their duals are characterized in Sections 3 and 4, respectively. As an application, the characterization and enumeration of all linear complimentary dual constacylic codes of length $2\ell^m p^n$ are obtained. Since it is known that self-dual constacyclic codes can only occur among the classes of cyclic and negacyclic codes, and that self-dual cyclic codes over $\mathbb{F}_q$ do not exist because p is odd, it follows that all self-dual constacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$ can only occur among the class of negacyclic codes. We provide all such self-dual negacyclic codes.

2 Preliminaries

Starting from this section till the end of this paper, $\mathbb{F}_q$ denotes the finite field of order q, where q is a power of an odd prime p. Let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. For $\beta \in \mathbb{F}_q^*$, we denote by $\mathrm{ord}(\beta)$ the order of β in the group $\mathbb{F}_q^*$; then $\mathrm{ord}(\beta)$ is a divisor of $q-1$, and β is called a *primitive* $\mathrm{ord}(\beta)$*th root of unity*. It is known that $\mathbb{F}_q^*$ is generated by a primitive $(q-1)$th root ξ of unity, i.e., $\mathbb{F}_q^* = \langle \xi \rangle$. As usual, for integers a, b and a prime l, $a \mid b$ means that a divides b, $l^a \| b$ means that $l^a \mid b$ but $l^{a+1} \nmid b$.

Let m be a positive integer and ℓ an odd prime different from p. Let $\mathbb{Z}_{\ell^m} = \{[b]_{\ell^m} \mid b \text{ is an integer}\}$ be the ring consisting of all residue classes modulo ℓ^m and $\mathbb{Z}_{\ell^m}^*$ be the unit group of the ring. It is well

known that $\mathbb{Z}_{\ell^m}^*$ is a cyclic group. We denote by $\langle q \rangle$, the cyclic subgroup of $\mathbb{Z}_{\ell^m}^*$ generated by $[q]_{\ell^m}$. Let $\langle q \rangle$ act on $\mathbb{Z}_{\ell^m}$ by the following rule:

$$q^i \cdot [b]_{\ell^m} = [bq^i]_{\ell^m}, \quad \text{for any integer } i \text{ and } [b]_{\ell^m} \in \mathbb{Z}_{\ell^m}.$$

For any integer t, the orbit of $[t]_{\ell^m}$,

$$C_t = \left\{ t, tq, tq^2, \cdots tq^{m_t - 1} \right\}$$

is called the *q-cyclotomic coset of t modulo* ℓ^m, where the elements in the brace are calculated modulo ℓ^m and m_t is the cardinality of the orbit of $[t]_{\ell^m}$. It is readily seen that m_t is equal to the multiplicative order of q modulo $\frac{\ell^m}{\gcd(\ell^m, t)}$.

We denote by $\mathrm{ord}_\ell(q) = f$, the multiplicative order of q in $\mathbb{Z}_\ell^*$. Write

$$q^f = 1 + \ell^s t, \quad \ell \nmid t, \ s \geq 1.$$

For any integer r, $1 \leq r \leq m$, let

$$\lambda(r) := f\ell^{\max(r-s,0)}. \tag{2.1}$$

One knows that $\mathrm{ord}_{\ell^r}(q) = \lambda(r)$ (see [2] or [30]). Let $\delta(r) = \frac{\phi(\ell^r)}{\lambda(r)}$, where ϕ denotes Euler's phi-function. Let g be a fixed generator of the cyclic group $\mathbb{Z}_{\ell^m}^*$. By [30, Theorem 1], $C_0 = \{0\}$, and

$$C_{\ell^{m-r}g^k} = \left\{ \ell^{m-r}g^k, \ell^{m-r}g^k q, \cdots, \ell^{m-r}g^k q^{\lambda(r)-1} \right\}, \ 0 \leq k \leq \delta(r) - 1, \ 1 \leq r \leq m,$$

consist all the distinct q-cyclotomic cosets modulo ℓ^m. It is clear that the number of nonzero q-cyclotomic cosets modulo ℓ^m is equal to $e = \sum_{r=1}^{m} \delta(r)$. To simplify notation, we simply write $C_{\rho_0} = \{0\}$ and C_{ρ_k}, $1 \leq k \leq e$, to denote all the distinct q-cyclotomic cosets modulo ℓ^m, where C_{ρ_k} is the q-cyclotomic cosets modulo ℓ^m containing ρ_k.

Take η to be a primitive ℓ^mth root of unity (maybe in an extension field of $\mathbb{F}_q$), and denote by $M_{\rho_k}(X)$, the minimal polynomial of η^{ρ_k} over $\mathbb{F}_q$. It is well known that (e.g. see [19, Theorem 4.1.1]):

$$X^{\ell^m} - 1 = M_{\rho_0}(X) M_{\rho_1}(X) M_{\rho_2}(X) \cdots M_{\rho_e}(X), \tag{2.2}$$

with

$$M_{\rho_0}(X) = X - 1, \quad M_{\rho_k}(X) = \prod_{s \in C_{\rho_k}} (X - \eta^s), \ 1 \leq k \leq e,$$

all being monic irreducible in $\mathbb{F}_q[X]$.

We need to determine the distinct q^2-cyclotomic cosets modulo ℓ^m. It requires to consider two subcases. If $f = \mathrm{ord}_\ell(q)$ is odd, namely $\lambda(r) = \mathrm{ord}_{\ell^r}(q)$ is odd for each $1 \leq r \leq m$, then $\mathrm{ord}_{\ell^r}(q) = \mathrm{ord}_{\ell^r}(q^2)$, which means that the cyclic subgroup generated by $[q]_{\ell^r}$ in $\mathbb{Z}_{\ell^r}^*$ is equal to the cyclic subgroup generated by $[q^2]_{\ell^r}$, i.e. $\langle q \rangle = \langle q^2 \rangle$ in $\mathbb{Z}_{\ell^r}^*$; in particular, $\langle q \rangle = \langle q^2 \rangle$ in $\mathbb{Z}_{\ell^m}^*$. By the definition of q^2-cyclotomic cosets, $C_{\rho_0} = \{0\}$ and C_{ρ_k}, $1 \leq k \leq e$, also consist all the distinct q^2-cyclotomic cosets modulo ℓ^m. It follows that Formula (2.2) gives the irreducible factorization of $X^{\ell^m} - 1$ in $\mathbb{F}_{q^2}[X]$. If f is even, we deduce that $\mathrm{ord}_{\ell^r}(q^2) = \frac{\lambda(r)}{2}$ for any $1 \leq r \leq m$. It is straightforward to verify that $D_0 = \{0\}$,

$$D_{\ell^{m-r}g^j} = \left\{ \ell^{m-r}g^j, \ell^{m-r}g^j \cdot q^2, \cdots, \ell^{m-r}g^j \cdot q^{2(\frac{\lambda(r)}{2}-1)} \right\},$$

and

$$D_{\ell^{m-r}g^j q} = \left\{ \ell^{m-r}g^j q, \ell^{m-r}g^j q \cdot q^2, \cdots, \ell^{m-r}g^j q \cdot q^{2(\frac{\lambda(r)}{2}-1)} \right\}$$

consist all the distinct q^2-cyclotomic cosets modulo ℓ^m, where $0 \leq j \leq \delta(r) - 1$ and $1 \leq r \leq m$. Observe that

$$C_{\ell^{m-r}g^j} = D_{\ell^{m-r}g^j} \bigcup D_{\ell^{m-r}g^j q}, \quad \text{for each } 0 \leq j \leq \delta(r) - 1 \ \text{ and } \ 1 \leq r \leq m.$$

For simplify, we write $D_{\rho_0} = \{0\}$, D_{ρ_k} and $D_{\rho_k q}$, $1 \le k \le e$ such that $C_{\rho_k} = D_{\rho_k} \bigcup D_{\rho_k q}$, to denote all the distinct q^2-cyclotomic cosets modulo ℓ^m. By [19, Theorem 4.1.1] again, we have

$$X^{\ell^m} - 1 = (X-1)N_{\rho_1}(X)N_{\rho_1 q}(X)N_{\rho_2}(X)N_{\rho_2 q}(X)\cdots N_{\rho_e}(X)N_{\rho_e q}(X), \tag{2.3}$$

with

$$N_{\rho_k}(X) = \prod_{s \in D_{\rho_k}} (X - \eta^s), \quad N_{\rho_k q}(X) = \prod_{t \in D_{\rho_k q}} (X - \eta^t), \quad 1 \le k \le e,$$

all being monic irreducible in $\mathbb{F}_{q^2}[X]$.

In the rest of this section, we recall some basic concepts and results about constacyclic codes over $\mathbb{F}_q$. Let $\mathbb{F}_q^n$ be the $\mathbb{F}_q$-vector space of n-tuples. A *linear code* C of length n over $\mathbb{F}_q$ is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$. If λ is a nonzero element of $\mathbb{F}_q$, a linear code C of length n over $\mathbb{F}_q$ is called λ-*constacyclic* if $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C$ for every $(c_0, c_1, \cdots, c_{n-1}) \in C$. When λ =1, λ-constacyclic codes are just cyclic codes and when $\lambda = -1$, λ-constacyclic codes are known as negacyclic codes.

For any λ-constacyclic code C of length n over $\mathbb{F}_q$, the *dual code of* C is defined as $C^\perp = \{u \in \mathbb{F}_q^n \mid u \cdot v = 0, \text{for any } v \in C\}$, where $u \cdot v$ denotes the standard Euclidean inner product of u and v in $\mathbb{F}_q^n$. The code C is said to be *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if $C = C^\perp$. It turns out that the dual of a λ-constacyclic code is a λ^{-1}-constacyclic code; specifically, the dual of a cyclic code is a cyclic code and the dual of a negacyclic code is a negacyclic code (e.g. see [14, Proposition 2.2.]).

