A special class of repeated-root constacyclic codes

Abstract

Let $\mathbb{F}_q$ be a finite field with q elements where q be a prime power. Among the classes of constacyclic codes of length $5\ell p^s$ over $\mathbb{F}_q$ we define an equivalence relation such that the classes of constacyclic codes which have the same structure are viewed to be equivalent. In this paper we classify the classes of constacyclic codes of length 5ℓ and give the explicit generator polynomials of all the constacyclic codes and their dual codes.

Key Words. Cyclic codes, Constacyclic codes, Cyclotomic cosets, Finite fields

Mathematics Subject Classification (2000) 11T71, 94B15, 12Y05.

1 Introduction

Constacyclic codes were first introduced by Berlekamp in 1968 [3]. Repeated-root constacyclic codes were first introduced by [4] and [17]. In recent decades, Many authors have studied the repeated-root constacyclic codes. The length of a constacyclic codes is an important metric for a constacyclic codes, to determine the generator polynomials of all constacyclic codes of arbitrary length over finite fields is an important problem. Dinh [8, 9, 10, 11] has studied repeated-root constacyclic codes of lengths $2p^s$, $3p^s$, $4p^s$ and $6p^s$. In [7, 5], Chen et al. classify constacyclic codes over $\mathbb{F}_q$. Literature [1, 14, 15, 2] have investigated the structure of constacyclic codes of different lengths respectively. [16] give the explicit generator polynomials of all the constacyclic codes of length $p_1p_2^2p^s$ over $\mathbb{F}_q$ and their dual codes.

In this paper, We classify the classes of constacyclic codes of length $5\ell p^s$ over $\mathbb{F}_q$ into some equivalence classes and give the explicit generator polynomials for different equivalence classes.

This paper is organized as follows. In Section 2 we give a brief background on constacyclic codes over finite fields. In Section 3 we give the explicite q-cyclotomic cosets modulo 5ℓ. In Section 4 we we determine all the generators of such constacyclic codes by classify the classes of constacyclic codes of length 5ℓ.

2 Preliminaries

Let $\mathbb{F}_q$ be a q elements finite field where q is a power of a prime number p. Let ξ be a generator element of the cyclic group $\mathbb{F}_q^*$, i.e., $\mathbb{F}_q^* = \langle\xi\rangle$. First we introduce several classical results need in paper. The reader is referred to [12, 13] for more details on finite fields and cyclotomic polynomials.

Let p be a odd prime, and r be a primitive root of p. Assume that $(r+tp)^{p-1} \not\equiv 1 \pmod{p^2}$. Then for any $k \geq 1$, $r+tp$ is a primitive root of p^k.

Furthermore, let $n \geq 2$ and $k = ord(a)$, the multiplicative order of a module n. Let $a \in \mathbb{F}_q^*$ then $x^n - a$ is irreducible over $\mathbb{F}_q$ if and only iff for very prime divisor d of n, if $d|k$ then d not divides $\frac{q-1}{k}$, and if $4 \mid n$, then $4 \mid (q-1)$.

Let C be a linear code of length n, for any nonzero element $\lambda \in \mathbb{F}_q$, We call C is a λ-constacyclic if $(c_0, c_1, \cdots, c_{n-1}) \in C$ implies $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C$. We known λ-constacyclic code C of length n over $\mathbb{F}_q$ one-to-one correspondence the ideal $(g(x))$ of the quotient ring $\mathbb{F}_q[x]/(x^n - \lambda)$, where $g(x)|x^n - \lambda$. And, the dual code of code C is given by $C^\perp = \{x \in \mathbb{F}_q^n : x \cdot y = 0, \forall y \in C\}$, where $x \cdot y$ is the Euclidean inner product of x and y. If $g(x)$ is generator polynomials of cyclic code C, thent $g(x) \mid x^n - \lambda$, and define $h(x) = \dfrac{x^n - \lambda}{g(x)}$, then $h(x)$ is the parity check polynomial of cyclic code C. Thus the dual code $C^\perp$ is generated by $h(x)^* = h(0)^{-1} x^{deg(h(x))} h(\dfrac{1}{2})$. If $C \subseteq C^\perp$, then we called C a self-orthogonal, and if $C = C^\perp$ then we called C be a self-dual code. We known there exist a self-dual cyclic codes of length n over $\mathbb{F}_q$ if and only if 2 divide n and q.

For any positive integer n, let s be a positive integer little than $n-1$, that is $0 \leq s \leq n-1$, then the q-cyclotomic coset of s modulo n is defined by

$$C_s = \{s, sq, \cdots, sq^{n_s - 1}\},$$

where n_s is the multiplicative order of q modulo $\dfrac{n}{\gcd(s,n)}$, that is n_s is the least positive integer such that $sq^{n_s} \equiv s \pmod{n}$.

If β is a n-th primitive root of unit in some extension field of $\mathbb{F}_q$, then for any $0 < t < n$,

$$M_t(x) = \prod_{i \in C_t} (x - \beta^i)$$

is the minimal polynomial of β^t over $\mathbb{F}_q$, and

$$x^n - 1 = \prod M_t(x)$$

is the irreducible factorization of $x^n - 1$ over $\mathbb{F}_q$, where t runs over a complete set of q-cyclotomic cosets modulo n. By study the q-cyclotomic cosets modulo n, we can determine all the λ-constacyclic codes of length n over $\mathbb{F}_q$,

3 Explicit cyclotomic cosets modulo 5ℓ

It is a well-known result that when n is an odd prime with $\gcd(n, p) = 1$, then all the q cyclotomic cosets modulo n are $C_0 = \{0\}$ and $C_k = \{g^k, g^k q, \cdots, g^k q^{n_k - 1}\}$, for any $1 \leq k \leq e = \dfrac{\varphi(\ell)}{m}$, where φ is Euler's phi-function, $\mathbb{Z}_l^* = \langle g \rangle$, and $m = ord_n(q)$ is the multiplicative order of q in $\mathbb{Z}_n^*$.

Let $n = \ell$ be a odd prime. In this section, we provide all the q-cyclotomic cosets modulo 5ℓ so that we can give the factorization of $x^{5\ell} - 1$ over $\mathbb{F}_q$. First notice that if $f = ord_\ell(q)$, then we have that

(1) If $q \equiv 1 \pmod 5$ then $ord_{5\ell}(q) = f$, .

(2) If $q \equiv 4 \pmod 5$ and f even then $ord_{5\ell}(q) = f$.

(3) If $q \equiv 4 \pmod 5$ and f odd then $ord_{5\ell}(q) = 2f$.

