Repaeted-root constacyclic codes of length $5\ell p^s$

Abstract

Let q be a prime power and let $\mathbb{F}_q$ be a finite field with q elements. 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

As generalizition of cyclic codes and negacyclic codes, constacyclic codes were first introduced by Berlekamp in 1968 [3]. Given a nonzero element λ of finite filed $\mathbb{F}_q$, 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 $(c_0, c_1, \cdots, c_{n-1}) \in C$. Constacyclic codes over finite fields are a remarkable class of linear codes. The class of constacyclic codes includes the class of cyclic codes and the class of negacyclic codes as proper subclasses. Constacyclic codes have rich algebraic structure so that they can be efficiently encoded and decoded by means of shift registers. Repeated-root constacyclic codes were a special class of constacyclic codes. Repeated-root constacyclic codes were first studied by Castagnoli et al [16] and van Lint [15], where they showed that repeated-root cyclic codes have a concatenated construction and are not asymptotically good.

Recently, repeated-root constacyclic codes have been studied by many authors. To determine the generator polynomials of all constacyclic codes of arbitary length over finite fields is an important problem. Dinh studied repeated-root constacyclic codes of lengths $2p^s$, $3p^s$, $4p^s$ and $6p^s$ in a series of papers [7, 8, 9, 10]. He determined the algebraic structure of these repeated-root constacyclic codes over finite fields in terms of their generator polynomials. In [6], Chen et al. introduced an equivalence relation called isometry for the nonzero elements of $\mathbb{F}_q$ to classify constacyclic codes of length n over $\mathbb{F}_q$. They have the same distance structures and the same algebraic structures for belonging to the same equivalence classes induced by isometry. Furthermore, in [4], Chen et al. considered a more specified relationship than isometry that enabled us to obtain more explicit description of generator polynomials of all constacyclic codes. According to the equivalence classes, all constacyclic codes of length ℓp^s over $\mathbb{F}_{q^m}$ and their duals are characterized, where ℓ is a prime different from p and s is a positive integer. Recently, Chen et al. [5] determined the algebraic structure of all constacyclic codes of length $2\ell^t p^s$ over $\mathbb{F}_{p^r}$ and their dual codes in terms of their generator polynomials, where ℓ, p are distinct odd primes and s, t, r are positive integers. In 2012, Bakshi and Raka [1] also determined all Λ-constacyclic codes of length $2^t p^s (t \geq 1, s \geq 0$ are integers) over $\mathbb{F}_{p^r}$ using different methods from Chen et al.. Sharma [13] determined all constacyclic codes of length $\ell^t p^s$ over $\mathbb{F}_{p^r}$ and their dual codes, where ℓ, p are distinct

primes, ℓ is odd and s, t, r are positive integers. In another recent work, Sharma et al. [14], they determine generator polynomials of all constacyclic codes of length $4\ell^m p^n$ over the finite field $\mathbb{F}_q$, where p, ℓ are distinct odd primes, q is a power of p and m, n are positive integers. They also determine their dual codes, and list all self-dual constacyclic codes of length $4\ell^m p^n$ over $\mathbb{F}_q$. Batoul et al. [2] investigated the structure of constacyclic codes of length $2^a mp^r$ over $\mathbb{F}_{p^s}$ with $a \geq 1$ and $(m, p) = 1$. They also provided certain sufficient conditions under which these codes are equivalent to cyclic codes of length $2^a mp^r$ over $\mathbb{F}_{p^s}$.

In this paper, we determine all the constacyclic codes of length $5\ell p^s$ over $\mathbb{F}_q$. Obviously, there are $q-1$ classes of constacyclic codes of length n over $\mathbb{F}_q$, however, many of them are turned out to be equivalent in the sense that they have the same structure. We first classify the classes of constacyclic codes into some equivalence classes, then according to these equivalence classes we give all the explicit generator polynomials of all the constacyclic codes of length $5\ell p^s$ over $\mathbb{F}_q$.