We know that any λ-constacyclic code C of length n over $\mathbb{F}_q$ is identified with exactly one ideal of the quotient algebra $\mathbb{F}_q[X]/\langle X^n - \lambda\rangle$, 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 and denote it by $C = \langle g(X)\rangle$. Assume that $C = \langle g(X)\rangle$ is a λ-constacyclic code of length n over $\mathbb{F}_q$, where $g(X)$ is the generator polynomial of C. Let $h(X) = \frac{X^n - \lambda}{g(X)}$. It is known that its dual code $C^\perp$ has generator polynomial $h^*(X)$, where $h^*(X) = h(0)^{-1}X^{\deg h}h(\frac{1}{X})$ is called the *reciprocal polynomial* of $h(X)$. Note that $h^*(X)$ is a monic divisor of $X^n - \lambda^{-1}$. If a polynomial is equal to its reciprocal polynomial, then it is called *self-reciprocal*. Suppose that $f(X) \in \mathbb{F}_q[X]$ is a polynomial with leading coefficient $a_n \neq 0$. We denote by $\hat{f}(X)$, the monic polynomial such that $\hat{f}(X) = a_n^{-1}f(X)$.

3 Constacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$

Let ℓ be an odd prime different from p as before. Recall from (2.1) that $\mathrm{ord}_{\ell^r}(q) = \lambda(r)$ and $\delta(r) = \frac{\phi(\ell^r)}{\lambda(r)}$, $1 \le r \le m$. We take a primitive ℓ^mth root η of unity in the finite field $\mathbb{F}_{q^{\lambda(m)}}$; by (2.2), we have the factorization of $X^{2\ell^m p^n} - 1$ into irreducible factors over $\mathbb{F}_q$ as follows:

$$X^{2\ell^m p^n} - 1 = (X^{2\ell^m} - 1)^{p^n} = (X^{\ell^m} - 1)^{p^n}(X^{\ell^m} + 1)^{p^n} = \prod_{i=0}^{e} M_{\rho_i}(X)^{p^n}\hat{M}_{\rho_i}(-X)^{p^n}. \tag{3.1}$$

The following lemma (see [9, Theorem 3.2]) shows that in order to obtain all constacyclic codes of length n over $\mathbb{F}_q$, we only need to consider λ-constacyclic codes, where λ runs over any fixed transversal of $\langle \xi^n\rangle$ in $\langle \xi\rangle$.

Lemma 3.1. *For any $\lambda, \mu \in \mathbb{F}_q^*$, the following four statements are equivalent:*

- **(i)** $\lambda^{-1}\mu \in \langle \xi^n\rangle$.
- **(ii)** $(\lambda^{-1}\mu)^d = 1$, *where* $d = \frac{q-1}{\gcd(n, q-1)}$.
- **(iii)** *λ and μ are n-equivalent in $\mathbb{F}_q^*$, namely there exists an element $a \in \mathbb{F}_q^*$ such that $a^n\lambda = \mu$.*
- **(iv)** *There exists an $a \in \mathbb{F}_q^*$ such that*

$$\varphi_a : \ \mathbb{F}_q[X]/\langle X^n - \mu\rangle \ \to \ \mathbb{F}_q[X]/\langle X^n - \lambda\rangle$$
$$f(X) \mapsto f(aX),$$

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

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

If λ and μ are n-equivalent, we say that, the λ-constacyclic codes of length n are n-equivalent to the μ-constacyclic codes of length n. That is, it is enough to study the n-equivalence classes of constacyclic codes.

By Lemma 3.1, the number of $2\ell^m p^n$-equivalence classes in $\mathbb{F}_q^*$ is equal to $\gcd(2\ell^m p^n, q-1) = \gcd(2\ell^m, q-1)$. Clearly, the cases $\gcd(\ell, q-1) = 1$ and $\gcd(\ell, q-1) = \ell$ are distinguishable.

We first consider the case $\gcd(\ell, q-1) = 1$. In this situation, we have

$$\mathbb{F}_q^* = \langle \xi \rangle = \langle \xi^{2\ell^m p^n} \rangle \cup \xi^{p^n} \langle \xi^{2\ell^m p^n} \rangle,$$

which means the λ-constacyclic codes are $2\ell^m p^n$-equivalent to the cyclic codes or ξ^{p^n}-constacyclic codes by Lemma 3.1. Since $X^2 - \xi \in \mathbb{F}_q[X]$ is irreducible, it follows that $\mathbb{F}_{q^2}$ is a splitting field for $X^2 - \xi$ over $\mathbb{F}_q$. Now an element α_1 in $\mathbb{F}_{q^2}$ can be found such that $\alpha_1^2 = \xi$. It is readily seen that $\alpha_1 \in \mathbb{F}_{q^2}$ is a primitive $2(q-1)$th root of unity, which gives that $\alpha_1 \in \mathbb{F}_{q^2}$ and $\alpha_1 \notin \mathbb{F}_q$.

Let

$$S = \Big\{ \alpha \in \mathbb{F}_{q^2}^* \,\Big|\, \alpha \text{ is a primitive } 2(q-1)\text{th root of unity} \Big\}.$$

It follows from $\gcd(\ell^m, 2(q-1)) = 1$ that there is a bijection $\theta : S \to S$ such that $\theta(\alpha) = \alpha^{\ell^m}$ for any $\alpha \in S$. Thus, a unique element of S, say β_1, can be found such that $\alpha_1^{-1} = \theta(\beta_1) = \beta_1^{\ell^m}$, i.e., $\beta_1^{\ell^m} \alpha_1 = 1$. Obviously, $\beta_1 \notin \mathbb{F}_q$. We claim that $\beta_1^q = -\beta_1$. To see this, it is enough to show that $\beta_1^2 \in \mathbb{F}_q$. Note that $\beta_1^{2q-2} = 1$, which implies $\beta_1^{2q} = \beta_1^2$, as claimed.

Theorem 3.2. *With respect to the above notations, we assume further that* $\gcd(\ell, q-1) = 1$. *Let C be a λ-constacyclic code of length $2\ell^m p^n$ over $\mathbb{F}_q$. Then one of the following statements holds:*

(A) *either $\lambda \in \langle \xi^2 \rangle$, then $a^{2\ell^m p^n} \lambda = 1$ for some $a \in \mathbb{F}_q^*$, and we have*

$$C = \left\langle \prod_{i=0}^{e} \hat{M}_{\rho_i}(aX)^{\varepsilon_i} \hat{M}_{\rho_i}(-aX)^{\epsilon_i} \right\rangle, \qquad 0 \le \varepsilon_i, \epsilon_i \le p^n, \quad \text{for any } \ i = 0, 1, \cdots, e;$$

(B) *or $\lambda \notin \langle \xi^2 \rangle$, then $b^{2\ell^m p^n} \lambda = \xi^{p^n}$ for some $b \in \mathbb{F}_q^*$, and there are two subcases:*

(B1) *if $f = \mathrm{ord}_\ell(q)$ is odd, we have that*

$$C = \left\langle \prod_{i=0}^{e} \hat{S}_i(bX)^{\varepsilon_i} \right\rangle, \qquad 0 \le \varepsilon_i \le p^n, \text{ for any } \ i = 0, 1, \cdots, e,$$

where $S_i(X) = \hat{M}_{\rho_i}(\beta_1 X) \hat{M}_{\rho_i}(-\beta_1 X)$ for each $0 \le i \le e$.

(B2) *if $f = \mathrm{ord}_\ell(q)$ is even, we have that*

$$C = \left\langle \hat{P}(bX)^{\varepsilon} \prod_{i=0}^{e} \hat{Q}_i(bX)^{\varepsilon_i} \hat{R}_i(bX)^{\epsilon_i} \right\rangle, \qquad 0 \le \varepsilon, \varepsilon_i, \epsilon_i \le p^n, \text{ for any } \ i = 0, 1, \cdots, e,$$

where $P(X) = (X - \beta_1^{-1})(X + \beta_1^{-1})$, $Q_i(X) = \hat{N}_{\rho_i}(\beta_1 X) \hat{N}_{\rho_i q}(-\beta_1 X)$ and $R_i(X) = \hat{N}_{\rho_i q}(\beta_1 X) \hat{N}_{\rho_i}(-\beta_1 X)$ for each $0 \le i \le e$.

Proof. Since $\gcd(\ell, q-1) = 1$, it is clear that $\langle \xi^{2\ell^m p^n} \rangle = \langle \xi^2 \rangle$. From $\lambda \in \langle \xi^2 \rangle$, we have $\lambda^{-1} \in \langle \xi^2 \rangle$, which implies that an element $a \in \mathbb{F}_q^*$ can be found satisfying $a^{2\ell^m p^n} = \lambda^{-1}$, i.e., $a^{2\ell^m p^n} \lambda = 1$. By (3.1),

$$(aX)^{2\ell^m p^n} - 1 = \prod_{i=0}^{e} M_{\rho_i}(aX)^{p^n} \hat{M}_{\rho_i}(-aX)^{p^n}.$$

This leads to

$$X^{2\ell^m p^n} - \lambda = X^{2\ell^m p^n} - a^{-2\ell^m p^n} = \prod_{i=0}^{e} \hat{M}_{\rho_i}(aX)^{p^n} \hat{M}_{\rho_i}(-aX)^{p^n},$$

proving (A).