(4) If $q \equiv 2$ or $q \equiv 3 \pmod 5$ and $4 \mid f$ then $ord_{5\ell}(q) = f$, .

(5) If $q \equiv 2$ or $q \equiv 3 \pmod 5$ and $2 \mid f$ but $4 \nmid f$ then $ord_{5\ell}(q) = 2f$.

(6) If $q \equiv 2$ or $q \equiv 3 \pmod 5$ and f odd then $ord_{5\ell}(q) = 4f$.

We claim that we can find a primitive root of unity r modulo ℓ satisfies $gcd(\frac{r^{\ell-1}-1}{\ell}, \ell) = 1$. To see that, we let r_1 to be any primitive root of unity modulo ℓ. If $\ell^2 \nmid r_1^{\ell-1} - 1$, we let $r = r_1$. Otherwise, we set $r = r_1 + \ell$, and it is easy to prove that r satisfies the above condition. Assume that $g = r + (1-r)\ell^4$, then we have that

$$g^{\ell-1} - 1 \equiv (r + (1-r)\ell^4)^{\ell-1} - 1 \equiv r^{\ell-1} - 1 \pmod{\ell^2}.$$

Therefore $\gcd(\frac{g^{\ell-1}-1}{\ell}, \ell) = \gcd(\frac{r^{\ell-1}-1}{\ell}, \ell) = 1$. For $r + tp$ is a primitive root of p^k, it follows immediately that g is a primitive root of unity modulo ℓ^t for all $t \geq 1$, and $g \equiv 1 \pmod 5$.

Lemma 1. **(1)** *When $q \equiv 1 \pmod 5$, the q cyclotomic cosets modulo 5ℓ can be written as $C_0 = \{0\}$, $C_\ell = \{\ell\}$, $C_{2\ell} = \{2\ell\}$, $C_{-\ell} = \{-\ell\}$, $C_{-2\ell} = \{-2\ell\}$, and $C_{ag^k} = \{ag^k, ag^kq, \cdots, ag^kq^{f-1}\}$ for $a \in R = \{1, 2, -1, -2, 5\}$ and $e - 1 \geq k \geq 0$.*

(2) *When f is even and $q \equiv 4 \pmod 5$, we can write all q-cyclotomic cosets modulo 5ℓ as $C_0 = \{0\}$, $C_\ell = \{\ell, \ell q\}$, $C_{2\ell} = \{2\ell, 2\ell q\}$, $C_{g^{k'}} = \{g^{k'}, g^{k'}q, \cdots, g^{k'}q^{f-1}\}$, $C_{2g^{k'}} = \{2g^{k'}, 2g^{k'}q, \cdots, 2g^{k'}q^{f-1}\}$ for $2e - 1 \geq k' \geq 0$, and $C_{5g^g} = \{5g^k, 5g^kq, \cdots, 5g^kq^{f-1}\}$ for $e - 1 \geq k \geq 0$.*

(3) *When f is odd and $q \equiv 4 \pmod 5$, we can write all q-cyclotomic cosets modulo 5ℓ as $C_0 = \{0\}$, $C_\ell = \{\ell, \ell q\}$, $C_{2\ell} = \{2\ell, 2\ell q\}$, $C_{g^k} = \{g^k, g^kq, \cdots, g^kq^{2f-1}\}$, $C_{2g^k} = \{2g^k, 2g^kq, \cdots, 2g^kq^{2f-1}\}$, and $C_{5g^k} = \{5g^k, 5g^kq, \cdots, 5g^kq^{f-1}\}$ for $e - 1 \geq k \geq 0$.*

(4) *When $4 \mid f$ and $q \equiv 2, 3 \pmod 5$, we can write all q-cyclotomic cosets modulo 5ℓ as $C_0 = \{0\}$, $C_\ell = \{\ell, \ell q, \ell q^2, \ell q^3\}$, $C_{g^{k'}} = \{g_{k'}, g^{k'}q, \cdots, g^{k'}q^{f-1}\}$ for $4e - 1 \geq k' \geq 0$, and $C_{5g^k} = \{5g^k, 5g^kq, \cdots, 5g^kq^{f-1}\}$ for $e - 1 \geq k \geq 0$.*

(5) *When $2 \mid f$ but $4 \nmid f$ and $q \equiv 2$ or $3 \pmod 5$, we can write all q-cyclotomic cosets modulo 5ℓ as $C_0 = \{0\}$, $C_\ell = \{\ell, \ell q, \ell q^2, lq^3\}$, $C_{g^{k'}} = \{g_{k'}, g^{k'}q, \cdots, g^{k'}q^{2f-1}\}$ for $2e - 1 \geq k' \geq 0$, and $C_{5g^k} = \{5g^k, 5g^kq, \cdots, 5g^kq^{f-1}\}$ for $e - 1 \geq k \geq 0$.*

(6) *When f is odd and $q \equiv 2, 3 \pmod 5$, we can write all q-cyclotomic cosets modulo 5ℓ as $C_0 = \{0\}$, $C_\ell = \{\ell, \ell q, \ell q^2, \ell q^3\}$, $C_{g^k} = \{g_k, g^kq, \cdots, g^kq^{4f-1}\}$, and $C_{5g^k} = \{5g^k, 5g^kq, \cdots, 5g^kq^{f-1}\}$ for $e - 1 \geq k \geq 0$.*

Proof. The methods for proving the above six cases are more or less the same, and we will take the second case as an example. First since $g \equiv 1 \pmod 5$ is a fixed primitive root of unity modulo l, it is easy to verify that C_0, C_ℓ, $C_{2\ell}$, $C_{g^{k'}}$, $C_{2g^{k'}}$ for $2e - 1 \geq k' \geq 0$ and C_{5g^k} for $e - 1 \geq k \geq 0$ are q-cyclotomic cosets modulo 5ℓ. We will then show that all these cosets are distinct.

Assume that a_1, a_2, k_1, k_2 and j satisfy the definitions in (2), if $a_1g^{k_1} \equiv a_2g^{k_2}q^j$, Since $gcd(a_1, 5\ell) = gcd(a_1g^{k_1}, 5\ell) = gcd(a_2g^{k_2}q^j, 5\ell) = gcd(a_2, 5\ell)$, therefore we have that $a_1 = a_2$ or $a_1 \neq a_2$, but in both cases a_1 and a_2 are not equal to 5. We split the proof into two subcases.

Subcase 1. $a_1 = a_2$. In this case, we have $g^{k_1-k_2} \equiv q^j \pmod \ell$ and $g^{(k_1-k_2)f} \equiv 1 \pmod \ell$, thus $\varphi(\ell) \mid (k_1 - k_2)f$, $\frac{\varphi(\ell)}{f} \mid (k_1 - k_2)$, this shows that $k_1 = k_2$.