The remainder of this paper is organized as follows. In Section 2 we give a brief background on some basic results of constacyclic codes over finite fields, and we give all the q-cyclotomic cosets modulo 5ℓ explicitly in section 3. In Section 4 we classify the classes of constacyclic codes of length 5ℓ, and according to this we determine all the generators of such constacyclic codes.

2 Preliminaries

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime number p, and 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 of number theory and finite fields which we need in the following parts. The reader is referred to [11, 12] for more details on finite fields and cyclotomic polynomials.

Lemma 1. *Assume that r is a primitive root of the odd prime p and $(r+tp)^{p-1}$ is not congruent to 1 modulo p^2. Then $r+tp$ is a primitive root of p^k for each $k \geq 1$.*

Lemma 2. *Suppose that $n \geq 2$, and let $k = ord(a)$ be the multiplicative order of a. Then for any $a \in \mathbb{F}_q^*$, the binomial $x^n - a$ is irreducible over $\mathbb{F}_q$ if and only if*

(1) *Every prime divisor of n divides k, but not $\frac{q-1}{k}$;*

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

For any nonzero element $\lambda \in \mathbb{F}_q$, a linear code C of length n is called λ-constacyclic if $(c_0, c_1, \cdots, c_{n-1}) \in C$ implies $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C$. A λ-constacyclic code C of length n over $\mathbb{F}_q$ can be regarded as an ideal $(g(x))$ of the quotient ring $\mathbb{F}_q[x]/(x^n - \lambda)$, where $g(x)$ is a divisor of $x^n - \lambda$. Let C be a λ-constacyclic code of length n over $\mathbb{F}_q$, then 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 $x \cdot y$ denotes the Euclidean inner product of x and y. If C is generated by a polynomial $g(x)$ which satisfies that $g(x) \mid x^n - \lambda$, and $h(x)$ is given by $h(x) = \dfrac{x^n - \lambda}{g(x)}$, then $h(x)$ is called the parity check polynomial of code C. It is a classical result that the dual code $C^\perp$ is generated by $h(x)^*$, where $h(x)^* = h(0)^{-1} x^{deg(h(x))} h(\frac{1}{2})$ is the reciprocal polynomial of $h(x)$. The code C is called to be a self-orthogonal if $C \subseteq C^\perp$ and a self-dual code if $C = C^\perp$. For self-dual cyclic code, a well-known result states that there exist self-dual cyclic codes of length n over $\mathbb{F}_q$ if and only if n is even and the characteristic of $\mathbb{F}_q$ is $p = 2$.

Let n be any positive integer. For any integer s, $0 \leq s \leq n-1$, the definition of q-cyclotomic coset of s modulo n is given by

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

where n_s is the least positive integer such that $sq^{n_s} \equiv s \pmod{n}$. Then it is easy to see that n_s is equal to the multiplicative order of q modulo $\frac{n}{\gcd(s,n)}$. If α is a primitive nth root of unit in some extension field of $\mathbb{F}_q$, then the polynomial $M_s(x) = \prod_{i \in C_s}(x - \alpha^i)$ is the minimal polynomial of α^s over $\mathbb{F}_q$, and

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

gives the irreducible factorization of $x^n - 1$ over $\mathbb{F}_q$, where s runs over a complete set of representations from distinct q-cyclotomic cosets modulo n. Therefore to determine all the λ-constacyclic codes of length n over $\mathbb{F}_q$, we need to consider the q-cyclotomic cosets modulo n.

3 q-cyclotomic cosets modulo 5ℓ

It is a well-known result that when $n = \ell$ is an odd prime with $\gcd(\ell, p) = 1$, all the distinct q-cyclotomic cosets modulo ℓ are $C_0 = \{0\}$ and $C_k = \{g^k, g^k q, \cdots, g^k q^{n_k - 1}\}$, for any integer k, $1 \leq k \leq e = \frac{\varphi(\ell)}{f}$, where g is a fixed generator of the cyclic group $\mathbb{Z}_l^*$, $f = ord_\ell(q)$ is the multiplicative order of q in $\mathbb{Z}_\ell^*$, and φ is Euler's phi-function.