Assume now that $\lambda \notin \langle \xi^2 \rangle$, which forces $\lambda \in \xi^{p^n}\langle \xi^2 \rangle$. We first give the irreducible factorization of $X^{2\ell^m p^n} - \xi^{p^n}$ over $\mathbb{F}_q$. Clearly, it suffices to determine the irreducible factors of $X^{2\ell^m} - \xi$ over $\mathbb{F}_q$. As discussed previously, we take α_1 to be an element in $\mathbb{F}_{q^2}$ so that $\alpha_1^2 = \xi$. That is, we have the irreducible factorization of $X^2 - \xi$ in $\mathbb{F}_{q^2}[X]$, $X^2 - \xi = (X - \alpha_1)(X + \alpha_1)$. It follows that $X^{2\ell^m} - \xi = (X^{\ell^m} - \alpha_1)(X^{\ell^m} + \alpha_1)$. There exists an element $\beta_1 \in \mathbb{F}_{q^2}$ such that $\beta_1^{\ell^m}\alpha_1 = 1$; furthermore, β_1 satisfies $\beta_1^q = -\beta_1$.

At this point, the cases f being odd and even diverge.

Assume first that f is odd. By the discussion in Section 2, we know that $C_{\rho_0} = \{0\}$ and C_{ρ_k}, $1 \le k \le e$, consist all the distinct q^2-cyclotomic cosets modulo ℓ^m. That is to say, Formula (2.2) gives the irreducible factorization of $X^{\ell^m} - 1$ over $\mathbb{F}_{q^2}$. Substituting $\beta_1 X$ for X into Formula (2.2), we get the irreducible factorization of $X^{\ell^m} - \alpha_1$ over $\mathbb{F}_{q^2}$:

$$X^{\ell^m} - \alpha_1 = \hat{M}_{\rho_0}(\beta_1 X)\hat{M}_{\rho_1}(\beta_1 X)\cdots\hat{M}_{\rho_e}(\beta_1 X).$$

Similarly, we have the irreducible factorization of $X^{\ell^m} + \alpha_1$ over $\mathbb{F}_{q^2}$:

$$X^{\ell^m} + \alpha_1 = \hat{M}_{\rho_0}(-\beta_1 X)\hat{M}_{\rho_1}(-\beta_1 X)\cdots\hat{M}_{\rho_e}(-\beta_1 X).$$

Combining these results, we have

$$X^{2\ell^m} - \xi = (X^{\ell^m} - \alpha_1)(X^{\ell^m} + \alpha_1) = \prod_{i=0}^{e} \hat{M}_{\rho_i}(\beta_1 X)\hat{M}_{\rho_i}(-\beta_1 X),$$

which is the monic irreducible factorization of $X^{2\ell^m} - \xi$ over $\mathbb{F}_{q^2}$. Let $S_i(X) = \hat{M}_{\rho_i}(\beta_1 X)\hat{M}_{\rho_i}(-\beta_1 X)$ for each $0 \le i \le e$. We claim that $S_i(X)$ is an irreducible polynomial over $\mathbb{F}_q$. Recall that

$$\hat{M}_{\rho_i}(\beta_1 X) = \prod_{k \in C_{\rho_i}} (X - \beta_1^{-1}\eta^k) \quad \text{and} \quad \hat{M}_{\rho_i}(-\beta_1 X) = \prod_{k \in C_{\rho_i}} (X + \beta_1^{-1}\eta^k).$$

Then $\beta_1^{-1}\eta^k$ gives all the roots of $\hat{M}_{\rho_i}(\beta_1 X)$ when k ranges over C_{ρ_i}. Since f is odd, we have proved that C_{ρ_i} is also a q^2-cyclotomic coset modulo ℓ^m. For $k \in C_{\rho_i}$, it follows from $\beta_1^q = -\beta_1$ that $(\beta_1^{-1}\eta^k)^q = \beta_1^{-q}\eta^{kq} = -\beta_1^{-1}\eta^{kq}$. Now $kq \in C_{\rho_i}$ and $\hat{M}_{\rho_i}(-\beta_1 X) = \prod_{k \in C_{\rho_i}} (X + \beta_1^{-1}\eta^k)$, which shows that $(\beta_1^{-1}\eta^k)^q$ is a root of $\hat{M}_{\rho_i}(-\beta_1 X)$. We deduce that $S_i(X) = \hat{M}_{\rho_i}(\beta_1 X)\hat{M}_{\rho_i}(-\beta_1 X)$ is an irreducible polynomial over $\mathbb{F}_q$, as claimed. We get the irreducible factorization of $X^{2\ell^m p^n} - \xi$ over $\mathbb{F}_q$ as follows:

$$X^{2\ell^m p^n} - \xi^{p^n} = (X^{2\ell^m} - \xi)^{p^n} = \prod_{i=0}^{e} \left(\hat{M}_{\rho_i}(\beta_1 X)\hat{M}_{\rho_i}(-\beta_1 X)\right)^{p^n} = \prod_{i=0}^{e} S_i(X)^{p^n}. \tag{3.2}$$

Since $\lambda \in \xi^{p^n}\langle \xi^{2\ell^m p^n} \rangle$, there exists an element $b \in \mathbb{F}_q^*$ such that $b^{2\ell^m p^n}\lambda = \xi^{p^n}$. We establish the following $\mathbb{F}_q$-algebra isomorphism:

$$\mathbb{F}_q[X]/\langle X^{2\ell^m p^n} - \xi^{p^n} \rangle \longrightarrow \mathbb{F}_q[X]/\langle X^{2\ell^m p^n} - \lambda \rangle, \quad f(X) \longrightarrow f(bX).$$

By (3.2), we get the irreducible factorization of $X^{2\ell^m p^n} - \lambda$ over $\mathbb{F}_q$:

$$X^{2\ell^m p^n} - \lambda = \prod_{i=0}^{e} \hat{S}_i(bX)^{p^n},$$

which gives the desired result.

It remains to consider the case when f is even. It is known that D_0, $D_{\ell^{m-r}g^j}$ and $D_{\ell^{m-r}g^j q}$ consist all the distinct q^2-cyclotomic cosets modulo ℓ^m, where $0 \le j \le \delta(r) - 1$ and $1 \le r \le m$. That is,

$$X^{\ell^m} - 1 = (X - 1)N_{\rho_1}(X)N_{\rho_1 q}(X)N_{\rho_2}(X)N_{\rho_2 q}(X)\cdots N_{\rho_e}(X)N_{\rho_e q}(X),$$

gives the irreducible factorization of $X^{\ell^m}-1$ over $\mathbb{F}_{q^2}$ as has been shown in (2.3). Working as the same with the case of f being odd, we get the irreducible factorizations of $X^{\ell^m}-\alpha_1$ and $X^{\ell^m}+\alpha_1$ over $\mathbb{F}_{q^2}$:

$$X^{\ell^m}-\alpha_1=(X-\beta_1^{-1})\hat{N}_{\rho_1}(\beta_1X)\hat{N}_{\rho_1q}(\beta_1X)\hat{N}_{\rho_2}(\beta_1X)\hat{N}_{\rho_2q}(\beta_1X)\cdots\hat{N}_{\rho_e}(\beta_1X)\hat{N}_{\rho_eq}(\beta_1X),$$

$$X^{\ell^m}+\alpha_1=(X+\beta_1^{-1})\hat{N}_{\rho_1}(-\beta_1X)\hat{N}_{\rho_1q}(-\beta_1X)\hat{N}_{\rho_2}(-\beta_1X)\hat{N}_{\rho_2q}(-\beta_1X)\cdots\hat{N}_{\rho_e}(-\beta_1X)\hat{N}_{\rho_eq}(-\beta_1X).$$

Now the irreducible factorization of $X^{2\ell^m}-\xi$ over $\mathbb{F}_{q^2}$ is given by

$$X^{2\ell^m}-\xi=(X^{\ell^m}-\alpha_1)(X^{\ell^m}+\alpha_1)=(X-\beta_1^{-1})(X+\beta_1^{-1})\prod_{i=0}^{e}\hat{N}_{\rho_i}(\beta_1X)\hat{N}_{\rho_iq}(\beta_1X)\hat{N}_{\rho_i}(-\beta_1X)\hat{N}_{\rho_iq}(-\beta_1X).$$

Let $P(X)=(X-\beta_1^{-1})(X+\beta_1^{-1})$, $Q_i(X)=\hat{N}_{\rho_i}(\beta_1X)\hat{N}_{\rho_iq}(-\beta_1X)$ and $R_i(X)=\hat{N}_{\rho_iq}(\beta_1X)\hat{N}_{\rho_i}(-\beta_1X)$ for each $0\le i\le e$. Using arguments similar to the proof in (A), we see that $P(X)$, $Q_i(X)$ and $R_i(X)$ are irreducible polynomials over $\mathbb{F}_q$. Then we get the irreducible factorization of $X^{2\ell^mp^n}-\xi^{p^n}$ over $\mathbb{F}_q$ as follows:

$$X^{2\ell^mp^n}-\xi^{p^n}=(X^{2\ell^m}-\xi)^{p^n}=P(X)^{p^n}\prod_{i=0}^{e}Q_i(X)^{p^n}R_i(X)^{p^n}. \tag{3.3}$$

Finally, we get the irreducible factorization of $X^{2\ell^mp^n}-\lambda$ over $\mathbb{F}_q$:

$$X^{2\ell^mp^n}-\lambda=\hat{P}(bX)^{p^n}\prod_{i=0}^{e}\hat{Q}_i(bX)^{p^n}\hat{R}_i(bX)^{p^n}.$$

□

Next we consider the case $\gcd(\ell,q-1)=\ell$, namely $\ell\mid(q-1)$. We use Lemma 3.1 again to obtain the concerning results. We first adopt the following notations: $\ell^u\|(q-1), v=\min\{m,u\}$ and $\zeta=\xi^{\frac{q-1}{\ell^v}}$.