Subcase 2. $a_1 \neq a_2$ and none of them is equal to 5, we have that $a_1a_2^{-1} \equiv g^{k_2-k_1}q^j \pmod{5\ell}$, but notice that $a_1a_2^{-1} \equiv \pm 2 \pmod 5$ and $g^{k_2-k_1}q^j \equiv \pm 1 \pmod 5$, It's a contradiction. Thus given that the q-cyclotomic are all distinct, we simply show that they are all q-cyclotomic cosets to complete the proof. Note that

$$|C_0| + |C_\ell| + |C_{2\ell}| + \sum_{k'=0}^{2e-1} |C_{g^{k'}}| + \sum_{k'=0}^{2e-1} |C_{2g^{k'}}| + \sum_{k=0}^{e-1} |C_{5g^k}| = 5 + 2ef + 2ef + ef = 5(ef+1) = 5(\varphi(\ell)+1) = 5\ell.$$

Thus the conclusion holds. □

It is a classical result that the q-cyclotomic cosets modulo n is related to the irreducible factorization of $x^n - 1$ over $\mathbb{F}_q$. Explicitly, Let F be an extension field of $\mathbb{F}_q$ and α be a primitive nth root of unity in F , then the minimal polynomial of α^s over $\mathbb{F}_q$ is

$$M_s(x) = \prod_{i \in C_s} (x - \alpha^i),$$

and

$$x^n - 1 = \prod M_s(x)$$

gives the factorization of the irreducible factorization $x^n - 1$ over $\mathbb{F}_q$, where s runs over a complete set of representatives from distinct q-cyclotomic coset modulo n.

Theorem 1. *The exact irreducible expression for $x^{5\ell} - 1$ over $\mathbb{F}_q$ can be given as follows*

(1) *Let $R = \{1, 2, 3, 4, 5\}$, then $x^{5\ell} - 1 = B_0(x)B_\ell(x)B_{2\ell}(x)B_{3\ell}(x)B_{4\ell}(x) \prod_{a \in R} \prod_{k=0}^{e-1} B_{ag^k}(x)$ for $q \equiv 1 \pmod 5$.*

(2) $x^{5\ell} - 1 = B_0(x)B_\ell(x)B_{2\ell}(x) \prod_{k'=0}^{2e-1} B_{g^{k'}}(x)B_{2g^{k'}}(x) \prod_{k=0}^{e-1} B_{5g^k}(x)$ *for $2|f$ and $q \equiv 4 \pmod 5$.*

(3) $x^{5\ell} - 1 = B_0(x)B_\ell(x)B_{2\ell}(x) \prod_{k=0}^{e-1} B_{g^k}(x)B_{2g^k}(x)B_{5g^k}(x)$ *for $2 \nmid f$ and $q \equiv 4 \pmod 5$.*

(4) $x^{5\ell} - 1 = B_0(x)B_\ell(x) \prod_{k'=0}^{4e-1} B_{g^{k'}}(x) \prod_{k=0}^{e-1} B_{5g^k}(x)$ *for $4 \mid f$ and $q \equiv 2$ or $3 \pmod 5$.*

(5) $x^{5\ell} - 1 = B_0(x)B_\ell(x) \prod_{k'=0}^{2e-1} B_{g^{k'}}(x) \prod_{k=0}^{e-1} B_{5g^k}(x)$ *for $2 \mid f$ but $4 \nmid f$ and $q \equiv 2$ or $3 \pmod 5$.*

(6) $x^{5\ell} - 1 = B_0(x)B_\ell(x) \prod_{k=0}^{e-1} B_{g^k}(x)B_{5g^k}(x)$ *for $2 \nmid f$ and $q \equiv 2$ or $3 \pmod 5$.*

4 Generator polynomials of constacyclic codes of length $5\ell p^s$ with their dual codes

In this section, we will determine the generator polynomials and their dual codes for all constacyclic codes of length $5\ell p^s$ on $\mathbb{F}_q$, where q is a power of p, ℓ is an odd prime number different from odd prime numbers p, and s is a positive integer.

Obviously, The class number of constacyclic codes of length n over $\mathbb{F}_q$ are $q - 1$. However, in these classes, in the sense that the algebraic structures are the same, many of them are equivalent. For $\lambda, \mu \in \mathbb{F}_q^*$, they are called n-equivalent if one of the four statements in the following lemma holds.

The following facts are taken from [5]. Let $\mathbb{F}_q$ be a finite fields, then for any $\lambda, \mu \in \mathbb{F}_q^*$, $\lambda^{-1}\mu \in \langle \xi^n \rangle$ if and only if $(\lambda^{-1}\mu)^d = 1$, where $d = \frac{q-1}{gcd(n,q-1)}$. Furthermore, they are equivalent to there exists an element $a \in \mathbb{F}_q*$ such that $a^n\lambda = \mu$, that is λ and μ are n-equivalent in $\mathbb{F}_q^*$. From $\mathbb{F}_q$-algebra isomorphism point of view, this is equivalent to there exists an $a \in \mathbb{F}_q^*$ such that

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

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

Based on the facts above, the value of $d = gcd(5\ell p^s, q - 1)$ has four cases, that is

$$d = 1, \quad 5\ell, \quad 5, \quad \ell.$$

4.1 For the case of $d = 1$

For $d = gcd(q-1, 5\ell p^s) = 1$, we have the following theorem.

Theorem 2. *Let $d = gcd(q-1, 5\ell p^s) = 1$, then for any $\lambda \in \mathbb{F}_q^*$, there is a unique $w \in \mathbb{F}_q^*$ such that $a^{5\ell p^s}\lambda = 1$. This shows that λ-constacyclic codes C of length $5\ell p^s$ over $\mathbb{F}_q$ are equivalent to the cyclic codes. In this context, the explicit irreducible factorization of $x^{5\ell p^s} - \lambda$ over $\mathbb{F}_q$ can be expressed in the following form*

(1) When $2|f$ and $q \equiv 4 \pmod 5$, we have

$$x^{5\ell p^s} - \lambda = \widehat{B}_{2\ell}(wx)^{p^s}\widehat{B}_{\ell}(wx)^{p^s}\widehat{B}_0(wx)^{p^s}\prod_{k'=0}^{2e-1}\widehat{B}_{g^{k'}}(wx)^{p^s}\widehat{B}_{2g^{k'}}(wx)^{p^s}\prod_{k=0}^{e-1}\widehat{B}_{5g^k}(wx)^{p^s},$$