In this section, we determine 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) $ord_{5\ell}(q) = f$, when $q \equiv 1 \pmod{5}$.

(2) $ord_{5\ell}(q) = f$, when $q \equiv 4 \pmod{5}$ with f even.

(3) $ord_{5\ell}(q) = 2f$, when $q \equiv 4 \pmod{5}$ with f odd.

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

(5) $ord_{5\ell}(q) = 2f$, when $q \equiv 2$ or $q \equiv 3 \pmod{5}$ with $2 \mid f$ but $4 \nmid f$.

(6) $ord_{5\ell}(q) = 4f$, when $q \equiv 2$ or $q \equiv 3 \pmod{5}$ with f odd.

We claim that there exists a primitive root r modulo ℓ such that $gcd(\frac{r^{\ell-1} - 1}{\ell}, \ell) = 1$. To see that, we let r_1 to be any primitive root 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 trivial to verify that r satisfies the 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 $\gcd(\frac{g^{\ell-1} - 1}{\ell}, \ell) = \gcd(\frac{r^{\ell-1} - 1}{\ell}, \ell) = 1$. By Lemma 1, it follows immediately that g is a primitive root modulo ℓ^t for all $t \geq 1$ such that $g \equiv 1 \pmod{5}$. Now we give all the distinct q-cyclotomic cosets modulo 5ℓ.

Lemma 3. (1) *If $q \equiv 1 \pmod{5}$, then we have that all the distinct q-cyclotomic cosets modulo 5ℓ are given by $B_0 = \{0\}$, $B_\ell = \{\ell\}$, $B_{2\ell} = \{2\ell\}$, $B_{-\ell} = \{-\ell\}$, $B_{-2\ell} = \{-2\ell\}$, and $B_{ag^k} = \{ag^k, ag^k q, \cdots, ag^k q^{f-1}\}$ for $a \in R = \{1, 2, -1, -2, 5\}$ and $0 \leq k \leq e - 1$.*

(2) *If $q \equiv 4 \pmod{5}$ and f is even, we have that all the distinct q-cyclotomic cosets modulo 5ℓ are given by $B_0 = \{0\}$, $B_\ell = \{\ell, \ell q\}$, $B_{2\ell} = \{2\ell, 2\ell q\}$, $B_{g^{k'}} = \{g^{k'}, g^{k'} q, \cdots, g^{k'} q^{f-1}\}$, $B_{2g^{k'}} = \{2g^{k'}, 2g^{k'} q, \cdots, 2g^{k'} q^{f-1}\}$ for $0 \leq k' \leq 2e - 1$, and $B_{5g^g} = \{5g^k, 5g^k q, \cdots, 5g^k q^{f-1}\}$ for $0 \leq k \leq e - 1$.*

(3) *If $q \equiv 4 \pmod{5}$ and f is odd, we have that all the distinct q-cyclotomic cosets modulo 5ℓ are given by $B_0 = \{0\}$, $B_\ell = \{\ell, \ell q\}$, $B_{2\ell} = \{2\ell, 2\ell q\}$, $B_{g^k} = \{g^k, g^k q, \cdots, g^k q^{2f-1}\}$, $B_{2g^k} = \{2g^k, 2g^k q, \cdots, 2g^k q^{2f-1}\}$, and $B_{5g^k} = \{5g^k, 5g^k q, \cdots, 5g^k q^{f-1}\}$ for $0 \leq k \leq e - 1$.*