Theorem 3.3. *With respect to the above notations, we assume further that $\ell\mid(q-1)$. For any nonzero element λ of $\mathbb{F}_q$ and any λ-constacyclic code C of length $2\ell^mp^n$ over $\mathbb{F}_q$, one of the following holds:*

(I) *$\lambda\in\langle\xi^{2\ell^v}\rangle$, then $c_1^{2\ell^mp^n}\lambda=1$ for an element $c_1\in\mathbb{F}_q$ and we have (The empty product is taken to be 1):*

$$C=\left\langle\prod_{i=0}^{\ell^v-1}\left(X-c_1^{-1}\zeta^i\right)^{\varepsilon_i}\left(X+c_1^{-1}\zeta^i\right)^{\epsilon_i}\cdot\prod_{j=1}^{m-u}\prod_{\substack{k=1\\ \ell\nmid k}}^{\ell^v}\left(X^{\ell^j}-c_1^{-\ell^j}\zeta^k\right)^{\tau_k^j}\left(X^{\ell^j}+c_1^{-\ell^j}\zeta^k\right)^{\sigma_k^j}\right\rangle,$$

where $0\le\varepsilon_i,\epsilon_i\le p^n$ for any $0\le i\le\ell^v-1$, and $0\le\tau_k^j,\sigma_k^j\le p^n$ for each $1\le j\le m-u$ and $1\le k\le\ell^v$ with $\ell\nmid k$.

(II) *$\lambda\in\xi^{\ell^vp^n}\langle\xi^{2\ell^v}\rangle$, then $c_2^{2\ell^mp^n}\lambda=\xi^{\ell^vp^n}$ for an element $c_2\in\mathbb{F}_q$ and one of the following holds:*

(II.A) *if $m\le u$, then*

$$C=\left\langle\prod_{i=0}^{\ell^m-1}(X^2-c_2^{-2}\xi\alpha^i)^{\varepsilon_i}\right\rangle,\qquad 0\le\varepsilon_i\le p^n,\quad \text{for any } i=0,1,\cdots,\ell^m-1,$$

where $\alpha=\xi^{\frac{q-1}{\ell^m}}$ is a primitive ℓ^mth root of unity in $\mathbb{F}_q$;

(II.B) *otherwise, we have that*

$$C=\left\langle\prod_{i=0}^{\ell^u-1}\left(X^2-c_2^{-2}\beta^{-1}\zeta^i\right)^{\varepsilon_i}\cdot\prod_{j=1}^{m-u}\prod_{\substack{k=1\\ \ell\nmid k}}^{\ell^u}\left(X^{2\ell^j}-c_2^{-2\ell^j}\beta^{-\ell^j}\zeta^k\right)^{\sigma_k^j}\right\rangle,\qquad 0\le\varepsilon_i,\sigma_k^j\le p^n$$

where β is an element in $\langle\xi^{\ell^u}\rangle$ such that $\beta^{\ell^m}\xi^{\ell^u}=1$.

(III) $\lambda \in \xi^{jp^n}\langle \xi^{2\ell^v}\rangle$ *with* $1 \le j \le 2\ell^v - 1$ *except* $j = \ell^v$, *then there exists* $d_1 \in \mathbb{F}_q^*$ *such that* $d_1^{2\ell^m p^n}\lambda = \xi^{jp^n}$; *write* $j = y\ell^z$ *with* $\gcd(y, \ell) = 1$ *and* $0 \le z \le v-1$. *There are two subcases:*

(III.A) *if the integer* y *is odd, then we have*

$$C = \left\langle \prod_{i=0}^{\ell^z - 1} (X^{2\ell^{m-z}} - d_1^{-2\ell^{m-z}}\delta^i \xi^y)^{\varepsilon_i} \right\rangle, \qquad 0 \le \varepsilon_i \le p^n;$$

(III.B) *otherwise, writing* $y = 2y_0$, *we have*

$$C = \left\langle \prod_{i=0}^{\ell^z - 1} (X^{\ell^{m-z}} - d_1^{-\ell^{m-z}}\delta^i \xi^{y_0})^{\varepsilon_i} (X^{\ell^{m-z}} + d_1^{-\ell^{m-z}}\delta^i \xi^{y_0})^{\epsilon_i} \right\rangle, \qquad 0 \le \varepsilon_i, \epsilon_i \le p^n,$$

where $\delta = \xi^{(q-1)/\ell^z}$ *is a primitive* ℓ^z*th root of unity in* $\mathbb{F}_q$.

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 $\langle \xi^{2\ell^m p^n}\rangle = \langle \xi^{2\ell^m}\rangle = \langle \xi^{2\ell^v}\rangle$ and the index $|\mathbb{F}_q^* : \langle \xi^{2\ell^v}\rangle| = 2\ell^v$. Thus the multiplicative group $\mathbb{F}_q^*$ is decomposed into disjoint union of cosets over the subgroup $\langle \xi^{2\ell^v}\rangle$ as follows:

$$\mathbb{F}_q^* = \langle \xi \rangle = \langle \xi^{2\ell^v}\rangle \cup \xi^{p^n}\langle \xi^{2\ell^v}\rangle \cup \cdots \cup \xi^{(2\ell^v - 1)p^n}\langle \xi^{2\ell^v}\rangle. \tag{3.4}$$

So the element λ of $\mathbb{F}_q^*$ belongs to exactly one of the cosets, i.e. there is a unique integer j with $0 \le j \le 2\ell^v - 1$ such that $\lambda \in \xi^{jp^n}\langle \xi^{2\ell^v}\rangle$. We get that λ is $2\ell^m p^n$-equivalent to ξ^{jp^n}.

Case (I): $j = 0$, i.e., λ and 1 are $2\ell^m p^n$-equivalent. We have an element $c_1 \in \mathbb{F}_q^*$ such that $c_1^{2\ell^m p^n}\lambda = 1$. It needs to obtain the irreducible factorization of $X^{2\ell^m p^n} - 1$ over $\mathbb{F}_q$. Obviously,

$$X^{2\ell^m p^n} - 1 = (X^{\ell^m p^n} - 1)(X^{\ell^m p^n} + 1) = (X^{\ell^m} - 1)^{p^n}(X^{\ell^m} + 1)^{p^n}.$$

By [8, Theorem 3.1], we have the irreducible factorization of $X^{\ell^m} - 1$ over $\mathbb{F}_q$ as follows (The empty product is taken to be 1):

$$X^{\ell^m} - 1 = \prod_{i=0}^{\ell^v - 1} (X - \zeta^i) \cdot \prod_{j=1}^{m-u} \prod_{\substack{k=1 \\ \ell \nmid k}}^{\ell^v} (X^{\ell^j} - \zeta^k).$$

Since ℓ is odd, we can easily get the irreducible factorization of $X^{\ell^m} + 1$ over $\mathbb{F}_q$:

$$X^{\ell^m} + 1 = \prod_{i=0}^{\ell^v - 1} (X + \zeta^i) \cdot \prod_{j=1}^{m-u} \prod_{\substack{k=1 \\ \ell \nmid k}}^{\ell^v} (X^{\ell^j} + \zeta^k).$$

Then

$$X^{2\ell^m p^n} - 1 = \prod_{i=0}^{\ell^v - 1} (X - \zeta^i)^{p^n} (X + \zeta^i)^{p^n} \cdot \prod_{j=1}^{m-u} \prod_{\substack{k=1 \\ \ell \nmid k}}^{\ell^v} (X^{\ell^j} - \zeta^k)^{p^n} (X^{\ell^j} + \zeta^k)^{p^n}.$$

Hence

$$X^{2\ell^m p^n} - \lambda = \prod_{i=0}^{\ell^v - 1} (X - c_1^{-1}\zeta^i)^{p^n} (X + c_1^{-1}\zeta^i)^{p^n} \cdot \prod_{j=1}^{m-u} \prod_{\substack{k=1 \\ \ell \nmid k}}^{\ell^v} (X^{\ell^j} - c_1^{-\ell^j}\zeta^k)^{p^n} (X^{\ell^j} + c_1^{-\ell^j}\zeta^k)^{p^n}.$$

The conclusion (I) holds.

Case (II): $j = \ell^v$. We have an element $c_2 \in \mathbb{F}_q^*$ such that $c_2^{2\ell^m p^n}\lambda = \xi^{\ell^v p^n}$. We need to obtain the irreducible factorization of $X^{2\ell^m} - \xi^{\ell^v}$ over $\mathbb{F}_q$. There are two subcases, namely $m \le u$ and $m > u$.

If $m \le u$ then $m = \min\{m, u\} = v$. We assume that $\alpha = \xi^{\frac{q-1}{\ell^m}}$ is a primitive ℓ^mth root of unity in $\mathbb{F}_q$. Thus,

$$X^{2\ell^m p^n} - \xi^{\ell^v p^n} = \left(X^{2\ell^m} - \xi^{\ell^m}\right)^{p^n} = \prod_{i=0}^{\ell^m - 1} (X^2 - \xi\alpha^i)^{p^n},$$

gives the irreducible factorization of $X^{2\ell^m p^n} - \xi^{\ell^v p^n}$ over $\mathbb{F}_q$ (Use [24, Theorem 3.75]).

