Repeated-root constacyclic codes of length $3lp^s$ and their dual codes *

LiuLi, LiLanqiang

Department of Mathematics, Hefei University of Technology, Hefei 230009, Anhui, P.R.China

Abstract: Let $p \neq 3$ be any prime and $l \neq 3$ be any odd prime with $gcd(p, l) = 1$. $F_q^* = \langle \xi \rangle$ is decomposed into mutually disjoint union of $gcd(q-1, 3lp^s)$ coset over the subgroup $\langle \xi^{3lp^s} \rangle$, where ξ is a primitive $(q-1)$th root of unity. We classify all repeated-root constacyclic codes of length $3lp^s$ over the finite field F_q into some equivalence classes by the decomposition, where $q = p^m$, s and m are positive integers. According to the equivalence classes, we explicitly determine the generator polynomials of all repeated-root constacyclic codes of length $3lp^s$ over F_q and their dual codes. Self-dual cyclic(negacyclic) codes of length $3lp^s$ over F_q exist only when $p = 2$. And we give all self-dual cyclic(negacyclic) codes of length $3l2^s$over F_{2^m} and its enumeration.

Keywords: Repeated-root constacyclic codes, Cyclic(negacyclic) codes, Dual codes, Generator polynomial.

1 Introduction

Constacyclic codes over finite fields play a very important role in the theory of error-correcting codes. More important, constacyclic codes have practical applications. As these codes have rich algebraic structures, so that they can be efficiently encoded and decoded using shift registers. They also have very good error-correcting properties. All of those explain their preferred role in engineering.

Repeated-root cyclic codes were first investigated in the most generality in the 1990s by Castagnoli in[1] and Van Lint in[2]. In their papers, they proved that repeated-root cyclic have a concatenated construction, and are asymptotically bad. But we know that there still exists a few optimal such codes by $[12-14]$, which encourage many scholars to study the class of codes. For example, Dinh determined the generator polynomials of all constacyclic codes and their dual codes over F_q, of length $2p^s, 3p^s$ and $6p^s$, in $[3-5]$. Since then, these results have been extended to more general code lengths. In 2012, G.K. Bakshi and M. Raka give the generator polynomials of all constacyclic codes of length $2^t p^s$ over F_q in [6], where q is a power of an odd prime P. In 2014, B. Chen, H.Q. Dinh and H. Liu study all constacyclic codes of length lp^s over F_q in [7], where l is a prime different from p. In [7], all constacyclic codes of length lp^s over F_q and their dual codes are obtained. And given all self-dual and all linear complementary dual constacyclic codes. In resent, in [8], Anuradha Sharma explicitly determine the generator polynomials of all repeated-root constacyclic codes of length $l^t p^s$ over F_{p^m} and their dual codes. Further, they listed all self-dual cyclic and negacyclic codes and also determine all self-orthogonal cyclic and negacyclic codes of length $l^t p^s$ over F_{p^m}. What's more, B. Chen, H.Q. Dinh and H. Liu studied all constacyclic codes of length $2l^m p^s$ over F_q of characteristic p in [9]. And they given the characterization and enumeration of all linear complementary dual and self-dual constacyclic codes of length $2l^m p^s$ over F_q. In the conclusion of their paper, they said that it would be interesting to study all constacyclic codes of length $kl^m p^s$ over F_q, where p is the characteristic of F_q, l is an odd prime different from p and k is a prime different from l and p. However, this is very hard to work. In this paper, we study all

* E-mail addresses: liuli-1128@163.com(LiuLi), lilanqiang716@126.com(LiLanqiang).
This research is supported by the National Natural Science Foundation of China (No.11201107,No.11401154).

constacyclic codes of length $3lp^s$ over F_q, where $p \neq 3$ is any prime and $l \neq 3$ is any odd prime with $gcd(p, l) = 1$, which is helpful to study all constacyclic codes of more generate lengths for us.

In this paper, we decompose the multiplicative cyclic group $F_q^* = \langle \xi \rangle$ into mutually disjoint union of coset of $\langle \xi^{3lp^s} \rangle$, which are one-to-one correspondence to the equivalence classes of all constacyclic in section 3. Based on the decomposition, we explicitly determine the generator polynomials of all $\lambda-$constacyclic codes of length $3lp^s$ over F_q and their dual codes in section 4, where λ is any none-zero element of F_q and $q = p^m$ is a power of prime. As an application, we also give all self-dual cyclic(negacyclic) codes of length $3l2^s$ over F_{2^m} and its enumeration in section 5.

2 Preliminaries

Let F_q be the finite field of order q, where $q = p^m$, $p \neq 3$ is a prime and the characteristic of the field, m is a positive integer. Let $F_q^* = \langle \xi \rangle$ is the multiplicative cyclic group of none-zero elements of F_q, where ξ is a primitive $(q-1)$th root of unity.

For any element $\lambda \in F_q^*$, $\lambda-$constacyclic codes of length n over F_q are regarded as the ideals $\langle g(x) \rangle$ of the quotient ring $F_q[x]/(x^n - \lambda)$, where $g(x)|x^n - \lambda$. Further, the definition of the dual code of code C as follows,

$$C^{\perp} = \{x \in F_q^n | x \cdot y = 0, \forall y \in C\},$$

where $x \cdot y$ denotes the Euclidean inner product of x and y in F_q^n. The code C is called to be self-orthogonal code if $C \subseteq C^{\perp}$ and self-dual code if $C = C^{\perp}$. Let C be a $\lambda-$constacyclic code of length n over F_q is generated by a polynomial $g(x)$, i.e $C = \langle g(x) \rangle$. As $g(x)|x^n - \lambda$, then there exists a polynomial $h(x) \in F_q[x]$ such that $h(x) = \frac{x^n - \lambda}{g(x)}$. It's clear that $h(x)$ is also monic if $g(x)$ is monic. The polynomial $h(x)$ is said the parity check polynomial of code C. And it's well known that the dual code $C^{\perp}$ is generated by $h(x)^*$, where $h(x)^*$ is the reciprocal polynomial of $h(x)$. For any $f(x) \in F_q[x]$, the reciprocal polynomial of $f(x)$ is defined as $f(x)^* = f(0)^{-1} x^{deg(f(x))} f(\frac{1}{x})$. It's obvious that $(f_1 f_2)^* = f_1^* f_2^*$, and $(f_1^*)^* = f_1$, for any polynomials $f_1(x), f_2(x) \in F_q[x]$.