Therefore, for λ-constacyclic codes C we have that

$$C = \left\langle \widehat{B}_{2\ell}(wx)^{\varepsilon_1}\widehat{B}_{\ell}(wx)^{\varepsilon_2}\widehat{B}_0(wx)^{\varepsilon_3}\prod_{k'=0}^{2e-1}\widehat{B}_{g^{k'}}(wx)^{\tau_{k'}}\widehat{B}_{2g^{k'}}(wx)^{\nu_{k'}}\prod_{k=0}^{e-1}\widehat{B}_{5g^k}(wx)^{\rho_k}\right\rangle,$$

and for the dual codes of C

$$\begin{aligned} C^{\perp} &= \Big\langle \widehat{B}_0(w^{-1}x)^{p^s-\varepsilon_1}\widehat{B}_{-\ell}(w^{-1}x)^{p^s-\varepsilon_2}\widehat{B}_{-2\ell}(w^{-1}x)^{p^s-\varepsilon_3} \\ &\quad \times \prod_{k'=0}^{2e-1}\widehat{B}_{-g^{k'}}(w^{-1}x)^{p^s-\tau_{k'}}\widehat{B}_{-2g^{k'}}(w^{-1}x)^{p^s-\nu_{k'}}\prod_{k=0}^{e-1}\widehat{B}_{-5g^k}(w^{-1}x)^{p^s-\rho_k}\Big\rangle, \end{aligned}$$

where $0 \le \varepsilon_1, \varepsilon_2, \varepsilon_3, \tau_{k'}, \nu_{k'}, \rho_k \le p^s$ for any $k \in \{0, 1, \cdots, e-1\}$ and $k^{'} \in \{0, 1, \cdots, 2e-1\}$.

(2) When $2 \nmid f$ and $q \equiv 4 \pmod 5$, we have

$$x^{5\ell p^s} - \lambda = \widehat{B}_{2\ell}(wx)^{p^s}\widehat{B}_{\ell}(wx)^{p^s}\widehat{B}_0(wx)^{p^s}\prod_{k=0}^{e-1}\widehat{B}_{g^k}(wx)^{p^s}\widehat{B}_{2g^k}(wx)^{p^s}\widehat{B}_{5g^k}(wx)^{p^s}.$$

Therefore, for λ-constacyclic codes C we have that

$$C = \left\langle \widehat{B}_0(wx)^{\varepsilon_1}\widehat{B}_{\ell}(wx)^{\varepsilon_2}\widehat{B}_{2\ell}(wx)^{\varepsilon_3}\prod_{k=0}^{e-1}\widehat{B}_{g^k}(wx)^{\tau_k}\widehat{B}_{2g^k}(wx)^{\nu_k}\widehat{B}_{5g^k}(wx)^{\rho_k}\right\rangle,$$

and for dual codes of C, we have

$$\begin{aligned} C^{\perp} &= \Big\langle \widehat{B}_0(w^{-1}x)^{p^s-\varepsilon_1}\widehat{B}_{-\ell}(w^{-1}x)^{p^s-\varepsilon_2}\widehat{B}_{-2\ell}(w^{-1}x)^{p^s-\varepsilon_3} \\ &\quad \times \prod_{k=0}^{e-1}\widehat{B}_{-g^k}(w^{-1}x)^{p^s-\tau_k}\widehat{B}_{-2g^k}(w^{-1}x)^{p^s-\nu_k}\widehat{B}_{-5g^k}(w^{-1}x)^{p^s-\rho_k}\Big\rangle, \end{aligned}$$

where $p^s \ge \varepsilon_1, \varepsilon_2, \varepsilon_3, \tau_k, \nu_k, \rho_k \ge 0$ and $k \in \{0, 1, \cdots, e-1\}$.

(3) When $4 \mid f$ and $q \equiv 2$ or $3 \pmod 5$, we have

$$x^{5\ell p^s} - \lambda = \widehat{B}_0(wx)^{p^s}\widehat{B}_{\ell}(wx)^{p^s}\prod_{k'=0}^{4e-1}\widehat{B}_{g^{k'}}(wx)^{p^s}\prod_{k=0}^{e-1}\widehat{B}_{5g^k}(wx)^{p^s}.$$

Therefore, for λ-constacyclic codes C we have that

$$C = \left\langle \widehat{B}_0(wx)^{\varepsilon_1} \widehat{B}_\ell(wx)^{\varepsilon_2} \prod_{k'=0}^{4e-1} \widehat{B}_{g^{k'}}(wx)^{\tau_{k'}} \prod_{k=0}^{e-1} \widehat{B}_{5g^k}(wx)^{\nu_k} \right\rangle,$$

and for dual codes of C, we have

$$C^\perp = \left\langle \widehat{B}_0(w^{-1}x)^{p^s-\varepsilon_1} \widehat{B}_{-\ell}(w^{-1}x)^{p^s-\varepsilon_2} \prod_{k'=0}^{4e-1} \widehat{B}_{-g^{k'}}(w^{-1}x)^{p^s-\tau_{k'}} \prod_{k=0}^{e-1} \widehat{B}_{-5g^k}(w^{-1}x)^{p^s-\nu_k} \right\rangle,$$

where $p^s \geq \varepsilon_1, \varepsilon_2, \tau_{k'}, \nu_k \geq 0$, for $k^{'} \in \{0, 1, \cdots, 4e-1\}$ and $k \in \{0, 1, \cdots, e-1\}$.

(4) When $2 \mid f$ but $4 \nmid f$ and $q \equiv 2$ or $3 \pmod 5$, we have

$$x^{5\ell p^s} - \lambda = \widehat{B}_0(wx)^{p^s} \widehat{B}_\ell(wx)^{p^s} \prod_{k'=0}^{2e-1} \widehat{B}_{g^{k'}}(wx)^{p^s} \prod_{k=0}^{e-1} \widehat{B}_{5g^k}(wx)^{p^s}.$$

Therefore, for λ-constacyclic codes C we have that

$$C = \left\langle \widehat{B}_0(wx)^{\varepsilon_1} \widehat{B}_\ell(wx)^{\varepsilon_2} \prod_{k'=0}^{2e-1} \widehat{B}_{g^{k'}}(wx)^{\tau_{k'}} \prod_{k=0}^{e-1} \widehat{B}_{5g^k}(wx)^{\nu_k} \right\rangle,$$

and for the dual codes of C

$$C^\perp = \left\langle \widehat{B}_0(w^{-1}x)^{p^s-\varepsilon_1} \widehat{B}_{-\ell}(w^{-1}x)^{p^s-\varepsilon_2} \prod_{k'=0}^{2e-1} \widehat{B}_{-g^{k'}}(w^{-1}x)^{p^s-\tau_{k'}} \prod_{k=0}^{e-1} \widehat{B}_{-5g^k}(w^{-1}x)^{p^s-\nu_k} \right\rangle,$$

where $p^s \geq \varepsilon_1, \varepsilon_2, \tau_{k'}, \nu_k \geq 0$, for $k^{'} \in \{0, 1, \cdots, 2e-1\}$ and $k \in \{0, 1, \cdots, e-1\}$.