Otherwise, $u = \min\{m, u\} = v$. Then there exists an element β in $\langle \xi^{\ell^u} \rangle$ such that $\beta^{\ell^m} \xi^{\ell^u} = 1$. Indeed, $\psi : \langle \xi^{\ell^u} \rangle \to \langle \xi^{\ell^u} \rangle,\ x \mapsto x^{\ell^m}$, is a group automorphism. This implies that a unique element $\beta \in \langle \xi^{\ell^u} \rangle$ can be found such that $\psi(\beta) = \beta^{\ell^m} = \xi^{-\ell^u}$, i.e., $\beta^{\ell^m} \xi^{\ell^u} = 1$. In particular, β is a primitive $\frac{q-1}{\ell^u}$th root of unity. We get the irreducible factorization of $X^{\ell^m} - \xi^{\ell^u}$ as follows:

$$X^{\ell^m} - \xi^{\ell^u} = \prod_{i=0}^{\ell^u - 1} \left(X - \beta^{-1}\zeta^i\right) \cdot \prod_{j=1}^{m-u} \prod_{\substack{k=1 \\ \ell \nmid k}}^{\ell^u} \left(X^{\ell^j} - \beta^{-\ell^j}\zeta^k\right).$$

Using [24, Theorem 3.75], it is easily checked that

$$X^{2\ell^m} - \xi^{\ell^u} = \prod_{i=0}^{\ell^u - 1} \left(X^2 - \beta^{-1}\zeta^i\right) \cdot \prod_{j=1}^{m-u} \prod_{\substack{k=1 \\ \ell \nmid k}}^{\ell^u} \left(X^{2\ell^j} - \beta^{-\ell^j}\zeta^k\right)$$

gives the irreducible factorization of $X^{2\ell^m} - \xi^{\ell^u}$ over $\mathbb{F}_q$.

Case (III): $0 < j < 2\ell^v$ except $j = \ell^v$. We can assume that $j = y\ell^z$ with $\gcd(y, \ell) = 1$ and $0 \le z \le v - 1$. Since $\ell^v \mid (q-1)$, we see that $\delta = \xi^{(q-1)/\ell^z}$ is a primitive ℓ^zth root of unity in $\mathbb{F}_q$. Noting that $z < m$, we have

$$\left(\frac{X^{\ell^{m-z}}}{\xi^y}\right)^{\ell^z} - 1 = \left(\frac{X^{\ell^{m-z}}}{\xi^y} - 1\right)\left(\frac{X^{\ell^{m-z}}}{\xi^y} - \delta\right) \cdots \left(\frac{X^{\ell^{m-z}}}{\xi^y} - \delta^{\ell^z - 1}\right),$$

hence

$$\left(\frac{X^{\ell^{m-z}}}{\xi^y}\right)^{\ell^z p^n} - 1 = \left(\frac{X^{\ell^{m-z}}}{\xi^y} - 1\right)^{p^n} \left(\frac{X^{\ell^{m-z}}}{\xi^y} - \delta\right)^{p^n} \cdots \left(\frac{X^{\ell^{m-z}}}{\xi^y} - \delta^{\ell^z - 1}\right)^{p^n};$$

that is,

$$X^{\ell^m p^n} - \xi^{y\ell^z p^n} = (X^{\ell^{m-z}} - \xi^y)^{p^n} (X^{\ell^{m-z}} - \delta\xi^y)^{p^n} \cdots (X^{\ell^{m-z}} - \delta^{\ell^z - 1}\xi^y)^{p^n}.$$

Thus

$$X^{2\ell^m p^n} - \xi^{y\ell^z p^n} = (X^{2\ell^{m-z}} - \xi^y)^{p^n} (X^{2\ell^{m-z}} - \delta\xi^y)^{p^n} \cdots (X^{2\ell^{m-z}} - \delta^{\ell^z - 1}\xi^y)^{p^n}. \tag{3.5}$$

Now we need to give the irreducible factorization of $X^{2\ell^m p^n} - \xi^{y\ell^z p^n}$ over $\mathbb{F}_q$. There are two subcases:

(III.A) The integer y is odd. In this case, we assert that Equation (3.5) gives the irreducible factorization of $X^{2\ell^m p^n} - \xi^{y\ell^z p^n}$ over $\mathbb{F}_q$. It suffices to check that each polynomial $X^{2\ell^{m-z}} - \delta^i \xi^y$ is irreducible over $\mathbb{F}_q$, $0 \le i \le \ell^z - 1$. Recall that $\ell \nmid y$, $\ell^z < \ell^m$ and $\ell^u \| \mathrm{ord}(\xi)$. One can check that $\ell \mid \mathrm{ord}(\delta^i \xi^y)$ and $\ell \nmid \frac{q-1}{\mathrm{ord}(\delta^i \xi^y)}$; meanwhile $2 \mid \mathrm{ord}(\delta^i \xi^y)$ and $2 \nmid \frac{q-1}{\mathrm{ord}(\delta^i \xi^y)}$. Using [24, Theorem 3.75], we get the desired result.

(III.B) We are left to investigate the case $y = 2y_0$. Clearly, $X^{2\ell^m} - \xi^{2y_0\ell^z} = (X^{\ell^m} - \xi^{y_0\ell^z})(X^{\ell^m} + \xi^{y_0\ell^z})$. Hence, we get the irreducible factorization of $X^{2\ell^m p^n} - \xi^{y\ell^z p^n}$ over $\mathbb{F}_q$:

$$X^{2\ell^m p^n} - \xi^{y\ell^z p^n} = \prod_{i=0}^{\ell^z - 1} (X^{\ell^{m-z}} - \delta^i \xi^{y_0})^{p^n} (X^{\ell^{m-z}} + \delta^i \xi^{y_0})^{p^n}.$$

□

4 Dual codes

In this section, the duals of all constacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$ are explicitly obtained, where ℓ is an odd prime different from p. Among other results, all linear complementary-dual (LCD) cyclic and negacyclic codes are provided; all self-dual negacyclic codes of this length are also determined.

We give our results according to Theorem 3.2 and Theorem 3.3. The next two results give the structures of the duals of all constacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$.

Corollary 4.1. *With the notation of Theorem 3.2, we have that*

(A) $\lambda \in \langle \xi^2 \rangle$. *If C is a λ-constacyclic code presenting in Theorem 3.2* (A)*, then its dual code is the λ^{-1}-constacyclic code given by*

$$C^{\perp} = \left\langle \prod_{i=0}^{e} \hat{M}_{-\rho_i}(a^{-1}X)^{p^n-\varepsilon_i} \hat{M}_{-\rho_i}(-a^{-1}X)^{p^n-\epsilon_i} \right\rangle;$$

(B1) $\lambda \notin \langle \xi^2 \rangle$ *and f is odd. If C is a λ-constacyclic code presenting in Theorem 3.2* (B1)*, then its dual code is the λ^{-1}-constacyclic code given by*

$$C^{\perp} = \left\langle \prod_{i=0}^{e} \hat{S}_{-i}(b^{-1}X)^{p^n-\varepsilon_i} \right\rangle,$$

where $S_{-i}(X) = \hat{M}_{-\rho_i}(\beta_1^{-1}X)\hat{M}_{-\rho_i}(-\beta_1^{-1}X)$ for each $0 \le i \le e$;

(B2) $\lambda \notin \langle \xi^2 \rangle$ *and f is even. If C is a λ-constacyclic code presenting in Theorem 3.2* (B2)*, then its dual code is the λ^{-1}-constacyclic code given by*

$$C^{\perp} = \left\langle \hat{P}^*(b^{-1}X)^{p^n-\varepsilon} \prod_{i=0}^{e} \hat{Q}_{-i}(b^{-1}X)^{p^n-\varepsilon_i} \hat{R}_{-i}(b^{-1}X)^{p^n-\epsilon_i} \right\rangle,$$

where $P^*(X) = (X-\beta_1)(X+\beta_1)$, $Q_{-i}(X) = \hat{N}_{-\rho_i}(\beta_1^{-1}X)\hat{N}_{-\rho_i q}(-\beta_1^{-1}X)$ and $R_{-i}(X) = \hat{N}_{-\rho_i q}(\beta_1^{-1}X)\hat{N}_{-\rho_i}(-\beta_1^{-1}X)$ for each $0 \le i \le e$.

Proof. We just give a proof for (A), the other cases can be proved similarly. As shown in the proof of Theorem 3.2, the monic irreducible factorization of $X^{2\ell^m p^n} - \lambda$ over $\mathbb{F}_q$ is given by

$$X^{2\ell^m p^n} - \lambda = \prod_{i=0}^{e} \hat{M}_{\rho_i}(aX)^{p^n} \hat{M}_{\rho_i}(-aX)^{p^n}.$$

Then

$$h(X) = \frac{X^{2\ell^m p^n} - \lambda}{g(X)} = \prod_{i=0}^{e} \hat{M}_{\rho_i}(aX)^{p^n-\varepsilon_i} \hat{M}_{\rho_i}(-aX)^{p^n-\epsilon_i}.$$

It follows that $C^{\perp}$ has generator polynomial

$$h^*(X) = \prod_{i=0}^{e} \hat{M}_{-\rho_i}(a^{-1}X)^{p^n-\varepsilon_i} \hat{M}_{-\rho_i}(-a^{-1}X)^{p^n-\epsilon_i}.$$

□

The next result is a direct consequence of Theorem 3.3, so we omit its proof here.