(4) *If $q \equiv 2$ or $3 \pmod 5$ and $4 \mid f$, we have that all the distinct q-cyclotomic cosets modulo 5ℓ are given by $B_0 = \{0\}$, $B_\ell = \{\ell, \ell q, \ell q^2, \ell q^3\}$, $B_{g^{k'}} = \{g_{k'}, g^{k'}q, \cdots, g^{k'}q^{f-1}\}$ for $0 \le k' \le 4e-1$, and $B_{5g^k} = \{5g^k, 5g^k q, \cdots, 5g^k q^{f-1}\}$ for $0 \le k \le e-1$.*

(5) *If $q \equiv 2$ or $3 \pmod 5$ and $2 \mid f$ but $4 \nmid f$, we have that all the distinct q-cyclotomic cosets modulo 5ℓ are given by $B_0 = \{0\}$, $B_\ell = \{\ell, \ell q, \ell q^2, lq^3\}$, $B_{g^{k'}} = \{g_{k'}, g^{k'}q, \cdots, g^{k'}q^{2f-1}\}$ for $0 \le k' \le 2e-1$, and $B_{5g^k} = \{5g^k, 5g^k q, \cdots, 5g^k q^{f-1}\}$ for $0 \le k \le e-1$.*

(6) *If $q \equiv 2$ or $3 \pmod 5$ and f is odd, we have that all the distinct q-cyclotomic cosets modulo 5ℓ are given by $B_0 = \{0\}$, $B_\ell = \{\ell, \ell q, \ell q^2, \ell q^3\}$, $B_{g^k} = \{g_k, g^k q, \cdots, g^k q^{4f-1}\}$, and $B_{5g^k} = \{5g^k, 5g^k q, \cdots, 5g^k q^{f-1}\}$ for $0 \le k \le e-1$.*

Proof. The methods to prove the above 6 situations are similar, and we will give the proof of the second situation as a instance. First since g is a fixed primitive root modulo l such that $g \equiv 1 \pmod 5$, it is trivial to verify that B_0, B_ℓ, $B_{2\ell}$, $B_{g^{k'}}$, $B_{2g^{k'}}$ for $0 \le k' \le 2e-1$ and B_{5g^k} for $0 \le k \le e-1$ are q-cyclotomic cosets modulo 5ℓ. And then we will show that all these cosets are all distinct. If we have that $a_1 g^{k_1} \equiv a_2 g^{k_2} q^j$, where a_1, a_2, k_1, k_2 and j satisfy the definitions in (2). Since $gcd(a_1, 5\ell) = gcd(a_1 g^{k_1}, 5\ell) = gcd(a_2 g^{k_2} q^j, 5\ell) = gcd(a_2, 5\ell)$, we have that either $a_1 = a_2$ or $a_1 \ne a_2$ and both a_1 and a_2 are not equal to 5. We divide the proof into 2 subcases.

Subcase 1. If $a_1 = a_2$, we have that $g^{k_1-k_2} \equiv q^j \pmod \ell$ and $g^{(k_1-k_2)f} \equiv 1 \pmod \ell$, therefore $\varphi(\ell) \mid (k_1-k_2)f$ and $\dfrac{\varphi(\ell)}{f} \mid (k_1-k_2)$, which indicates that $k_1 = k_2$.

Subcase 2. If $a_1 \ne a_2$ and none of them is equal to 5, we have that $a_1 a_2^{-1} \equiv g^{k_2-k_1} q^j \pmod{5\ell}$, but notice that $a_1 a_2^{-1} \equiv \pm 2 \pmod 5$ and $g^{k_2-k_1} q^j \equiv \pm 1 \pmod 5$, which is a contradiction. Hence the given cosets are all distinct, and we only need to prove they are all the q-cyclotomic cosets to complete the proof. Notice that

$$|B_0|+|B_\ell|+|B_{2\ell}|+\sum_{k'=0}^{2e-1}|B_{g^{k'}}|+\sum_{k'=0}^{2e-1}|B_{2g^{k'}}|+\sum_{k=0}^{e-1}|B_{5g^k}| = 5+2ef+2ef+ef = 5(ef+1) = 5(\varphi(\ell)+1) = 5\ell.$$