(5) When f is odd and $q \equiv 2$ or $3 \pmod 5$, we have

$$x^{5\ell p^s} - \lambda = \widehat{B}_0(wx)^{p^s} \widehat{B}_\ell(wx)^{p^s} \prod_{k=0}^{e-1} \widehat{B}_{g^k}(wx)^{p^s} \widehat{B}_{5g^k}(wx)^{p^s}.$$

Therefore, for λ-constacyclic codes C we have that

$$C = \left\langle \widehat{B}_0(wx)^{\varepsilon_1} \widehat{B}_\ell(wx)^{\varepsilon_2} \prod_{k=0}^{e-1} \widehat{B}_{g^k}(wx)^{\tau_k} \widehat{B}_{5g^k}(wx)^{\nu_k} \right\rangle,$$

and for dual codes of C, we have

$$C^\perp = \left\langle \widehat{B}_0(w^{-1}x)^{p^s-\varepsilon_1} \widehat{B}_{-\ell}(w^{-1}x)^{p^s-\varepsilon_2} \prod_{k=0}^{e-1} \widehat{B}_{-g^k}(w^{-1}x)^{p^s-\tau_k} \widehat{B}_{-5g^k}(w^{-1}x)^{p^s-\nu_k} \right\rangle,$$

where $p^s \geq \varepsilon_1, \varepsilon_2, \tau_k, \nu_k \geq 0$, for $k \in \{0, 1, \cdots, e-1\}$.

Proof. The conclusion follows from Lemma 1 and Theorem 1 directly. □

4.2 Analysis

To discuss the other cases, we first prove a more general result.

Let p is a prime number, $q = p^k$, and $\mathbb{F}_q$ be a q elements finite field. Assume that $n = p^e p_1^{e_1} \cdots p_s^{e_s}$ be the prime factorization of n and $p_1^{e_1} \cdots p_s^{e_s} \mid q-1$, i.e., $e_i \leq v_{p_i}(q-1)$ for $1 \leq i \leq s$.

It is trivial to verify that

$$\mathbb{F}_q^* = \langle \xi \rangle = \langle \xi^{p_1^{e_1} \cdots p_s^{e_s}} \rangle \bigcup \langle \xi^{p_1^{e_1} \cdots p_s^{e_s}} \rangle \xi^{p^e} \bigcup \cdots \bigcup \langle \xi^{p_1^{e_1} \cdots p_s^{e_s}} \rangle \xi^{p^e (p_1^{e_1} \cdots p_s^{e_s} - 1)}.$$

For $\lambda \in \langle \xi^{p_1^{e_1} \cdots p_s^{e_s}} \rangle \xi^{j \cdot p^e}$, where $p_1^{e_1} \cdots p_s^{e_s} - 1 \geq j \geq 0$, there is an element $w \in \mathbb{F}_q^*$ such that $w^n \lambda = \xi^{j \cdot p^e}$. Note that we can write j as $j = y \cdot p_1^{v_1} \cdots p_s^{v_s}$, where $v_i = \min\{e_i, v_{p_i}(j)\}$. Then we have that

$$x^n - \xi^{j \cdot p^e} = (x^{p_1^{e_1} \cdots p_s^{e_s}} - \xi^{y \cdot p_1^{v_1} \cdots p_s^{v_s}})^{p^e} = \xi^{j \cdot p^e} ((\frac{x^{p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}}}{\xi^y})^{p_1^{v_1} \cdots p_s^{v_s}} - 1)^{p^e}.$$

Let $\delta = \xi^{\frac{q-1}{p_1^{v_1} \cdots p_s^{v_s}}}$ be a $p_1^{v_1} \cdots p_s^{v_s}$-th primitive root of unity, then

$$\begin{aligned} x^n - \xi^{j \cdot p^e} &= \xi^{j \cdot p^e} (\frac{x^{p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}}}{\xi^y} - 1)^{p^e} \cdot (\frac{x^{p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}}}{\xi^y} - \delta)^{p^e} \cdots (\frac{x^{p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}}}{\xi^y} - \delta^{p_1^{v_1} \cdots p_s^{v_s} - 1})^{p^e} \\ &= (x^{p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}} - \xi^y)^{p^e} (x^{p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}} - \delta \xi^y)^{p^e} \cdots (x^{p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}} - \delta^{p_1^{v_1} \cdots p_s^{v_s} - 1} \xi^y)^{p^e}. \end{aligned}$$

For $0 \leq i \leq p_1^{v_1} \cdots p_s^{v_s} - 1$, $\delta^i \xi^y = \xi^{y + i \cdot \frac{q-1}{p_1^{v_1} \cdots p_s^{v_s}}}$, therefore

$$ord(\delta^i \xi^y) = \frac{q-1}{gcd(q-1, y + i \cdot \frac{q-1}{p_1^{v_1} \cdots p_s^{v_s}})},$$

and

$$\frac{q-1}{ord(\delta^i \xi^y)} = gcd(q-1, y + i \cdot \frac{q-1}{p_1^{v_1} \cdots p_s^{v_s}}).$$

For each $p_i \mid p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}$, we have that $v_i = v_{p_i}(j)$ and $v_i < e_i$, hence $p_i \nmid y$. Since $v_i < e_i \leq v_{p_i}(q-1)$, $p_i \mid \frac{q-1}{p_1^{v_1} \cdots p_s^{v_s}}$, therefore $p_i \nmid y + i \cdot \frac{q-1}{p_1^{v_1} \cdots p_s^{v_s}}$ and $p_i \mid \frac{q-1}{y + i \cdot \frac{q-1}{p_1^{v_1} \cdots p_s^{v_s}}}$. Moreover if $4 \mid p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}$, then $4 \mid p_1^{e_1} \cdots p_s^{e_s} \mid q-1$. Thus, each $x^{p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}} - \xi^y \delta^i$ is irreducible over $\mathbb{F}_q$.

Based on the discussion above, we get the explicit factorization of $x^n - \lambda$ over $\mathbb{F}_q$.