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 as follows:

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

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

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

gives the factorization of $(x^n - 1)$ into irreducible factors over F_q, where s runs over a complete set of representatives from distinct $q-$cyclotomic coset modulo n.

Obviously, when $n = l$, where $l \neq 3$ is an odd prime with $gcd(l, p) = 1$, we get that all the distinct $q-$cyclotomic coset modulo l are $C_0 = \{0\}$ and $C_k = \{g^k, g^k q, ..., g^k q^{n_k - 1}\}$, for any integer k, $1 \leq k \leq e = \frac{\phi(l)}{f}$, by $[15, Theory1]$, where g is a fixed generator of the cyclic group Z_l^*, $f = ord_l(q)$ is the multiplicative order of q in Z_l^*, and ϕ is Euler's phi-function. Therefor, we have that the irreducible factorization of $x^l - 1$ in F_q is given by

$$x^l - 1 = M_0(x) M_1(x) M_2(x) ... M_e(x),$$

where $M_i(x) = \prod_{j \in C_i}(x - \eta^i)$ with η is a primitive lth root of unity.

Further, we determine all the distinct q^3-cyclotomic coset modulo l, which is needed to prove our main results. There exists two subcases. when $gac(f,3) = 1$, it's easy to prove that $f = ord_l(q) = ord_l(q^3)$, then $\langle q \rangle = \langle q^3 \rangle$ in Z_l^*. According to the definition of q^3-cyclotomic coset modulo l, we have that C_0 and C_k, $1 \leq k \leq e = \frac{\phi(l)}{f}$, are also all of the distinct q^3-cyclotomic coset modulo l. When $gac(f,3) = 3$, we prove that $ord_l(q^3) = \frac{f}{3}$. It's easy to verify that $A_0 = \{0\}$,

$$A_k = \{g^k, g^k q^3, ..., g^k q^{3(\frac{f}{3}-1)}\},$$
$$A_{kq} = \{g^k q, g^k q q^3, ..., g^k q q^{3(\frac{f}{3}-1)}\},$$
$$A_{kq^2} = \{g^k q^2, g^k q^2 q^3, ..., g^k q^2 q^{3(\frac{f}{3}-1)}\},$$

consist of all the distinct q^3-cyclotomic coset modulo l, where $1 \leq k \leq e$,. Then, we have the irreducible factorization of $x^l - 1$ in $F_{q^3}[x]$ as follow:

$$x^l - 1 = A_0(x)A_1(x)A_q(x)A_{q^2}(X)A_2(x)A_{2q}(x)A_{2q^2}(x)...A_e(x)A_{eq}(x)A_{eq^2}(X),$$

where $A_0(x) = (x-1)$, $A_k(x) = \prod_{s \in A_k}(x - \eta^s)$, $A_{kq}(x) = \prod_{t \in A_{kq}}(x - \eta^t)$ and $A_{kq^2} = \prod_{j \in A_{kq^2}}(x - \eta^j)$, $1 \leq k \leq e$.

What's more, we also give all the distinct $q-$cyclotomic coset modulo $3l$, which is necessary to determine our main results. As $gac(q,3) = 1$, we have $q^{\phi(3)} \equiv 1(mod 3)$ by Euler's Theory, i.e. $q^2 \equiv 1(mod 3)$. Then, it's simple to verify that

$$ord_{3l} = \begin{cases} f, & q \equiv 1(mod 3); \\ f, & q \equiv 2(mod 3) with f even; \\ 2f, & q \equiv 2(mod 3) with f odd. \end{cases}$$

From $[16, Chapter 8]$, there exists a primitive root r modulo l such that $gcd(\frac{r^{l-1}-1}{l}, l) = 1$. Assume that $g = r + (1-r)l^2$, we have $g^{l-1} - 1 \equiv (r + (1-r)l^2)^{l-1} - 1 \equiv r^{l-1} - 1(mod l^2)$. Therefore, $gcd(\frac{g^{l-1}-1}{l}, l) = gcd(\frac{r^{l-1}-1}{l}, l) = 1$. It's clear that g is a primitive root modulo l^t, $1 \leq t$, such that $g \equiv 1(mod 3)$.

We give all the distinct $q-$cyclotomic coset modulo $3l$ by the following lemma.

Lemma 2.1. (I) If $q \equiv 1(mod 3)$, then, we have that all the distinct $q-$cyclotomic coset modulo $3l$ are given by

$$B_0 = \{0\}, B_l = \{l\}, B_{-l} = \{-l\},$$
$$B_{ag^k} = \{ag^k, ag^k q, ..., ag^k q^{f-1}\},$$

for $a \in R = \{1, -1, 3\}$ and $0 \leq k \leq e-1$.
(II) If $q \equiv 2(mod 3)$ and f is even, we have that all the distinct $q-$cyclotomic coset modulo $3l$ are given by $B_0 = \{0\}, B_l = \{l, lq\}$,

$$B_{g^{k'}} = \{g^{k'}, g^{k'} q, ..., g^{k'} q^{f-1}\}, for 0 \leq k' \leq 2e-1,$$
$$B_{3g^k} = \{3g^k, 3g^k q, ..., 3g^k q^{f-1}\}, for 0 \leq k \leq e-1.$$

(III) If $q \equiv 2(mod 3)$ and f is odd, we have that all the distinct $q-$cyclotomic coset modulo $3l$ are given by

$$B_0 = \{0\}, B_l = \{l, lq\},$$

$$B_{g^k} = \{g^k, g^k q, ..., g^k q^{2f-1}\},$$
$$B_{3g^k} = \{3g^k, 3g^k q, ..., 3g^k q^{f-1}\},$$

for $0 \leq k \leq e-1$.