Therefore the conclusion holds. □

It is a classical result that the irreducible factorization of x^n-1 over $\mathbb{F}_q$ is related to the q-cyclotomic cosets modulo n. Explicitly, if α denotes a primitive nth root of unity in some extension field of $\mathbb{F}_q$, then the polynomial $M_s(x) = \prod_{i \in C_s}(x-\alpha^i)$ is the minimal polynomial of α^s over $\mathbb{F}_q$, and

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

gives the factorization of x^n-1 into irreducible factor over $\mathbb{F}_q$, where s runs over a complete set of representatives from distinct q-cyclotomic coset modulo n. From Lemma 4 we get the irreducible factorization of $x^{5\ell}-1$ over $\mathbb{F}_q$.

Theorem 1. *The irreducible factorization of $x^{5\ell}-1$ over $\mathbb{F}_q$ is given as follows.*

(1) *If $q \equiv 1 \pmod 5$, then*

$$x^{5\ell}-1 = B_0(x)B_\ell(x)B_{2\ell}(x)B_{3\ell}(x)B_{4\ell}(x)\prod_{a\in R}\prod_{k=0}^{e-1}B_{ag^k}(x),$$

where $R = 1, 2, 3, 4, 5$.

(2) *If* $q \equiv 4 \pmod 5$ *and* f *is even, then*

$$x^{5\ell} - 1 = B_0(x)B_\ell(x)B_{2\ell}(x) \prod_{k'=0}^{2e-1} B_{g^{k'}}(x)B_{2g^{k'}}(x) \prod_{k=0}^{e-1} B_{5g^k}(x),$$

(3) *If* $q \equiv 4 \pmod 5$ *and* f *is odd, then*

$$x^{5\ell} - 1 = B_0(x)B_\ell(x)B_{2\ell}(x) \prod_{k=0}^{e-1} B_{g^k}(x)B_{2g^k}(x)B_{5g^k}(x),$$

(4) *If* $q \equiv 2$ *or* $3 \pmod 5$ *and* $4 \mid f$*, then*

$$x^{5\ell} - 1 = B_0(x)B_\ell(x) \prod_{k'=0}^{4e-1} B_{g^{k'}}(x) \prod_{k=0}^{e-1} B_{5g^k}(x),$$

(5) *If* $q \equiv 2$ *or* $3 \pmod 5$ *and* $2 \mid f$ *but* $4 \nmid f$*, then*

$$x^{5\ell} - 1 = B_0(x)B_\ell(x) \prod_{k'=0}^{2e-1} B_{g^{k'}}(x) \prod_{k=0}^{e-1} B_{5g^k}(x),$$

(6) *If* $q \equiv 2$ *or* $3 \pmod 5$ *and* f *is odd, then*

$$x^{5\ell} - 1 = B_0(x)B_\ell(x) \prod_{k=0}^{e-1} B_{g^k}(x)B_{5g^k}(x),$$

4 Constacyclic codes of length $5\ell p^s$ with their dual codes

In this section, we will determine generator polynomials of all constacyclic codes of length $5\ell p^s$ over $\mathbb{F}_q$ and their dual codes, where ℓ, p are distinct odd primes, q is a power of p and s is a positive integers.

Obviously, there are $q-1$ classes of constacyclic codes of length n over $\mathbb{F}_q$, however, many of them are turned out to be equivalent in the sense that they have the same structure. For $\lambda, \mu \in \mathbb{F}_q^*$, they are called n-equivalent if one of the four statements in the following lemma holds.

Lemma 4. *([4]) For any* $\lambda, \mu \in \mathbb{F}_q^*$*, the following four statements are equivalent:*

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

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

(3) λ *and* μ *are* n*-equivalent in* $\mathbb{F}_q^*$*, namely there exists an element* $a \in \mathbb{F}_q*$ *such that* $a^n\lambda = \mu$.

(4) *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* $gcd(n, q-1)$.

By Lemma 4, the value of d has the following four cases.