Theorem 3. *Let $q = p^k$ where p is a prime, $\mathbb{F}_q$ be a q elements finite field. Assume that $n = p^e p_1^{e_1} \cdots p_s^{e_s}$ be the prime factorization of n and $p_1^{e_1} \cdots p_s^{e_s} \mid q-1$, i.e., $e_i \leq v_{p_i}(q-1)$ for $s \geq i \geq 1$. For any $\lambda \in \mathbb{F}_q^*$, there is an element $w \in \mathbb{F}_q^*$ such that $w^n \lambda = \xi^{j \cdot p^e}$, where $p_1^{e_1} \cdots p_s^{e_s} - 1 \geq j \geq 0$. If we write j as $j = y \cdot p_1^{v_1} \cdots p_s^{v_s}$, where $v_i = \min\{v_{p_i}(j), e_i\}$. Then*

$$\begin{aligned} x^n - \lambda &= (x^{p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}} - w^{-p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}} \xi^y)^{p^e} (x^{p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}} - w^{-p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}} \delta \xi^y)^{p^e} \cdot \\ &\quad \cdots (x^{p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}} - w^{-p_1^{e_1 - v_1} \cdots p_s^{e_s - v_s}} \delta^{p_1^{v_1} \cdots p_s^{v_s} - 1} \xi^y)^{p^e}. \end{aligned}$$

Now we turn to the case that $p_1^{e_1} \cdots p_s^{e_s} \nmid q-1$. Notice that $gcd(p_1^{e_1} \cdots p_s^{e_s}, q) = 1$, thus there is a least positive integer m satisfy $q^m \equiv 1 (mod p_1^{e_1} \cdots p_s^{e_s})$, i.e., $p_1^{e_1} \cdots p_s^{e_s} \mid q^m - 1$. By Lifting-the-exponent Lemma, when m' is the smallest positive integer with $p_1 \cdots p_s \mid q^{m'} - 1$, then $m = m' p_1^{d_1} \cdots p_s^{d_s}$, where $d_i = \max\{e_i - v_{p_i}(q^{m'} - 1), 0\}$. For any $\lambda \in \mathbb{F}_q^*$, we get the explicit irreducible factorization of $x^n - \lambda$ over $\mathbb{F}_q$, we first consider that over $\mathbb{F}_{q^m}$. Let $\mathbb{F}_{q^m}^* = \langle \zeta \rangle = \langle \zeta^{p_1^{e_1} \cdots p_s^{e_s}} \rangle \cup \langle \zeta^{p_1^{e_1} \cdots p_s^{e_s}} \rangle \zeta^{p^e} \cup \cdots \cup \langle \zeta^{p_1^{e_1} \cdots p_s^{e_s}} \rangle \zeta^{p^e (p_1^{e_1} \cdots p_s^{e_s} - 1)}$.

For any $\lambda \in \mathbb{F}_q^* \subseteq \mathbb{F}_{q^m}^*$, there is a $w \in \mathbb{F}_{q^m}^*$ such that $w^n\lambda = \zeta^{j\cdot p^e}$, where $p_1^{e_1}\cdots p_s^{e_s} - 1 \geq j \geq 0$. By the above conclusion, we have over $\mathbb{F}_{q^m}$

$$\begin{aligned} x^n - \lambda &= (x^{p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}} - w^{-p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}}\xi^y)^{p^e}(x^{p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}} - w^{-p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}}\delta\xi^y)^{p^e}\cdot \\ &\quad \cdots\cdot(x^{p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}} - w^{-p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}}\delta^{p_1^{v_1}\cdots p_s^{v_s}-1}\xi^y)^{p^e}, \end{aligned}$$

gives the explicit irreducible factorization of $x^n - \lambda$. Therefore, any irreducible factor of $x^n - \lambda$ over $\mathbb{F}_q$ has the form

$$\begin{aligned} &(x^{p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}} - w^{-p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}}\delta^i\xi^y)^{p^e}(x^{p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}} - w^{-qp_1^{e_1-v_1}\cdots p_s^{e_s-v_s}}\delta^{qi}\xi^{qy})^{p^e}\cdot \\ &\cdots\cdot(x^{p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}} - w^{-q^{z_i-1}p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}}\delta^{i\cdot q^{z_i-1}}\xi^{y\cdot q^{z_i-1}})^{p^e}, \end{aligned}$$

where z_i is the smallest positive integer satisfy $w^{-q^{z_i}p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}}\delta^{i\cdot q^{z_i}}\xi^{y\cdot q^{z_i}} = w^{-p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}}\delta^i\xi^y$. Now we use the above result to discuss the left three cases of constacyclic codes of length $5\ell p^s$.

4.3 For the case of $d = 5\ell$

For $d = gcd(q-1, 5\ell p^s) = 5\ell$, we have the following theorem.

Theorem 4. *Let $d = gcd(q-1, 5\ell p^s) = 5\ell$, then $\mathbb{F}_q^* = \langle\xi\rangle = \langle\xi^{5\ell}\rangle \cup \langle\xi^{5\ell}\rangle\xi^{p^s} \cup \cdots \cup \langle\xi^{5\ell}\rangle\xi^{p^s(5\ell-1)}$. Let $\lambda \in \mathbb{F}_q^*$, then there exists $w \in \mathbb{F}_q^*$ such that $w^{5\ell p^s}\lambda = \xi^{j\cdot p^s}$, where $5\ell - 1 \geq j \geq 0$. Then j can be written as $j = y\cdot 5^{v_1}\ell^{v_2}$, where $v_1 = \min\{v_5(j), 1\}$, $v_2 = \min\{v_\ell(j), 1\}$. Furthermore, we have*

$$\begin{aligned} x^{5\ell p^s} - \lambda &= (x^{5^{1-v_1}\ell^{1-v_2}} - w^{-5^{1-v_1}\ell^{1-v_2}}\xi^y)^{p^s}(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta\xi^y)^{p^s} \\ &\quad \cdots(x^{5^{1-v_1}\ell^{1-v_2}} - w^{-5^{1-v_1}\ell^{1-v_2}}\delta^{5^{v_1}\ell^{v_2}-1}\xi^y)^{p^s}. \end{aligned}$$

Moreover, for λ-constacyclic codes C we have that

$$\begin{aligned} C &= \Big\langle (x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\xi^y)^{\varepsilon_1}(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta\xi^y)^{\varepsilon_2} \\ &\quad \cdots(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta^{5^{v_1}\ell^{v_2}-1}\xi^y)^{\varepsilon_{5^{v_1}\ell^{v_2}}}\Big\rangle, \end{aligned}$$

and for dual codes of C, we have

$$\begin{aligned} C^\perp &= \Big\langle (x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}}\xi^{-y})^{p^s-\varepsilon_1}(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}}\delta^{-1}\xi^{-y})^{p^s-\varepsilon_2} \\ &\quad \cdots(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}}\delta^{1-5^{v_1}\ell^{v_2}}\xi^{-y})^{p^s-\varepsilon_{5^{v_1}\ell^{v_2}}}\Big\rangle, \end{aligned}$$

where $0 \leq \varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{5^{v_1}\ell^{v_2}} \leq p^s$.