Corollary 4.2. *With the notation of Theorem 3.3, we have that*

(I) *If C is a λ-constacyclic code given as in Theorem 3.3* (I)*, then its dual code is the λ^{-1}-constacyclic code given by*

$$C^{\perp} = \left\langle \prod_{i=0}^{\ell^v-1} \left(X - c_1\zeta^{-i}\right)^{p^n-\varepsilon_i} \left(X + c_1\zeta^{-i}\right)^{p^n-\epsilon_i} \cdot \prod_{j=1}^{m-u} \prod_{\substack{k=1 \\ \ell \nmid k}}^{\ell^v} \left(X^{\ell^j} - c_1^{\ell^j}\zeta^{-k}\right)^{p^n-\tau_k^j} \left(X^{\ell^j} + c_1^{\ell^j}\zeta^{-k}\right)^{p^n-\sigma_k^j} \right\rangle.$$

(II.A) *If C is a λ-constacyclic code given as in Theorem 3.3* (II.A)*, then its dual code is the λ^{-1}-constacyclic code given by*

$$C^{\perp} = \left\langle \prod_{i=0}^{\ell^m-1} (X^2 - c_2^2 \xi^{-1} \alpha^{-i})^{p^n - \varepsilon_i} \right\rangle.$$

(II.B) *If C is a λ-constacyclic code given as in Theorem 3.3* (II.B)*, then its dual code is the λ^{-1}-constacyclic code given by*

$$C^{\perp} = \left\langle \prod_{i=0}^{\ell^u-1} \left(X^2 - c_2^2 \beta \zeta^{-i}\right)^{p^n - \varepsilon_i} \cdot \prod_{j=1}^{m-u} \prod_{\substack{k=1 \\ \ell \nmid k}}^{\ell^u} \left(X^{2\ell^j} - c_2^{2\ell^j} \beta^{\ell^j} \zeta^{-k}\right)^{p^n - \sigma_k^j} \right\rangle.$$

(III.A) *If C is a λ-constacyclic code given as in Theorem 3.3* (III.A)*, then its dual code is the λ^{-1}-constacyclic code given by*

$$C^{\perp} = \left\langle \prod_{i=0}^{\ell^z-1} (X^{2\ell^{m-z}} - d_1^{2\ell^{m-z}} \delta^{-i} \xi^{-y})^{p^n - \varepsilon_i} \right\rangle.$$

(III.B) *If C is a λ-constacyclic code given as in Theorem 3.3* (III.B)*, then its dual code is the λ^{-1}-constacyclic code given by*

$$C^{\perp} = \left\langle \prod_{i=0}^{\ell^z-1} (X^{\ell^{m-z}} - d_1^{\ell^{m-z}} \delta^{-i} \xi^{-y_0})^{p^n - \varepsilon_i} (X^{\ell^{m-z}} + d_1^{\ell^{m-z}} \delta^{-i} \xi^{-y_0})^{p^n - \epsilon_i} \right\rangle.$$

We devote the rest of this section to apply our results to investigate the situations of linear complimentary-dual (LCD) codes and self-dual codes. These are the two extreme connections between C and $C^{\perp}$, where $C \bigcap C^{\perp} = \{0\}$ (for LCD codes) and $C = C^{\perp}$ (for self-dual codes). The concept of LCD codes was introduced by Massey [25] in 1992. In the same paper, he showed that asymptotically good LCD codes exist, and presented applications of LCD codes such as they provided an optimum linear coding solution for the two-user binary adder channel. It was proven by Sendrier [29] that LCD codes meet the Gilbert-Varshamov bound. Necessary and sufficient conditions for cyclic codes [34] and certain class of quasi-cyclic codes [17] to be LCD codes were obtained.

For the case of LCD constacyclic codes, it was shown that any λ-constacyclic code with $\lambda \notin \{-1, 1\}$ is a LCD code ([16]). So in order to obtain all LCD λ-constacyclic codes, we only need to work on cyclic and negacyclic codes.

Recall that $\mathrm{ord}_{\ell}(q) = f$, the multiplicative order of q in $\mathbb{Z}_{\ell}^*$. Also recall that $\mathrm{ord}_{\ell^r}(q) = \lambda(r)$ and $\delta(r) = \frac{\phi(\ell^r)}{\lambda(r)}$, $1 \leq r \leq m$. We have to distinguish the cases when f is odd or even. If $f = \mathrm{ord}_{\ell}(q)$ is even, it has been shown that the monic irreducible factors of $X^{\ell^m} - 1$ are self-reciprocal (e.g. see [23, Theorem 1]). The next lemma is concerned with the case when f is odd, in which case it shows that all the irreducible factors of $X^{\ell^m} - 1$ are not self-reciprocal except the trivial factor $X - 1$.

Lemma 4.3. *Let ℓ be an odd prime relatively prime to q. Assume further that $f = \mathrm{ord}_{\ell}(q)$ is odd. If g is a fixed generator of the cyclic group $\mathbb{Z}_{\ell^m}^*$, then all the distinct q-cyclictomic cosets modulo ℓ^m are given by $C_0 = \{0\}$,*

$$C_{\ell^{m-r} g^k} = \left\{ \ell^{m-r} g^k, \ell^{m-r} g^k q, \cdots, \ell^{m-r} g^k q^{\lambda(r)-1} \right\},$$

$$C_{-\ell^{m-r} g^k} = \left\{ -\ell^{m-r} g^k, -\ell^{m-r} g^k q, \cdots, -\ell^{m-r} g^k q^{\lambda(r)-1} \right\},$$

where $1 \leq r \leq m$, $0 \leq k \leq \frac{\delta(r)}{2} - 1$.

Proof. We first claim that the cyclotomic cosets $C_{\ell^{m-r}g^k}$ and $C_{-\ell^{m-r}g^k}$ with $1 \le r \le m$, $0 \le k \le \frac{\delta(r)}{2} - 1$ are distinct from each other. Suppose otherwise that $C_{z\ell^{m-r_1}g^{k_1}} = C_{\ell^{m-r_2}g^{k_2}}$ for some $1 \le r_1, r_2 \le m$, $0 \le k_1, k_2 \le \frac{\delta(r)}{2} - 1$ and $z \in \{1, -1\}$. Then there exists some integer j such that

$$z\ell^{m-r_1}g^{k_1} \equiv \ell^{m-r_2}g^{k_2}q^j \pmod{\ell^m}. \tag{4.1}$$

It follows that $\gcd(z\ell^{m-r_1}g^{k_1}, \ell^m) = \gcd(\ell^{m-r_2}g^{k_2}q^j, \ell^m)$, which forces $r_1 = r_2$. Therefore, $zg^{k_1} \equiv g^{k_2}q^j \pmod{\ell^{r_1}}$, which gives $g^{2\lambda(r_1)k_1} \equiv g^{2\lambda(r_1)k_2} \pmod{\ell^{r_1}}$. We get $2\lambda(r_1)(k_1 - k_2) \equiv 0 \pmod{\phi(\ell^{r_1})}$, since g is of order $\phi(\ell^{r_1})$ in $\mathbb{Z}^*_{\ell^{r_1}}$. Hence, $k_1 = k_2$. Then (4.1) gives $z \equiv q^j \pmod{\ell^{r_1}}$. Using $\mathrm{ord}_{\ell^{r_1}}(q) = \lambda(r_1)$ again, we have that $\lambda(r_1)$ divides $2j$. Since $\lambda(r_1)$ is odd (f and ℓ are all the divisors of $\lambda(r_1)$), we get $\lambda(r_1)$ divides j. This leads to $1 \equiv q^j \pmod{\ell^{r_1}}$. We then see that $z = 1$, as claimed.

Finally,

$$|C_0| + \sum_{r=1}^{m}\sum_{k=0}^{\frac{\delta(r)}{2}-1}(|C_{\ell^{m-r}g^k}| + |C_{-\ell^{m-r}g^k}|) = 1 + \sum_{r=1}^{m}\sum_{k=0}^{\frac{\delta(r)}{2}-1} 2\lambda(r) = 1 + \sum_{r=1}^{m}\lambda(r)\delta(r) = \ell^m.$$

This completes the proof. □

Assuming that $\mathrm{ord}_\ell(q) = f$ is odd, by Lemma 4.3,

$$X^{\ell^m} - 1 = (X-1)\prod_{r=1}^{m}\prod_{k=0}^{\frac{\delta(r)}{2}-1} M_{\ell^{m-r}g^k}(X)M_{-\ell^{m-r}g^k}(X) \tag{4.2}$$

gives the irreducible factorization of $X^{\ell^m} - 1$ over $\mathbb{F}_q$. Clearly, in this case, $(X-1)^* = X - 1$ and $M^*_{\ell^{m-r}g^k}(X) = M_{-\ell^{m-r}g^k}(X)$ for each $1 \le r \le m$, $0 \le k \le \frac{\delta(r)}{2} - 1$.

The next result characterizes all LCD cyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$.