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

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

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

(4) $d = gcd(5\ell p^s, q-1) = l$.

4.1 $d = 1$

Theorem 2. *Assume that $d = gcd(q-1, 5\ell p^s) = 1$, then λ-constacyclic codes C of length $5\ell p^s$ over $\mathbb{F}_q$ are equivalent to the cyclic codes, i.e., for any $\lambda \in \mathbb{F}_q^*$, there exists a unique element $a \in \mathbb{F}_q^*$ such that $a^{5\ell p^s}\lambda = 1$. Furthermore, the irreducible factorization of $x^{5\ell p^s} - \lambda$ over $\mathbb{F}_q$ is given by*

(1) If $q \equiv 4 \pmod 5$ and f is even, then

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

Therefore we have that

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

and

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

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

(2) If $q \equiv 4 \pmod 5$ and f is odd, then

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

Therefore we have that

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

and

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

where $0 \le \varepsilon_1, \varepsilon_2, \varepsilon_3, \tau_k, \nu_k, \rho_k \le p^s$, for $k = 0, 1, \cdots, e-1$.

(3) If $q \equiv 2$ or $3 \pmod 5$ and $4 \mid f$, then

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

Therefore we have that

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

and

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

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

(4) If $q\equiv 2$ *or* $3 \pmod 5$ *and* $2\mid f$ *but* $4\nmid f$, *then*

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

Therefore we have that

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

and

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

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

(5) If $q\equiv 2$ *or* $3 \pmod 5$ *and* f *is odd, then*

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

Therefore we have that

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

and

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

where $0\leq\varepsilon_1,\varepsilon_2,\tau_k,\nu_k\leq p^s$, *for* $k=0,1,\cdots,e-1$.

Proof. The conclusion follows from Lemma 3 and Theorem 1 directly. □

4.2 Analysis

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

Let $\mathbb{F}_q$ be a finite field with q elements, where $q=p^k$ and p is a prime number. 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., $v_{p_i}(q-1)\geq e_i$ 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 $0 \le j \le p_1^{e_1}\cdots p_s^{e_s} - 1$, there exists an element $a \in \mathbb{F}_q^*$ such that $a^n\lambda = \xi^{j\cdot p^e}$. Notice that j can be written as $j = y \cdot p_1^{v_1}\cdots p_s^{v_s}$, where $v_i = mine_i, v_{p_i}(j)$. 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 primitive $p_1^{v_1}\cdots p_s^{v_s}$-th 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 $0 \le i \le p_1^{v_1}\cdots p_s^{v_s} - 1$, $\delta^i\xi^y = \xi^{y+i\cdot\frac{q-1}{p_1^{v_1}\cdots p_s^{v_s}}}$, 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 $e_i > v_i$ and $v_i = v_{p_i}(j)$, thus $p_i \nmid y$. Since $v_{p_i}(q-1) \ge e_i > v_i$, $p_i \mid \frac{q-1}{p_1^{v_1}\cdots p_s^{v_s}}$, which indicates that $p_i \nmid y + i\cdot\frac{q-1}{p_1^{v_1}\cdots p_s^{v_s}}$ 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 $4 \mid p_1^{e_1}\cdots p_s^{e_s} \mid q-1$. Hence by Lemma 2 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 above discussion, we get the following result on the factorization of $x^n - \lambda$ over $\mathbb{F}_q$.

Theorem 3. *Let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^k$ and p is a prime number. 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., $v_{p_i}(q-1) \ge e_i$ for $1 \le i \le s$. For any $\lambda \in \mathbb{F}_q^*$, there exists an element $a \in \mathbb{F}_q^*$ such that $a^n\lambda = \xi^{j\cdot p^e}$, where $0 \le j \le p_1^{e_1}\cdots p_s^{e_s} - 1$. If we 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*

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

gives the irreducible factorization of $x^n - \lambda$ over $\mathbb{F}_q$.