Proof. $[I]$ Firstly, we prove that the cyclotomic coset $B_{ag^k}, 0 \leq k \leq e-1$, are distinct. If there exist some k_1, k_2, $0 \leq k_1, k_2 \leq e-1$, such that $B_{ag^{k_1}} = B_{ag^{k_2}}$, then we have

$$a_1 g^{k_1} \equiv a_2 g^{k_2} q^j (mod 3l),$$

for some integer j, where $a_1, a_2 \in R = \{1, -1, 3\}$. Therefor, we get

$$gcd(a_1 g^{k_1}, 3l) = gcd(a_2 g^{k_2} q^j, 3l) = gcd(a_2 g^{k_2}, 3l).$$

From this, we can deduce $a_1 = a_2$ or $a_1 = -a_2 = \pm 1$.
If $a_1 = -a_2 = \pm 1$, then

$$-g^{k_1} \equiv g^{k_2} q^j (mod 3l), i.e. -1 \equiv g^{k_1 - k_2} q^j mod(3l),$$

for some integer j. Due to $g \equiv 1(mod 3)$ and $q \equiv 1(mod 3)$, we deduce $-1 \equiv 1(mod 3)$. This is a contradiction.
If $a_1 = a_2$, assume that $a_1 = a_2 = a$, then we have

$$ag^{k_1} \equiv ag^{k_2} q^j (mod 3l), i.e. g^{k_1 - k_2} \equiv q^j (mod l),$$

for some integer j. Further, we have $g^{(k_1-k_2)f} \equiv q^{jf} \equiv 1(mod l)$. As g is a primitive root modulo l, we get $\phi(l) | (k_1 - k_2)f$, i.e. $e = \frac{\phi(l)}{f} | k_1 - k_2$. Since $0 \leq k_1, k_2 \leq e-1$, we must have $k_1 = k_2$. Secondly, we get

$$\begin{aligned} |B_0| + |B_l| + |B_{-l}| + \sum_{a \in R} \sum_{k=0}^{e-1} |B_{ag^k}| &= 3 + \sum_{a \in R} \sum_{k=0}^{e-1} f \\ &= 3 + \sum_{a \in R} ef \\ &= 3 + 3\phi(l) \\ &= 3l. \end{aligned}$$

So, the conclusion (I) holds. The conclusions (II) and (III) are also established in a similar way.

Assume that $B_o(x), B_l(x), B_{-l}(x)$ and $B_{ag^k}(x)$ are the minimal polynomials of the corresponding coset B_o, B_l, B_{-l} and B_{ag^k}. From the above lemma, we get the following theory immediately.

Theory 2.2. The irreducible factorization of $x^{3l} - 1$ over F_q as follows:
(I) If $q \equiv 1(mod 3)$, then

$$x^{3l} - 1 = B_0(x) B_l(x) B_{-l}(x) \prod_{a \in R} \prod_{k=0}^{e-1} B_{ag^k}(x),$$

where $a \in R = \{1, -1, 3\}$ and $0 \leq k \leq e-1$.
(II) If $q \equiv 2(mod 3)$ and f is even, then

$$x^{3l} - 1 = B_0(x)B_l(x) \prod_{k'=0}^{2e-1} B_{g^{k'}}(x) \prod_{k=0}^{e-1} B_{3g^k}(x),$$

where $0 \leq k \leq e-1, 0 \leq k^{'} \leq 2e-1$.
(III) If $q \equiv 2(mod 3)$ and f is odd, then

$$x^{3l} - 1 = B_0(x)B_l(x) \prod_{k=0}^{e-1} B_{g^k}(x) \prod_{k=0}^{e-1} B_{3g^k}(x),$$

where $0 \leq k \leq e-1$.

The next two lemmas give the necessary and sufficient conditions for judging the reducibility of binomials and trinomial, which were given by Wan Z in [17].

Lemma 2.3. Suppose that $n \geq 2$, Let $k = ord(a)$ be the multiplicative order of a, for any $a \in F_q^*$. Then, the binomial $x^n - a$ is irreducible over F_q if and only if
(i) Every prime divisor of n divides k, but does not divide $\frac{(q-1)}{k}$;
(ii) If $4|n$, then $4|(q-1)$.

Lemma 2.4. Let t be a positive integer, and $H(x) \in F_q[x]$ be irreducible over F_q with $deg(H(x)) = n$, x does not divide $H(x)$. and e denote the order of any root of $H(x)$. Then $H(x^t)$ is irreducible over F_q if and only if
(i) Each prime divisor of t divides e;
(ii) $gcd(t, \frac{q^n-1}{e}) = 1$;
(iii) If $4|t$, then $4|(q^n-1)$.

3 A classification of constacyclic codes of length $3lp^s$

Let ξ be a primitive $(q-1)$th root of unity and $F_q^* = \langle \xi \rangle$ be a cyclic group of order $(q-1)$ as before. It's easy to verify that $\langle \xi^{3lp^s} \rangle = \langle \xi^{3l} \rangle = \langle \xi^d \rangle$ and the index $|F_q^* : \langle \xi^{3lp^s} \rangle| = d$, where $d = gcd(q-1, 3lp^s)$. Thus, the multiplicative cyclic group F_q^* can be decomposed into mutually disjoint union of coset over the subgroup $\langle \xi^{3lp^s} \rangle$ as follows:

Lemma 3.1. $F_q^* = \langle \xi \rangle = \langle \xi^d \rangle \bigcup \xi^{p^s} \langle \xi^d \rangle \bigcup ... \bigcup \xi^{p^s(d-1)} \langle \xi^d \rangle$, where d is the great common divisor of $q-1$ and $3lp^s$.

According to the properties of the coset, we obtain the following lemma immediately.

Lemma 3.2. For any two none-zero elements λ and μ of F_q, there exists some integer j,$0 \leq j \leq d-1$ such that $\lambda, \mu \in \xi^{jp^s} \langle \xi^d \rangle$ if and only if $\lambda^{-1}\mu \in \langle \xi^d \rangle$, where $d = gcd(q-1, 3lp^s)$.

If λ and μ in the same coset, we build a one-to-one correspondence between $\lambda-$constacyclic code and $\mu-$constacyclic code of length $3lp^s$ over F_q as following theory, which shows that $\lambda-$constacyclic code and $\mu-$constacyclic code are equivalent.