Theorem 4.4. *Let ℓ be an odd prime different from p. The following statements hold:*

(i) If $f = \mathrm{ord}_\ell(q)$ is odd, then there are exactly 2^{e+2} LCD cyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$ generated by

$$(X-1)^{\varepsilon_0}(X+1)^{\epsilon_0}\prod_{r=1}^{m}\prod_{k=0}^{\frac{\delta(r)}{2}-1} M_{\ell^{m-r}g^k}(X)^{\varepsilon_k^r}M_{-\ell^{m-r}g^k}(X)^{\varepsilon_k^r}\hat{M}_{\ell^{m-r}g^k}(-X)^{\sigma_k^r}\hat{M}_{-\ell^{m-r}g^k}(-X)^{\sigma_k^r},$$

where $\varepsilon_0, \epsilon_0, \varepsilon_k^r, \sigma_k^r \in \{0, p^n\}$, for every $1 \le r \le m$ and $0 \le k \le \frac{\delta(r)}{2} - 1$;

(ii) if $f = \mathrm{ord}_\ell(q)$ is even, then there are exactly $2^{2(e+1)}$ LCD cyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$ generated by

$$\prod_{i=0}^{e}\hat{M}_{\rho_i}(X)^{\varepsilon_i}\hat{M}_{\rho_i}(-X)^{\epsilon_i}, \qquad \varepsilon_i, \epsilon_i \in \{0, p^n\}, \quad i = 0, 1, \cdots, e.$$

Proof. We just give a proof for (i), since the proof for (ii) is similar. We get the desired result by computing the intersection of C and $C^\perp$. Form Lemma 4.3 and (4.2), we can assume that C is a cyclic code of length $2\ell^m p^n$ over $\mathbb{F}_q$ generated by

$$(X-1)^{\varepsilon_0}(X+1)^{\epsilon_0}\prod_{r=1}^{m}\prod_{k=0}^{\frac{\delta(r)}{2}-1} M_{\ell^{m-r}g^k}(X)^{\varepsilon_k^r}M_{-\ell^{m-r}g^k}(X)^{\epsilon_k^r}\hat{M}_{\ell^{m-r}g^k}(-X)^{\sigma_k^r}\hat{M}_{-\ell^{m-r}g^k}(-X)^{\tau_k^r},$$

where $0 \le \varepsilon_0, \epsilon_0 \le p^n$, $0 \le \varepsilon_k^r, \epsilon_k^r, \sigma_k^r, \tau_k^r \le p^n$ for every $1 \le r \le m$ and $0 \le k \le \frac{\delta(r)}{2} - 1$. Then its dual code $C^\perp$ has generator polynomial

$$(X-1)^{p^n-\varepsilon_0}(X+1)^{p^n-\epsilon_0}\prod_{r=1}^{m}\prod_{k=0}^{\frac{\delta(r)}{2}-1} M_{-\ell^{m-r}g^k}(X)^{p^n-\varepsilon_k^r}M_{\ell^{m-r}g^k}(X)^{p^n-\epsilon_k^r}\hat{M}_{-\ell^{m-r}g^k}(-X)^{p^n-\sigma_k^r}\hat{M}_{\ell^{m-r}g^k}(-X)^{p^n-\tau_k^r}.$$

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

$$\begin{aligned} p^n &= \max\{\varepsilon_0, p^n - \varepsilon_0\} = \max\{\epsilon_0, p^n - \epsilon_0\} \\ &= \max\{\varepsilon_k^r, p^n - \epsilon_k^r\} = \max\{\epsilon_k^r, p^n - \varepsilon_k^r\} \\ &= \max\{\sigma_k^r, p^n - \tau_k^r\} = \max\{\tau_k^r, p^n - \sigma_k^r\}, \end{aligned}$$

for every $1 \le r \le m$ and $0 \le k \le \frac{\delta(r)}{2} - 1$, which is equivalent to

$$\varepsilon_0, \epsilon_0 \in \{0, p^n\}, \quad \varepsilon_k^r, \sigma_k^r \in \{0, p^n\}, \quad \varepsilon_k^r = \epsilon_k^r, \quad \sigma_k^r = \tau_k^r.$$

We complete the proof of statement (i). □

Next we give all LCD negacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$. Note that 1 and -1 are $2\ell^m p^n$-equivalent if $q \equiv 1 \pmod 4$; in this case, let γ be a primitive fourth root of unity in $\mathbb{F}_q$. That is, $X^2 + 1 = (X - \gamma)(X + \gamma)$. We take an element β in $\mathbb{F}_q$ so that $\beta^{\ell^m}\gamma = 1$. Clearly, $\beta^{-1} = -\beta$. If $q \equiv 3 \pmod 4$, then X^2+1 is irreducible over $\mathbb{F}_q$; let ς be an element in $\mathbb{F}_{q^2}$ satisfying $X^2+1 = (X-\varsigma)(X+\varsigma)$. We take θ in $\mathbb{F}_{q^2}$ so that $\theta^{\ell^m}\varsigma = 1$. It follows that $\theta^{-1} = \theta^q = -\theta$.

Theorem 4.5. *Let $f = \mathrm{ord}_\ell(q)$. With the notation given above, we have that*

(i) *if $q \equiv 1 \pmod 4$, then there are exactly 2^{e+1} LCD negacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$ generated by*

$$\prod_{i=0}^{e} \hat{M}_{\rho_i}(\beta X)^{\varepsilon_i} \hat{M}_{-\rho_i}(-\beta X)^{\varepsilon_i}, \quad \varepsilon_i \in \{0, p^n\}, \quad i = 0, 1, \cdots, e;$$

(ii) *if $q \equiv 3 \pmod 4$ and f is odd, then there are exactly $2^{1+\frac{e}{2}}$ LCD negacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$ generated by*

$$(X^2+1)^{\varepsilon_0} \prod_{r=1}^{m} \prod_{k=0}^{\frac{\delta(r)}{2}-1} I_{r,k}(X)^{\varepsilon_k^r} J_{r,k}(X)^{\varepsilon_k^r}, \qquad \varepsilon_0, \varepsilon_k^r, \epsilon_k^r \in \{0, p^n\},$$

where $I_{r,k}(X) = \hat{M}_{\ell^{m-r}g^k}(\theta X)\hat{M}_{\ell^{m-r}g^k}(-\theta X)$ and $J_{r,k}(X) = \hat{M}_{-\ell^{m-r}g^k}(\theta X)\hat{M}_{-\ell^{m-r}g^k}(-\theta X)$ for every $1 \le r \le m$ and $0 \le k \le \frac{\delta(r)}{2} - 1$;

(iii) *if $q \equiv 3 \pmod 4$ and $f \equiv 2 \pmod 4$, then there are exactly 2^{1+2e} LCD negacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$ generated by*

$$(X^2+1)^{\varepsilon_0} \prod_{k=1}^{e} S_k(X)^{\varepsilon_k} T_k(X)^{\epsilon_k}, \qquad \varepsilon_0, \varepsilon_k, \epsilon_k \in \{0, p^n\}, \quad k = 1, \cdots, e,$$

where $S_k(X) = \hat{N}_{\rho_k}(\theta X)\hat{N}_{\rho_k q}(-\theta X)$ and $T_k(X) = \hat{N}_{\rho_k}(-\theta X)\hat{N}_{\rho_k q}(\theta X)$;

(iv) *if $q \equiv 3 \pmod 4$ and $f \equiv 0 \pmod 4$, then there are exactly 2^{1+e} LCD negacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$ generated by*

$$(X^2+1)^{\varepsilon_0} \prod_{k=1}^{e} S_k(X)^{\varepsilon_k} T_k(X)^{\varepsilon_k}, \qquad \varepsilon_0, \varepsilon_k \in \{0, p^n\}, \quad k = 1, \cdots, e.$$

Proof. (i) We first indicate that, $C_{\rho_0} = \{0\}$ and

$$C_{-\ell^{m-r}g^k} = \{-\ell^{m-r}g^k, -\ell^{m-r}g^k q, \cdots, -\ell^{m-r}g^k q^{\lambda(r)-1}\},\ 0 \le k \le \delta(r) - 1,\ 1 \le r \le m,$$

also consist all the distinct q-cyclotomic cosets modulo ℓ^m. That is,

$$X^{\ell^m} - 1 = M_{-\rho_0}(X) M_{-\rho_1}(X) M_{-\rho_2}(X) \cdots M_{-\rho_e}(X),$$

gives the monic irreducible factorization of $X^{\ell^m}-1$ over $\mathbb{F}_q$. Since γ is a primitive fourth root of unity in $\mathbb{F}_q$, it follows that $X^{2\ell^m}+1=(X^{\ell^m}-\gamma)(X^{\ell^m}+\gamma)$. Then

$$X^{\ell^m}-\gamma=\gamma M_{\rho_0}(\beta X)M_{\rho_1}(\beta X)M_{\rho_2}(\beta X)\cdots M_{\rho_e}(\beta X),$$

$$X^{\ell^m}+\gamma=-\gamma M_{-\rho_0}(-\beta X)M_{-\rho_1}(-\beta X)M_{-\rho_2}(-\beta X)\cdots M_{-\rho_e}(-\beta X),$$

where β is an element in $\mathbb{F}_q$ with $\beta^{\ell^m}\gamma=1$. This implies that

$$X^{2\ell^m p^n}+1=\prod_{i=0}^{e}\hat{M}_{\rho_i}(\beta X)^{p^n}\hat{M}_{-\rho_i}(-\beta X)^{p^n},$$

gives the irreducible factorization of $X^{2\ell^m p^n}+1$ over $\mathbb{F}_q$. Recall that

$$M_{\rho_i}(X)=\prod_{j\in C_{\rho_i}}(X-\eta^j),\ 1\le i\le e.$$

Now it is routine to check that

$$\hat{M}^*_{\rho_i}(\beta X)=\prod_{j\in C_{\rho_i}}(X-\beta^{-1}\eta^j)^*=\prod_{j\in C_{\rho_i}}(X-\beta\eta^{-j})=\prod_{j\in C_{-\rho_i}}(X-\beta\eta^j)=\hat{M}_{-\rho_i}(-\beta X).$$

Using arguments similar to those of Theorem 4.4, we get the statement of (i).