4.4 For the case of $d = 5$

Remember that $f = ord_\ell(q)$ is the multiplicative order of q in $\mathbb{Z}_\ell^*$, hence $q^f \equiv 1(mod\ \ell)$. Since $5 \mid (q-1)$, thus f is the least positive integer satisfy $q^f \equiv 1 \pmod{5\ell}$. Obviously there exist a primitive element ζ in $\mathbb{F}_{q^f}^*$ satisfy $\xi = \zeta^{\frac{q^f-1}{q-1}} = \zeta^{1+q+\cdots+q^{f-1}}$. Then

$$\mathbb{F}_q^* = \langle\xi\rangle = \langle\xi^5\rangle \cup \langle\xi^5\rangle\xi^{p^s} \cup \cdots \cup \langle\xi^5\rangle\xi^{4p^s}$$

and

$$\mathbb{F}_{q^f}^* = \langle\zeta\rangle = \langle\zeta^{5\ell}\rangle \cup \langle\zeta^{5\ell}\rangle\zeta^{p^s} \cup \cdots \cup \langle\zeta^{5\ell}\rangle\zeta^{(5\ell-1)p^s}.$$

Since $\ell \mid (q^f-1)$ but $\ell \nmid (q-1)$, we have that $\ell \mid (1+q+\cdots+q^{f-1})$. Therefore $\xi^5 = \zeta^{5(1+q+\cdots+q^{f-1})} \in \langle\zeta^{5\ell}\rangle$, which indicates that $\langle\xi^5\rangle \subseteq \langle\zeta^{5\ell}\rangle$. Furthermore, for $0 \le j \le 4$, consider the following congruence equations

$$j' \equiv jf \pmod 5 \text{ and } j' \equiv 0 \pmod \ell.$$

By the Chinese remainder theorem, there is a unique solution up to modulo 5ℓ to the equations, and we denote the solution by j'. Then it is trivial to verify that $\xi^{j\cdot p^s} \in \langle\zeta^{5\ell}\rangle\zeta^{j'\cdot p^s}$. Hence we have the following theorem.

Theorem 5. *Let $d = gcd(5\ell p^s, q-1) = 5$, then for each $4 \ge j \ge 0$, there exist $w \in \mathbb{F}_{q^f}*$ satisfy $w^{5\ell p^s}\xi^{j\cdot p^s} = \zeta^{j'\cdot p^s}$. Furthermore, any irreducible factor of $x^{5\ell} - \xi^j$ over $\mathbb{F}_q$ has the form*

$$\begin{aligned}&(x^{5^{1-v_1}\ell^{1-v_2}} - w^{-5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'})(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{iq}\zeta^{y'q})\\ &\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - w^{-5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y'q^{z_i-1}}),\end{aligned}$$

where z_i is the smallest positive integer such that $w^{-q^{z_i}5^{1-v_1}\ell^{1-v_2}}\delta^{iq^{z_i}}\zeta^{y'q^{z_i}} = w^{5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'}$, and $j' = y'5^{v_1}\ell^{v_2}$, $v_1 = min\{v_5(j'), 1\}$, $v_2 = min\{v_\ell(j'), 1\}$.

For any $0 \le i, i' \le 5^{v_1}\ell^{v_2} - 1$, we define a equivalence relation $\sim$. For any i and j, $i \sim i' \Leftrightarrow w^{-q^m5^{1-v_1}\ell^{1-v_2}}\delta^{iq^m}\zeta^{y'q^m} = w^{5^{1-v_1}\ell^{1-v_2}}\delta^{i'}\zeta^{y'}$ for some integers $m \ge 0$. It is obvious to see that $\sim$ is an equivalence relation. For $\{0, 1, \cdots, 5^{v_1}\ell^{v_2} - 1\}$, let X be a complete equivalence class representatives to $\sim$. For each $i \in X$, we define the irreducible polynomial $M_i(x)$ as

$$\begin{aligned}&(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'})(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{iq}\zeta^{y'q})\\ &\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y'q^{z_i-1}}),\end{aligned}$$

and define $M_i^{'}(x)$ as

$$\begin{aligned}&(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}}\delta^{-i}\zeta^{-y'})(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{-iq}\zeta^{-y'q})\\ &\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{-iq^{z_i-1}}\zeta^{-y'q^{z_i-1}}),\end{aligned}$$

Then we can get the following theorem.

Theorem 6. *Let $d = gcd(5\ell p^s, q-1) = 5$. For each $4 \ge j \ge 0$, there is $w \in \mathbb{F}_{q^f}*$ satisfy $w^{5\ell p^s}\xi^{j\cdot p^s} = \zeta^{j'\cdot p^s}$. Then we can write the explicit irreducible factorization of $x^{5\ell p^s} - \xi^{jp^s}$ over $\mathbb{F}_q$ as*

$$x^{5\ell p^s} - \xi^{jp^s} = \prod_{i\in X} M_i(x)^{p^s}.$$

Moreover, for λ-constacyclic codes C we have that

$$C = \langle\prod_{i\in X} M_i(x)^{\varepsilon_i}\rangle,$$

and for dual codes of C, we have

$$C^\perp = \langle\prod_{i\in X} M_i^{'}(x)^{p^s-\varepsilon_i},$$

where $i \in X$ and $p^s \ge \varepsilon_i \ge 0$.

4.5 For the case of $d = \ell$

For $d = gcd(q-1, 5\ell p^s) = 5\ell$, we have the following theorem.

Theorem 7. *Let $d = gcd(5\ell p^s, q-1) = \ell$.*

(1) *When $q \equiv 4 \pmod 5$, for each $\ell - 1 \geq j \geq 0$, in the modulo 5ℓ sense, the system of equations*

$$j' \equiv 2j \pmod \ell \text{ and } j' \equiv 0 \pmod 5$$

there exist a unique solution j'. Furthermore, any irreducible factor of $x^{5\ell} - \xi^j$ has the form

$$(x^{5^{1-v_1}\ell^{1-v_2}} - w^{-5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'})(x^{5^{1-v_1}\ell^{1-v_2}} - w^{-5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{iq}\zeta^{y'q})$$
$$\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - w^{-5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y'q^{z_i-1}}),$$

where z_i is the smallest positive integer satisfy $w^{-q^{z_i}5^{1-v_1}\ell^{1-v_2}}\delta^{iq^{z_i}}\zeta^{y'q^{z_i}} = w^{5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'}$ and $j' = 5^{v_1}\ell^{v_2}y'$, $v_1 = \min\{v_5(j'), 1\}$, $v_2 = \min\{v_\ell(j'), 1\}$.