Theorem 3.3. Let λ and μ be any two elements of F_q^*. then there exists some integer $a \in F_q^*$ such that

$$\begin{aligned}&\varphi : F_q[x]/(x^{3lp^s} - \mu) \to F_q[x]/(x^{3lp^s} - \lambda)\\ &f(x) \mapsto f(ax)\end{aligned}$$

is an isomorphism, if and only if $\lambda, \mu \in \xi^{jp^s}\langle \xi^d \rangle$, where $0 \le j \le d-1$

Proof." $\Longrightarrow$ " If φ is an isomorphism, then we have

$$\mu = \varphi(\mu) = \varphi(x^{3lp^s}) = (\varphi(x))^{3lp^s} = (ax)^{3lp^s} = a^{3lp^s}x^{3lp^s} = a^{3lp^s}\lambda$$

i.e. $\lambda^{-1}\mu = a^{3lp^s}$.
As $a = \xi^k \in F_q^*$, for some positive integer k, then $\lambda^{-1}\mu = \xi^{k\cdot 3lp^s} \in \langle \xi^d \rangle$. By Lemma 3.2, we get that there exists j, $0 \le j \le d-1$, such that $\lambda, \mu \in \xi^{jp^s}\langle \xi^d \rangle$.
" $\Longleftarrow$ " If there exists j, $0 \le j \le d-1$, such that $\lambda, \mu \in \xi^{jp^s}\langle \xi^d \rangle$, then we have $\lambda^{-1}\mu \in \langle \xi^d \rangle = \langle \xi^{3lp^s} \rangle$ by Lemma 3.2 again. Thus, $\lambda^{-1}\mu = \xi^{k\cdot 3lp^s}$, for some integer k. Set $a = \xi^k$, then $\lambda a^{3lp^s} = \mu$. Further, we can easy prove that the following map is an isomorphism:

$$\begin{aligned}&\varphi : F_q[x]/(x^{3lp^s} - \mu) \to F_q[x]/(x^{3lp^s} - \lambda)\\ &f(x) \mapsto f(ax).\end{aligned}$$

From Theory 3.3, we get the following obvious corollaries.

Corollary 3.4. For any two elements λ and μ of F_q^*, $\lambda-$constacyclic code is equivalent to $\mu-$constacyclic code if and only if there exists j, $0 \le j \le d-1$, such that $\lambda, \mu \in \xi^{jp^s}\langle \xi^d \rangle$, Further, $\lambda-$constacyclic code and $\mu-$constacyclic code are both equivalent to $\xi^{jp^s}-$constacyclic code.

Corollary 3.5. Let λ be any element of F_q^*, then there exists some integer j, $0 \le j \le d-1$, such that $\lambda-$constacyclic code is equivalent to $\xi^{jp^s}-$constacyclic code.

Obviously, the Theory 3.3 and its two corollaries show that all constacyclic codes of length $3lp^s$ over F_q are classified into $d = gcd(q-1, 3lp^s)$ mutually disjoint classes. And it's enough to consider $\lambda-$constacyclic codes, where $\lambda = \xi^{jp^s}$, $0 \le j \le d-1$, and $d = gcd(q-1, 3lp^s)$, if we want to determine all constacyclic codes of length $3lp^s$ over F_q. Therefore, we mainly study $\lambda-$constacyclic codes in the section 4.

4 All constacyclic codes of length $3lp^s$ over F_q

Let $f(x)$ be any polynomial of $F_q[x]$ and leading coefficient $a_n \neq 0$, we denote $\widehat{f}(x) = a_n^{-1}f(x)$. Then, $\widehat{f}(x)$ is called to be the monic polynomial of $f(x)$.

From the above discussion in the section 3, we know that the number of equivalence constacyclic classes are equal to $d = gcd(q-1, 3lp^s)$. Apparently, there are many cases may occur about d. They are respectively the following four cases arise:
(i) $d = gcd(q-1, 3lp^s) = 1$.
(ii) $d = gcd(q-1, 3lp^s) = 3$.
(iii) $d = gcd(q-1, 3lp^s) = l$.
(iv) $d = gcd(q-1, 3lp^s) = 3l$.

4.1 All constacyclic codes of length $3lp^s$ over F_q when $d = 1$

From Lemma 3.1, we see that $F_q^* = \langle \xi \rangle$ is the decomposition of coset over the subgroup $\langle \xi^d \rangle$, when $d = gcd(q-1, 3lp^s) = 1$. In this situation, it's clear that all constacyclic codes of length $3lp^s$ over F_q are equivalent to the cyclic codes. Therefore, we have the following theorem.

Theorem 4.1. Let $d = gcd(q-1, 3lp^s) = 1$, then $\lambda-$constacyclic codes C of length $3lp^s$ over F_q are equivalent to the cyclic codes, for any $\lambda \in F_q^*$, i.e. there exists a unique element $a \in F_q^*$ such that $a^{3lp^s}\lambda = 1$. And the map

$$\begin{aligned} &\varphi_a : F_q[x]/(x^{3lp^s} - 1) \to F_q[x]/(x^{3lp^s} - \lambda) \\ &f(x) \mapsto f(ax) \end{aligned}$$

is an isomorphism.
Further, we have the irreducible factorization of $x^{3lp^s} - \lambda$ in $F_q[x]$ as follows:
(i) if f is even, then

$$x^{3lp^s} - \lambda = \widehat{B}_0(ax)^{p^s} \widehat{B}_l(ax)^{p^s} \prod_{k'=0}^{2e-1} \widehat{B}_{g^{k'}}(ax)^{p^s} \prod_{k=0}^{e-1} \widehat{B}_{3g^k}(ax)^{p^s},$$

where $0 \le k \le e-1, 0 \le k' \le 2e-1$.
Therefore, we have

$$C = \langle \widehat{B}_0(ax)^{\varepsilon_0} \widehat{B}_l(ax)^{\rho_l} \prod_{k'=0}^{2e-1} \widehat{B}_{g^{k'}}(ax)^{\tau_{k'}} \prod_{k=0}^{e-1} \widehat{B}_{3g^k}(ax)^{\upsilon_k} \rangle,$$

$$C^{\perp} = \langle \widehat{B}_0(a^{-1}x)^{p^s-\varepsilon_0} \widehat{B}_l(a^{-1}x)^{p^s-\rho_l} \prod_{k'=0}^{2e-1} \widehat{B}_{g^{k'}}(a^{-1}x)^{p^s-\tau_{k'}} \prod_{k=0}^{e-1} \widehat{B}_{3g^k}(a^{-1}x)^{p^s-\upsilon_k} \rangle$$

where $0 \le \varepsilon_0, \rho_l, \tau_{k'}, \upsilon_k \le p^s$, for any $k = 0, 1, 2, ..., e$, and $k' = 0, 1, 2, ..., 2e$.
(ii) If f is odd, then