(ii) From Lemma 4.3, the monic irreducible factorization of $X^{\ell^m}-1$ can be given as follows:

$$X^{\ell^m}-1=(X-1)\prod_{r=1}^{m}\prod_{k=0}^{\frac{\delta(r)}{2}-1}M_{\ell^{m-r}g^k}(X)M_{-\ell^{m-r}g^k}(X).$$

As discussed previously, an element $\varsigma\in\mathbb{F}_{q^2}$ can be found such that $X^2+1=(X-\varsigma)(X+\varsigma)$, which gives $X^{2\ell^m}+1=(X^{\ell^m}-\varsigma)(X^{\ell^m}+\varsigma)$. Further, we have $\theta^{\ell^m}\varsigma=1$, where $\theta\in\mathbb{F}_{q^2}$ satisfies $\theta^{-1}=-\theta=\theta^q$. Thus,

$$X^{\ell^m}-\varsigma=(X-\theta^{-1})\prod_{r=1}^{m}\prod_{k=0}^{\frac{\delta(r)}{2}-1}\hat{M}_{\ell^{m-r}g^k}(\theta X)\hat{M}_{-\ell^{m-r}g^k}(\theta X)$$

and

$$X^{\ell^m}+\varsigma=(X+\theta^{-1})\prod_{r=1}^{m}\prod_{k=0}^{\frac{\delta(r)}{2}-1}\hat{M}_{\ell^{m-r}g^k}(-\theta X)\hat{M}_{-\ell^{m-r}g^k}(-\theta X).$$

Therefore, the irreducible factorization of $X^{2\ell^m p^n}+1$ over $\mathbb{F}_q$ are given as follows:

$$X^{2\ell^m p^n}+1=(X^2+1)^{p^n}\prod_{r=1}^{m}\prod_{k=0}^{\frac{\delta(r)}{2}-1}I_{r,k}(X)^{p^n}J_{r,k}(X)^{p^n},$$

where $I_{r,k}(X)=\hat{M}_{\ell^{m-r}g^k}(\theta X)\hat{M}_{\ell^{m-r}g^k}(-\theta X)$ and $J_{r,k}(X)=\hat{M}_{-\ell^{m-r}g^k}(\theta X)\hat{M}_{-\ell^{m-r}g^k}(-\theta X)$ for every $1\le r\le m$ and $0\le k\le\frac{\delta(r)}{2}-1$. We just note that

$$\hat{M}^*_{\ell^{m-r}g^k}(\theta X)=\hat{M}_{-\ell^{m-r}g^k}(-\theta X),\quad \hat{M}^*_{\ell^{m-r}g^k}(-\theta X)=\hat{M}_{-\ell^{m-r}g^k}(\theta X).$$

That is, $I^*_{r,k}(X)=J_{r,k}(X)$.

Using similar arguments, we obtain (iii) and (iv). □

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. [16]). It is also known that self-dual cyclic codes over a finite field exist if and only if the code length is even and the characteristic of the underlying field is two ([20]). Thus, we focus on self-dual negacyclic codes, which also have received a good deal of attention.

Corollary 4.6. *With the notations as in Theorem 4.5, we have that*

(i) *if* $q \equiv 1 \pmod 4$, *then there are exactly* $(p^n+1)^{e+1}$ *self-dual negacyclic codes of length* $2\ell^m p^n$ *over* $\mathbb{F}_q$ *generated by*

$$\prod_{i=0}^{e} \hat{M}_{\rho_i}(\beta X)^{\varepsilon_i} \hat{M}_{-\rho_i}(-\beta X)^{p^n-\varepsilon_i}, \quad 0 \le \varepsilon_i \le p^n, \quad i = 0, 1, \cdots, e;$$

(ii) *if* $q \equiv 3 \pmod 4$, *then there does not exist self-dual negacyclic codes of length* $2\ell^m p^n$ *over* $\mathbb{F}_q$.

Proof. From Theorem 4.5 (i) and its proof, we know that

$$X^{2\ell^m p^n} + 1 = \prod_{i=0}^{e} \hat{M}_{\rho_i}(\beta X)^{p^n} \hat{M}_{-\rho_i}(-\beta X)^{p^n},$$

gives the irreducible factorization of $X^{2\ell^m p^n}+1$ over $\mathbb{F}_q$. Moreover, $\hat{M}^*_{\rho_i}(\beta X) = \hat{M}_{-\rho_i}(-\beta X)$. We deduce that (i) holds true.

(ii) It follows from 4.5 (ii)-(iv) that X^2+1 is a self-reciprocal irreducible polynomial of $X^{2\ell^m p^n}+1$ over $\mathbb{F}_q$. This gives that there does not exist self-dual negacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$. □

5 Conclusion

In this paper, we have classified all constacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$, where p is the characteristic of $\mathbb{F}_q$ and ℓ is an odd prime different from p. The characterization and enumeration of all linear complimentary dual and self-dual constacyclic codes of length $2\ell^m p^n$ over $\mathbb{F}_q$ are obtained at the same time.

It would be interesting to classify constacyclic codes over $\mathbb{F}_q$ of length $k\ell^m p^n$, where p is the characteristic of $\mathbb{F}_q$, ℓ is an odd prime different from p and k is a prime different from ℓ and p. However, this is not an easy task by using the same techniques developed in this paper.

We give an example to show the obstacles: Classify all constacyclic codes over $\mathbb{F}_7$ of length $5 \times 3^2 \times 7$, i.e., $k = 5, \ell = 3, p = 7, m = 2$ and $n = 1$. It follows from [Theorem 3.2, 7] that the number of 315-isometry classes of $\mathbb{F}_7^*$ is equal to 2. Let $\mathbb{F}_7^* = \langle \xi \rangle$, namely ξ is a primitive sixth root of unity. We need to give the irreducible factorization of $X^{315} - \lambda$ over $\mathbb{F}_7$. Using [Theorem 3.2, 7] again, $\lambda \cong_{315} 1$ or $\lambda \cong_{315} \xi$ ($\lambda \cong_{315} \mu$ means that λ is 315-isometric to μ by the notation in [7]). If $\lambda \cong_{315} 1$, then the irreducible factorization of $X^{315} - \lambda$ over $\mathbb{F}_7$ can be derived from the irreducible factorization of $X^{315} - 1$ over $\mathbb{F}_7$. However, it is not easy to give the irreducible factorization of $X^{315} - \xi$ over $\mathbb{F}_7$. Indeed, using Magma, one can see that there exist irreducible factors of $X^{315} - \xi$ over $\mathbb{F}_7$ with 5 terms; for example, $X^{36} + \xi^5 X^{27} + \xi^4 X^{18} - X^9 + \xi^2$ is one of the irreducible factors. (In our present case, the irreducible factors of $X^{2\times 3^2 \times 7} - \xi$ over $\mathbb{F}_7$ are binomials.)

The above example shows that a new or improved technique needs to be developed to handle the more general case.

Acknowledgements

This work was supported by NSFC (Grant No. 11171370) and self-determined research funds of CCNU from the colleges's basic research and operation of MOE (Grant No. CCNU14F01004). The research of Bocong Chen is also partially supported by Nanyang Technological University's research (Grant No. M4080456). The authors express their gratitude to the anonymous referees for meticulous reading and helpful comments.

References

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

[2] G. K. Bakshi, M. Raka, Self-dual and self-orthogonal negacyclic codes of length $2p^n$ over a finite field, Finite Fields Appl., **19**(2013), 39-54.

[3] E. R. Berlekamp, Negacyclic codes for the Lee metric, Proceedings of the Conference on Combinatorial Mathematics and Its Applications, Chapel Hill, NC (1968), 298-316.

[4] E. R. Berlekamp, Algebraic Coding Theory(Revised edition), Aegean Park, 1984.

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

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

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

[8] B. Chen, H. Liu, G. Zhang, A class of minimal cyclic codes over finite fields, Designs Codes Cryptogr., (2013), DOI: 10.1007/s10623-013-9857-9.

[9] B. Chen, H. Q. Dinh, H. Liu, Repeated-root constacyclic codes of length ℓp^s and their duals, Discrete Appl. Math., **177**(2014), 60-70.

[10] H. Q. Dinh, S. R. Lopez-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory, **8**(2004), 1728-1744.

[11] H. Q. Dinh, Complete distances of all negacyclic codes of length 2^s over Z_{2^a}, IEEE Trans. Inform. Theory, **1**(2007), 147-161.

[12] 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.

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

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

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

[16] H. Q. Dinh, Structure of repeated-root cyclic and negacyclic codes of length $6p^s$ and their duals, AMS Contemporary Mathematics, **609**(2014), 69-87.

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

[18] 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.

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

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

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

[22] X. Kai, S. Zhu, On the distance of cyclic codes of length 2^e over Z_4, Discrete Math., **310** (2010), 12-20.

[23] L. Kathuria, M. Raka, Existence of cyclic self-orthogonal codes: A note on a result of Vera Pless, Adv. Math. Commun., **6**(2012), 499-503.

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

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

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

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

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

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

[30] 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.

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

[32] Z. Wan, Lectures on Finite Fields and Galois Rings, World Scientific Publishing, 2003.

[33] J. Wolfmann, Negacyclic and cyclic codes over Z_4, IEEE Trans. Inform. Theory, **7**(1999), 2527-2532.

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