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 exists a least positive integer m such that $q^m \equiv 1 (mod p_1^{e_1}\cdots p_s^{e_s})$, i.e., $p_1^{e_1}\cdots p_s^{e_s} \mid q^m - 1$. By Lifting-the-exponent Lemma, if m' is the least positive integer such that $p_1\cdots p_s \mid q^{m'} - 1$, 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 $\lambda \in \mathbb{F}_q^*$, to obtain the 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 exists an element $a \in \mathbb{F}_{q^m}^*$ such that $a^n\lambda = \zeta^{j\cdot p^e}$, where $0 \le j \le p_1^{e_1}\cdots p_s^{e_s} - 1$. By the above conclusion, we have over $\mathbb{F}_{q^m}$

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

gives the irreducible factorization of $x^n-\lambda$. Hence each irreducible factor of $x^n-\lambda$ over $\mathbb{F}_q$ is of the form

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

where z_i is the least positive integer such that $a^{-q^{z_i}p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}}\delta^{i\cdot q^{z_i}}\xi^{y\cdot q^{z_i}}=a^{-p_1^{e_1-v_1}\cdots p_s^{e_s-v_s}}\delta^i\xi^y$.

Now we use the above result to discuss the left three cases of constacyclic codes of length $5\ell p^s$.

4.3 $d=5\ell$

Theorem 4. *Assume that $d=\gcd(q-1,5\ell p^s)=5\ell$, then $\mathbb{F}_q^*=\langle\xi\rangle=\langle\xi^{5\ell}\rangle\cup\langle\xi^{5\ell}\rangle\xi^{p^s}\cup\cdots\cup\langle\xi^{5\ell}\rangle\xi^{p^s(5\ell-1)}$. For any $\lambda\in\mathbb{F}_q^*$, there exists an element $a\in\mathbb{F}_q^*$ such that $a^{5\ell p^s}\lambda=\xi^{j\cdot p^s}$, where $0\le j\le 5\ell-1$. Then j can be written as $j=y\cdot 5^{v_1}\ell^{v_2}$, where $v_1=\min\{1,v_5(j)\}$ and $v_2=\min\{1,v_\ell(j)\}$. And*

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

gives the irreducible factorization of $x^{5\ell p^s}-\lambda$ over $\mathbb{F}_q$. Moreover, all the λ-constacyclic codes of length $5lp^s$ and their dual codes are given by

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

and

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

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

4.4 $d=5$

Remember that we denote the multiplicative order of q in $\mathbb{Z}^*$ by $f=ord_\ell(q)$. Then it is clear that f is the least positive integer such that $q^f\equiv 1(mod l)$. Since $5\mid(q-1)$, f is also the least positive integer such that $q^f\equiv 1\pmod{5\ell}$. Obviously we can find a primitive element ζ in $\mathbb{F}_{q^f}^*$ such that $\xi=\zeta^{\frac{q^f-1}{q-1}}=\zeta^{1+q+\cdots+q^{f-1}}$. 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 exists 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 get the following theorem.

Theorem 5. *Assume that $d = gcd(q-1, 5\ell p^s) = 5$, then for any $0 \le j \le 4$, there exists an element $a \in \mathbb{F}_{q^f}*$ such that $a^{5\ell p^s}\xi^{j\cdot p^s} = \zeta^{j'\cdot p^s}$. Moreover, each irreducible factor of $x^{5\ell} - \xi^j$ over $\mathbb{F}_q$ is of the form*

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

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

For any $0 \le i, i^{'} \le 5^{v_1}\ell^{v_2} - 1$, we define a relation $\sim$ to be such that $i \sim i^{'}$ if and only if $a^{-q^m5^{1-v_1}\ell^{1-v_2}}\delta^{iq^m}\zeta^{y'q^m} = a^{5^{1-v_1}\ell^{1-v_2}}\delta^{i^{'}}\zeta^{y'}$ for some nonnegative integers m. It is obvious to see that $\sim$ is an equivalence relation. Assume that X is a complete system of equivalence class representatives of $\{0, 1, \cdots, 5^{v_1}\ell^{v_2} - 1\}$ relative to this relation $\sim$. For any $i \in X$ we denote the irreducible polynomial

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

by $M_i(x)$, and denote

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

by $M_i^{'}(x)$. Then we have the following corollary.