$$x^{3lp^s} - \lambda = \widehat{B}_0(ax)^{p^s} \widehat{B}_l(ax)^{p^s} \prod_{k=0}^{e-1} \widehat{B}_{g^k}(ax)^{p^s} \prod_{k=0}^{e-1} \widehat{B}_{3g^k}(ax)^{p^s},$$

where $0 \le k \le e-1$.
Therefore, we have

$$C = \langle \widehat{B}_0(ax)^{\varepsilon_0} \widehat{B}_l(ax)^{\rho_l} \prod_{k=0}^{e-1} \widehat{B}_{g^k}(ax)^{\tau_k} \prod_{k=0}^{e-1} \widehat{B}_{3g^k}(ax)^{\upsilon_k} \rangle,$$

$$C^{\perp} = \langle \widehat{B}_0(a^{-1}x)^{p^s-\varepsilon_0} \widehat{B}_l(a^{-1}x)^{p^s-\rho_l} \prod_{k=0}^{e-1} \widehat{B}_{g^k}(a^{-1}x)^{p^s-\tau_k} \prod_{k=0}^{e-1} \widehat{B}_{3g^k}(a^{-1}x)^{p^s-\upsilon_k} \rangle,$$

where $0 \le \varepsilon_0, \rho_l, \tau_{k'}, \upsilon_k \le p^s$, for any $k = 0, 1, 2, ..., e$.

Proof. Proof is trivial.

4.2 All constacyclic codes of length $3lp^s$ over F_q when $d = 3$

In the section, we consider the second case, i.e. $d = gcd(q-1, 3lp^s) = 3$. In this situation, we have that $F_q^* = \langle \xi \rangle = \langle \xi^3 \rangle \bigcup \xi^{p^s} \langle \xi^3 \rangle \bigcup \xi^{2p^s} \langle \xi^3 \rangle$ is the decomposition of coset of F_q^* over subgroup $\langle \xi^{3lp^s} \rangle$, by Lemma 3.1. Therefore, it's enough to consider the cyclic codes, $\xi^{p^s}-$constcyclic codes and $\xi^{2p^s}-$constcyclic codes if we want to determine all constacyclic codes of length $3lp^s$ over F_q, when $gcd(q-1, 3lp^s) = 3$.

From the section 2, we have that the irreducible factorization of $x^l - 1$ is given by $x^l - 1 = \prod_{i=0}^{e} M_i(x)$, where $M_i(x) = \prod_{j \in C_i}(x - \eta^i)$ with η is a primitive lth root of unity. According to this, we deduce the following lemma immediately, which gives the irreducible factorization of $x^{lp^s} - \xi^j$ in $F_q[x]$, when $gcd(q-1, l) = 1$.

Lemma 4.2. Let $gcd(q-1, l) = 1$. Then, for any $\xi^j \in F_q^*$, there exists a unique element $b_j \in F_q^*$ such that $b_j^{lp^s} \xi^j = 1$. Further, the irreducible factorization of $x^{lp^s} - \xi^j$ is given by

$$x^{lp^s} - \xi^j = \prod_{i=0}^{e} \widehat{M_i}(b_j x)^{p^s},$$

where $M_i(x)$ is the minimal polynomial of the $q-$cyclotomic coset C_i modulo l.

Proof. Similar to Lemma 3.1, we have the decomposition of coset of $F_q^* = \langle \xi \rangle$ over the subgroup $\langle \xi^{lp^s} \rangle$ is given by $F_q^* = \langle \xi \rangle$, when $gcd(q-1, l) = 1$. Next, proof is trivial, by Theorem 3.3.

Lemma 4.3. Let $gcd(q-1, 3lp^s) = 3$. Then there exists an element $\alpha = \xi^{\frac{q-1}{3}}$ be a primitive $3-$th root of unity. Further, the irreducible factorization of $x^{3lp^s} - 1$ is given by

$$x^{3lp^s} - 1 = \prod_{i=0}^{e} M_i(x)^{p^s} \widehat{M_i}(b_{\frac{q-1}{3}} x)^{p^s} \widehat{M_i}(b_{\frac{2(q-1)}{3}} x)^{p^s},$$

where $M_i(x)$ is the minimal polynomial of the $q-$cyclotomic coset C_i modulo l and $b_{\frac{q-1}{3}}$, $b_{\frac{2(q-1)}{3}} \in F_q^*$.

Proof. As $gcd(q-1, 3lp^s) = 3$, then it's clear that $\alpha = \xi^{\frac{q-1}{3}} \in F_q^*$ is a primitive $3-$th root of unity. Hence, we have

$$x^{3lp^s} - 1 = (x^l - 1)^{p^s} (x^l - \xi^{\frac{q-1}{3}})^{p^s} (x^l - \xi^{\frac{2(q-1)}{3}})^{p^s}.$$

Further, by Lemma 4.2, we get

$$x^{3lp^s} - 1 = \prod_{i=0}^{e} M_i(x)^{p^s} \widehat{M_i}(b_{\frac{q-1}{3}} x)^{p^s} \widehat{M_i}(b_{\frac{2(q-1)}{3}} x)^{p^s},$$

where $M_i(x)$ is the minimal polynomial of the $q-$cyclotomic coset C_i modulo l and $b_{\frac{q-1}{3}}$, $b_{\frac{2(q-1)}{3}} \in F_q^*$.

Before determine $\langle \xi^{ip^s} \rangle-$constacyclic codes, $i = 1, 2$, we must explicitly factory the polynomial $x^{3lp^s} - \xi^{ip^s}$, $i = 1, 2$, into monic irreducible factors product. Obviously, we only need

determine the irreducible factorization of $x^{3l}-\xi^i$, $i=1,2$. Firstly, we consider the polynomial $x^3-\xi^i$, $i=1,2$. Since, $x^3-\xi^i$, $i=1,2$, is irreducible in $F_q[x]$, we get that F_{q^3} is a splitting field for $x^3-\xi^i$, $i=1,2$, over F_q. Thus, there exists $\nu_i \in F_{q^3}$ such that $\nu_i^3=\xi^i$, $i=1,2$. Further, it's easy to get that $\nu_i, \alpha\nu_i$, and $\alpha^2\nu_i$ are all the roots of $x^3-\xi^i$, $i=1,2$, F_{q^3}, where α is a primitive 3−th root of unity. In addition, we see that $\nu_i \in F_{q^3}$ but ν_i not in F_q, and ν_i is primitive $3(q-1)$−th roots of unity,$i=1,2$.