(2) *When $q \equiv 2, 3 \pmod 5$, for each $\ell - 1 \geq j \geq 0$, in the modulo 5ℓ sense, the system of equations*

$$j' \equiv 4j \pmod \ell$$

and

$$j' \equiv 0 \pmod 5$$

there exist a unique solution j'. Furthermore, any irreducible factor of $x^{5\ell} - \xi^j$ has the form

$$(x^{5^{1-v_1}\ell^{1-v_2}} - w^{-5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'})(x^{5^{1-v_1}\ell^{1-v_2}} - w^{-5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{iq}\zeta^{y'q})$$
$$\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - w^{-5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y'q^{z_i-1}}),$$

where z_i is the smallest positive integer satisfy $w^{-q^{z_i}5^{1-v_1}\ell^{1-v_2}}\delta^{iq^{z_i}}\zeta^{y'q^{z_i}} = w^{5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'}$, and $j' = y'5^{v_1}\ell^{v_2}$, $v_1 = \min\{v_5(j'), 1\}$, $v_2 = \min\{v_\ell(j'), 1\}$.

For any $0 \leq i, i' \leq 5^{v_1}\ell^{v_2} - 1$, we define equivalence relation $\sim$, for any i and $j \in \{0, 1, \cdots, 5^{v_1}\ell^{v_2} - 1\}$, $i \sim i' \Leftrightarrow w^{-q^m 5^{1-v_1}\ell^{1-v_2}}\delta^{iq^m}\zeta^{y'q^m} = w^{5^{1-v_1}\ell^{1-v_2}}\delta^{i'}\zeta^{y'}$ for some integer $m \geq 0$.

For $\{0, 1, \cdots, 5^{v_1}\ell^{v_2} - 1\}$, let X be a complete equivalence class representatives to $\sim$. For each $i \in X$, we define the irreducible polynomial $M_i(x)$ as

$$(x^{5^{1-v_1}\ell^{1-v_2}} - w^{-5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'})(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{iq}\zeta^{y'q})$$
$$\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - w^{-5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y'q^{z_i-1}}),$$

and define $M_i'(x)$ as

$$(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}}\delta^{-i}\zeta^{-y'})(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{-iq}\zeta^{-y'q})$$
$$\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{-iq^{z_i-1}}\zeta^{-y'q^{z_i-1}}).$$

Then we can get the following theorem.

Corollary 1. *Let $d = gcd(q-1, 5\ell p^s) = \ell$.*

(1) *When* $q \equiv 4 \pmod 5$*, and* $j, j^{'}$ *is defined as the above Theorem, we can write the explicit irreducible factorization of* $x^{5\ell p^s} - \xi^{jp^s}$ *over* $\mathbb{F}_q$ *as*

$$x^{5\ell p^s} - \xi^{jp^s} = \prod_{i \in X} M_i(x)^{p^s}.$$

Moreover, for λ*-constacyclic codes* C *we have that*

$$C = \langle \prod_{i \in X} M_i(x)^{\varepsilon_i} \rangle,$$

and for dual codes of C*, we have*

$$C^{\perp} = \langle \prod_{i \in X} M_i^{'}(x)^{p^s - \varepsilon_i},$$

where $i \in X$ *and* $p^s \geq \varepsilon_i \geq 0$*.*

(2) *When* $q \equiv 2, 3 \pmod 5$*, we can write the explicit irreducible factorization of* $x^{5\ell p^s} - \xi^{jp^s}$ *over* $\mathbb{F}_q$ *as*

$$x^{5\ell p^s} - \xi^{jp^s} = \prod_{i \in X} M_i(x)^{p^s}.$$

Moreover, for λ*-constacyclic codes* C *we have that*

$$C = \langle \prod_{i \in X} M_i(x)^{\varepsilon_i} \rangle,$$

and for dual codes of C*, we have*

$$C^{\perp} = \langle \prod_{i \in X} M_i^{'}(x)^{p^s - \varepsilon_i} \rangle,$$

where $i \in X$ *and* $p^s \geq \varepsilon_i \geq 0$*.*

Disclaimer (Artificial Intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT,COPILOT, etc) and text-to-image generators have been used during writing or editing of manuscripts.

Acknowledgement

The authors are grateful to the teacher who guided the writing and the anonymous referees for theirs usefulcomments which allow me to improve the manuscript.

Competing Interests

Author has declared that no competing interests exist.

References

[1] G.K. Bakshi, M. Raka, A class of constacyclic codes over a finite field, Finite Fields Appl. 18(2) (2012) 362-377.

[2] A. Batoul, K. Guenda, T. Aaron Gulliver, On repeated-root constacyclic codes of length $2^a mp^r$ over finite field, arXiv:1505.00356v1, 2015.

[3] E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill Book Company, New York, 1968.

[4] G. Castagnoli, J.L. Massey, On Repeated-Root Cyclic Codes. IEEE Trans. Inform. Theory, vol.37, No.2, Mar. 1991.

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

[6] B. Chen, H.Q. Dinh, H. Liu, Repeated-root constacyclic codes of length $\ell^m p^n$, Finite Fields Appl. 33, 137-159, 2015.

[7] B. Chen, Y. Fan, L. Lin, H. Liu, Constacyclic codes over finite fields, Finite Fields Appl. 18(6), 1217-1231, 2012.

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

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

[10] H.Q. Dinh, On repeated-root constacyclic codes of length $4p^s$. Asian-European J. Math. 6(2), 2013.

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

[12] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, fifth edition, Clarendon Press, Oxford, 1984, Ch. 16.

[13] R. Lidl and H. Niederreiter, Finite Fields, in Encyclopedia of Mathematics and Its Application, 2nd edn., vol 20, Cambridge University Press, Cambridge, 1997.

[14] A. Sharma, Repeated-root constacyclic codes of length $\ell^t p^s$ and their dual codes, Cryptogr. Commun. 7(2), 229-255, 2015.

[15] A. Sharma, S. Rani, Repeated-root constacyclic codes of length $4\ell^m p^n$, Finite Fields Appl., 40, 163-200, 2016.

[16] H. Wu, L. Zhu, Repeated-root constacyclic codes of length $p_1 p_2^t p^s$ and their duals, AIMS Math. 8 (6) (2023) 12793–12818.

[17] J.H. Van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory, 37(2), 343-345, Apr. 1991.