Corollary 1. *Assume that $d = gcd(q-1, 5\ell p^s) = 5$. For any $0 \le j \le 4$, there exists an element $a \in \mathbb{F}_{q^f}*$ such that $a^{5\ell p^s}\xi^{j\cdot p^s} = \zeta^{j'\cdot p^s}$. Then*

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

gives the irreducible factorization of $x^{5\ell p^s} - \xi^{jp^s}$ over $\mathbb{F}_q$. Furthermore we have that

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

and

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

where $0 \le \varepsilon_i \le p^s$, for $i \in X$.

4.5 $d = \ell$

Theorem 6. *Assume that $d = gcd(q-1, 5\ell p^s) = \ell$, then*

(1) *If $q \equiv 4 \pmod 5$, for any $0 \le j \le \ell - 1$, the following equations*

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

have a unique solution j' up to modulo 5ℓ. Moreover, each irreducible facotor of $x^{5\ell}-\xi^j$ over $\mathbb{F}_q$ is of the form

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

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

(2) *If $q\equiv 2,3 \pmod 5$, for any $0\le j\le \ell-1$, the following equations*

$$j'\equiv 4j \pmod \ell$$
$$j'\equiv 0 \pmod 5$$

have a unique solution j' up to modulo 5ℓ. Moreover, each irreducible facotor of $x^{5\ell}-\xi^j$ over $\mathbb{F}_q$ is of the form

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

where $j'=y'5^{v_1}\ell^{v_2}$, $v_1=min1,v_5(j')$, $v_2=min1,v_\ell(j')$, and z_i is the least positive integer such that $a^{-q^{z_i}5^{1-v_1}\ell^{1-v_2}}\delta^{iq^{z_i}}\zeta^{y'q^{z_i}}=a^{5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'}$.

For any $0\le i,i^{'}\le 5^{v_1}\ell^{v_2}-1$, we define a relation $\sim$ to be such that $i\sim i^{'}$ if and only if $a^{-q^m5^{1-v_1}\ell^{1-v_2}}\delta^{iq^m}\zeta^{y'q^m}=a^{5^{1-v_1}\ell^{1-v_2}}\delta^{i^{'}}\zeta^{y'}$ for some nonnegative integer m. It is obvious to see that $\sim$ is an equivalence relation. Assume that X is a complete system of equivalence class representatives of $\{0,1,\cdots,5^{v_1}\ell^{v_2}-1\}$ relative to this relation $\sim$. For any $i\in X$ we denote the irreducible polynomial

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

by $M_i(x)$, and denote

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

by $M_i^{'}(x)$.

Corollary 2. *Assume that $d=gcd(q-1,5\ell p^s)=\ell$, then*

(1) *If $q\equiv 4 \pmod 5$, and $j,j^{'}$ is defined as in the first case of Theorem 6, then*

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

gives the irreducible factorization of $x^{5\ell p^s}-\xi^{jp^s}$ over $\mathbb{F}_q$. Furthermore we have that

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

and

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

where $0 \leq \varepsilon_i \leq p^s$, *for* $i \in X$.

(2) *If* $q \equiv 2, 3 \pmod 5$, *and* $j, j^{'}$ *is defined as in the second case of Theorem 6, then*

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

gives the irreducible factorization of $x^{5\ell p^s} - \xi^{jp^s}$ *over* $\mathbb{F}_q$. *Furthermore we have that*

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

and

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

where $0 \leq \varepsilon_i \leq p^s$, *for* $i \in X$.

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.

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] 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.

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

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

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

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

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

[10] 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.

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

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

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

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

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

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