As $gcd(3(q-1),l)=1$, we can find a bijection θ from the set D to itself such that $\theta(\nu)=\nu^l$, for any $\nu \in D$, where D consist of all the primitive $3(q-1)-th$ roots of unity of $F_{q^3}^*$. Therefore, there exists a unique element $\omega_i \in D$ such that $\nu_i^{-1}=\theta(\omega_i)=\omega_i^l$, i.e. $\omega_i^l\nu_i=1$, $i=1,2$.

From the above discussion, we have the following two lemmas.

Lemma 4.4. The irreducible factorization of $x^{3l}-\xi$ over F_q as follows:
(I) If $gcd(f,3)=1$,

$$\begin{aligned} x^{3l}-\xi &= (x^l-\nu_1)(x^l-\alpha\nu_1)(x^l-\alpha^2\nu_1) \\ &= \prod_{i=0}^{e}\widehat{M}_i(\omega_1 x)\widehat{M}_i(\alpha\omega_1 x)\widehat{M}_i(\alpha^2\omega_1 x) \\ &= \prod_{i=0}^{e}R_i(x), \end{aligned}$$

where ν_1 is a root of $x^3-\xi$, ω_1 is a primitive $3(q-1)$−th root of unity, α is a primitive 3−th root of unity, and $R_i(x)=\widehat{M}_i(\omega_1 x)\widehat{M}_i(\alpha\omega_1 x)\widehat{M}_i(\alpha^2\omega_1 x)$ for any $i=0,1,2,...,e$.
(II) If $gcd(f,3)=3$,

$$x^{3l}-\xi=(x^l-\nu_1)(x^l-\alpha\nu_1)(x^l-\alpha^2\nu_1)$$

$$=(x-\omega_1^{-1})(x-\alpha\omega_1^{-1})(x-\alpha^2\omega_1^{-1})\prod_{i=1}^{e}\widehat{A}_i(\omega_1 x)\widehat{A}_{iq}(\omega_1 x)\widehat{A}_{iq^2}(\omega_1 x)$$

$$\widehat{A}_i(\alpha\omega_1 x)\widehat{A}_{iq}(\alpha\omega_1 x)\widehat{A}_{iq^2}(\alpha\omega_1 x)\widehat{A}_i(\alpha^2\omega_1 x)\widehat{A}_{iq}(\alpha^2\omega_1 x)\widehat{A}_{iq^2}(\alpha^2\omega_1 x)$$

$=P(x)\prod_{i=1}^{e}Q_i(x)U_i(x)Z_i(x)$,
where ν_1 is a root of $x^3-\xi$, ω_1 is a primitive $3(q-1)$−th root of unity, α is a primitive 3−th root of unity, and $P(x)=(x-\omega_1^{-1})(x-\alpha\omega_1^{-1})(x-\alpha^2\omega_1^{-1})$, $Q_i(x)=\widehat{A}_i(\omega_1 x)\widehat{A}_{iq}(\alpha\omega_1 x)\widehat{A}_{iq^2}(\alpha^2\omega_1 x)$, $U_i(x)=\widehat{A}_i(\alpha\omega_1 x)\widehat{A}_{iq}(\alpha^2\omega_1 x)\widehat{A}_{iq^2}(\omega_1 x)$, and $Z_i(x)=\widehat{A}_i(\alpha^2\omega_1 x)\widehat{A}_{iq}(\omega_1 x)\widehat{A}_{iq^2}(\alpha\omega_1 x)$ for any $i=1,2,...,e$.

Proof. (I) If $gcd(f,3)=1$, we get C_0 and C_k,$1\le k\le e=\frac{\phi(l)}{f}$ are all the q^3−cyclotomic coset modulo l, from the section 2. Let ν_1 be a root of $x^3-\xi$, i.e $\nu_i^3=\xi$, and α be a primitive 3−th root of unity. Then, we have $\nu_1, \alpha\nu_1$, and $\alpha^2\nu_1$ are all the roots of $x^3-\xi$, over F_{q^3}, i.e.

$$x^{3l}-\xi=(x^l-\nu_1)(x^l-\alpha\nu_1)(x^l-\alpha^2\nu_1).$$

By above discussion, we know that there exists ω_1 such that $\omega_1^l\nu_1=1$, where ω_1 is a primitive $3(q-1)$−th root of unity and $\omega_1^q=\alpha\omega_1$. As $gcd(3,l)=1$, we know $l\equiv 1(mod 3)$ or $l\equiv 2(mod 3)$. When $l\equiv 2(mod 3)$, we have $(\alpha\omega_1)^l\alpha\nu_1=\alpha^{l+1}=1$ and $(\alpha^2\omega_1)^l\alpha^2\nu_1=\alpha^{2(l+1)}=1$. When $l\equiv 1(mod 3)$, we have $(\alpha^2\omega_1)^l\alpha\nu_1=\alpha^{2l+1}=1$ and $(\alpha\omega_1)^l\alpha^2\nu_1=\alpha^{l+2}=1$. Hence, there always

exist $\omega_1, \alpha\omega_1$ and $\alpha^2\omega_1$ such that $\omega_1^l\nu_1 = 1$, $(\alpha\omega_1)^l\alpha\nu_1 = 1$ and $(\alpha^2\omega_1)^l\alpha^2\nu_1 = 1$ or $\omega_1^l\nu_1 = 1$, $(\alpha^2\omega_1)^l\alpha\nu_1 = 1$ and $(\alpha\omega_1)^l\alpha^2\nu_1 = 1$. Further, by Lemma 4.2, we get

$$x^{3l} - \xi = \prod_{i=0}^{e} \widehat{M}_i(\omega_1 x)\widehat{M}_i(\alpha\omega_1 x)\widehat{M}_i(\alpha^2\omega_1 x),$$

which is the monic irreducible factorization of $x^{3l} - \xi$ over F_{q^3}. And we have $\widehat{M}_i(\omega_1 x) = \prod_{k\in C_i}(x - \omega_1^{-1}\eta k)$, $\widehat{M}_i(\alpha\omega_1 x) = \prod_{k\in C_i}(x - \alpha^2\omega_1^{-1}\eta k)$ and $\widehat{M}_i(\alpha^2\omega_1 x) = \prod_{k\in C_i}(x - \alpha\omega_1^{-1}\eta k)$. Obviously, when k runs over C_i, $\omega_1^{-1}\eta^k$ gives all the roots of $\widehat{M}_i(\omega_1 x)$. As $\omega_1^q = \alpha\omega_1$ and $kq, kq^2 \in C_i$, we have $(\omega_1^{-1}\eta^k)^q = \alpha^2\omega_1^{-1}\eta^{kq}$ and $(\omega_1^{-1}\eta^k)^{q^2} = \alpha\omega_1^{-1}\eta^{kq^2}$, which gives a root of $\widehat{M}_i(\alpha\omega_1 x)$ and $\widehat{M}_i(\alpha^2\omega_1 x)$ respectively. Therefore, it's easy to deduce that $\widehat{M}_i(\omega_1 x)\widehat{M}_i(\alpha^2\omega_1 x)$ $\widehat{M}_i(\alpha^2\omega_1 x)$ is irreducible polynomial over F_q.
(II) When $gcd(f, 3) = 3$, we have that $A_0, A_k, A_{kq}, A_{kq^2}$ consist of all the distinct q^3-cyclotomic coset modulo l, where $1 \le k \le e$. Then, the irreducible factorization of $x^l - 1$ over F_{q^3} is given by

$$x^l - 1 = A_0(x)A_1(x)A_q(x)A_{q^2}(X)A_2(x)A_{2q}(x)A_{2q^2}(x)...A_e(x)A_{eq}(x)A_{eq^2}(X).$$

Next, in the same way with (I), we can proved the conclusion (II) holds.

Using arguments similar to the Proof in Lemma 4.3, we have the following lemma, and we omit its proof here.

Lemma 4.5. The irreducible factorization of $x^{3l} - \xi^2$ over F_q as follows:
(I) If $gcd(f, 3) = 1$,

$$\begin{aligned} x^{3l} - \xi^2 &= (x^l - \nu_2)(x^l - \alpha\nu_2)(x^l - \alpha^2\nu_2) \\ &= \prod_{i=0}^{e} \widehat{M}_i(\omega_2 x)\widehat{M}_i(\alpha\omega_2 x)\widehat{M}_i(\alpha^2\omega_2 x) \\ &= \prod_{i=0}^{e} R_i^{'}(x), \end{aligned}$$

where ν_2 is a root of $x^3 - \xi^2$, ω_2 is a primitive $3(q-1)-$th root of unity, α is a primitive $3-$th root of unity, and $R_i^{'}(x) = \widehat{M}_i(\omega_2 x)\widehat{M}_i(\alpha\omega_2 x)\widehat{M}_i(\alpha^2\omega_2 x)$ for any $i = 0, 1, 2, ..., e$.
(II) If $gcd(f, 3) = 3$,

$$x^{3l} - \xi^2 = (x^l - \nu_2)(x^l - \alpha\nu_2)(x^l - \alpha^2\nu_2)$$

$$= (x - \omega_2^{-1})(x - \alpha\omega_2^{-1})(x - \alpha^2\omega_2^{-1}) \prod_{i=1}^{e} \widehat{A}_i(\omega_2 x)\widehat{A}_{iq}(\omega_2 x)\widehat{A}_{iq^2}(\omega_2 x)$$

$$\widehat{A}_i(\alpha\omega_2 x)\widehat{A}_{iq}(\alpha\omega_2 x)\widehat{A}_{iq^2}(\alpha\omega_2 x)\widehat{A}_i(\alpha^2\omega_2 x)\widehat{A}_{iq}(\alpha^2\omega_2 x)\widehat{A}_{iq^2}(\alpha^2\omega_2 x)$$

$= P^{'}(x)\prod_{i=1}^{e} Q_i^{'}(x)U_i^{'}(x)Z_i^{'}(x)$,
where ν_2 is a root of $x^3-\xi^2$, ω_2 is a primitive $3(q-1)-$th root of unity, α is a primitive $3-$th root of unity, and $P^{'}(x) = (x-\omega_2^{-1})(x-\alpha\omega_2^{-1})(x-\alpha^2\omega_2^{-1})$, $Q_i^{'}(x) = \widehat{A}_i(\omega_2 x)\widehat{A}_{iq}(\alpha\omega_2 x)\widehat{A}_{iq^2}(\alpha^2\omega_2 x)$, $U_i^{'}(x) = \widehat{A}_i(\alpha\omega_2 x)\widehat{A}_{iq}(\alpha^2\omega_2 x)\widehat{A}_{iq^2}(\omega_2 x)$, and $Z_i^{'}(x) = \widehat{A}_i(\alpha^2\omega_2 x)\widehat{A}_{iq}(\omega_2 x)\widehat{A}_{iq^2}(\alpha\omega_2 x)$ for any $i = 1, 2, ..., e$.

Theorem 4.6. Let $gcd(q-1, 3lp^s) = 3$, and $\alpha = \xi^{\frac{q-1}{3}}$ is a primitive 3−th root of unity. For any element λ of F_q^* and $\lambda-$constacyclic code C of length $3lp^s$ over F_q, one of the following cases holds:
(I) If $\lambda \in \langle \xi^3 \rangle$, then there exists some element $c \in F_q^*$ such that $c^{3lp^s}\lambda = 1$, and we have

$$C = \langle \prod_{i=0}^{e} \widehat{M}_i(cx)^{\varepsilon_i} \widehat{M}_i(cb_{\frac{q-1}{3}}x)^{\sigma_i} \widehat{M}_{-i}(cb_{\frac{2(q-1)}{3}}x)^{\tau_i} \rangle,$$

$$C^{\perp} = \langle \prod_{i=0}^{e} \widehat{M}_{-i}(c^{-1}x)^{p^s-\varepsilon_i} \widehat{M}_{-i}(c^{-1}b^{-1}_{\frac{q-1}{3}}x)^{p^s-\sigma_i} \widehat{M}_i(c^{-1}b^{-1}_{\frac{2(q-1)}{3}}x)^{p^s-\tau_i} \rangle,$$

where $0 \le \varepsilon_i, \sigma_i, \tau_i \le p^s$ for any $i = 0, 1, 2, ..., e$.
(II) If $\lambda \in \xi^{p^s}\langle \xi^3 \rangle$, then there exists some element $c_1 \in F_q^*$ such that $c_1^{3lp^s}\lambda = xi^{p^s}$, and one of the following holds:
(i) If $gcd(f, 3) = 1$,

$$C = \langle \prod_{i=0}^{e} \widehat{R}_i(c_1x)^{\varepsilon} \rangle,$$

$$C^{\perp} = \langle \prod_{i=0}^{e} \widehat{R}_{-i}(c_1^{-1}x)^{p^s-\varepsilon} \rangle,$$

where $0 \le \varepsilon \le p^s$, $R_{-i}(x) = \widehat{M}_{-i}(\omega_1^{-1}x)\widehat{M}_{-i}(\alpha^2\omega_1^{-1}x)\widehat{M}_{-i}(\alpha\omega_1^{-1}x)$ for any $i = 0, 1, 2, ..., e$.
(ii) If $gcd(f, 3) = 3$,

$$C = \langle \widehat{P}(c_1x)^{\varepsilon} \prod_{i=1}^{e} \widehat{Q}_i^{\varepsilon_i}(c_1x)\widehat{U}_i^{\sigma_i}(x)\widehat{Z}_i^{\tau_i}(c_1x) \rangle,$$

$$C^{\perp} = \langle \widehat{P}^*(c_1^{-1}x)^{p^s-\varepsilon} \prod_{i=1}^{e} \widehat{Q}_{-i}^{p^s-\varepsilon_i}(c_1^{-1}x)\widehat{U}_{-i}^{p^s-\sigma_i}(c_1^{-1}x)\widehat{Z}_{-i}^{p^s-\tau_i}(c_1^{-1}x) \rangle,$$

where $0 \le \varepsilon_i, \sigma_i, \tau_i \le p^s$, $P^*(x) = (x-\omega_1)(x-\alpha^2\omega_1)(x-\alpha\omega_1)$, $Q_{-i}(x) = \widehat{A}_{-i}(\omega_1^{-1}x) \cdot \widehat{A}_{-iq}(\alpha^2\omega_1^{-1}x)\widehat{A}_{-iq^2}(\alpha\omega_1^{-1}x)$, $U_{-i}(x) = \widehat{A}_{-i}(\alpha^2\omega_1^{-1}x)\widehat{A}_{-iq}(\alpha\omega_1^{-1}x)\widehat{A}_{-iq^2}(\omega_1^{-1}x)$, and $Z_{-i}(x) = \widehat{A}_{-i}(\alpha\omega_1^{-1}x)\widehat{A}_{-iq}(\omega_1^{-1}x)\widehat{A}_{-iq^2}(\alpha^2\omega_1^{-1}x)$, for any $i = 1, 2, ..., e$.
(II) If $\lambda \in \xi^{2p^s}\langle \xi^3 \rangle$, then there exists some element $c_2 \in F_q^*$ such that $c_2^{3lp^s}\lambda = xi^{2p^s}$, and one of the following holds:
(i) If $gcd(f, 3) = 1$,

$$C = \langle \prod_{i=0}^{e} \widehat{R'}_i(c_2x)^{\varepsilon_i} \rangle,$$

$$C^{\perp} = \langle \prod_{i=0}^{e} \widehat{R'}_{-i}(c_2^{-1}x)^{p^s-\varepsilon_i} \rangle,$$

where $0 \le \varepsilon \le p^s$, $R'_{-i}(x) = \widehat{M}_{-i}(\omega_2^{-1}x)\widehat{M}_{-i}(\alpha^2\omega_2^{-1}x)\widehat{M}_{-i}(\alpha\omega_2^{-1}x)$ for any $i = 0, 1, 2, ..., e$.
(ii) If $gcd(f, 3) = 3$,

$$C = \langle \widehat{P'}(c_2x)^{\varepsilon} \prod_{i=1}^{e} \widehat{Q'}_i(c_2x)^{\varepsilon_i}\widehat{U'}_i(c_2x)^{\sigma_i}\widehat{Z'}_i(c_2x)^{\tau_i}) \rangle,$$

$$C^{\perp} = \langle \widehat{P'}^{*}(c_2^{-1}x)^{p^s-\varepsilon} \prod_{i=1}^{e} \widehat{Q'}_{-i}(c_2^{-1}x)^{p^s-\varepsilon_i} \widehat{U'}_{-i}(c_2^{-1}x)^{p^s-\sigma_i} \widehat{Z'}_{-i}(c_2^{-1}x)^{p^s-\tau_i} \rangle,$$

where $0 \leq \varepsilon_i, \sigma_i, \tau_i \leq p^s$, $P'^{*}(x) = (x-\omega_2)(x-\alpha^2\omega_2)(x-\alpha\omega_2)$, $Q'_{-i}(x) = \widehat{A}_{-i}(\omega_2^{-1}x) \cdot \widehat{A}_{-iq}(\alpha^2\omega_2^{-1}x)\widehat{A}_{-iq^2}(\alpha\omega_2^{-1}x)$, $U'_{-i}(x) = \widehat{A}_{-i}(\alpha^2\omega_2^{-1}x)\widehat{A}_{-iq}(\alpha\omega_2^{-1}x)\widehat{A}_{-iq^2}(\omega_2^{-1}x)$, and $Z'_{-i}(x) = \widehat{A}_{-i}(\alpha\omega_2^{-1}x)\widehat{A}_{-iq}(\omega_2^{-1}x)\widehat{A}_{-iq^2}(\alpha^2\omega_2^{-1}x)$ for any $i = 1, 2, ..., e$.

Proof. From Lemma 4.3, Lemma 4.4 and Lemma 4.5, we see that the theorem is straightforward.

4.3 All constacyclic codes of length $3lp^s$ over F_q when $d = l$

Let $d = gcd(q-1, 3lp^s) = l$, i.e. $l|(q-1)$, and $gad(q-1, 3) = 1$. Then there is an element $\eta = \xi^{\frac{q-1}{l}} \in F_q^*$, which is a primitive $l-$th root of unity. Therefor, we have the following lemma.

Lemma 4.7. Assume that $gcd(q-1, 3lp^s) = l$, and let $\eta = \xi^{\frac{q-1}{l}}$ be a primitive $l-$th root of unity in F_q. Then, the irreducible factorization of $x^{3lp^s} - 1$ over F_q as follows:

$$x^{3lp^s} - 1 = \prod_{k=1}^{l} (x-\eta^k)^{p^s}(x^2 + \eta^k x + \eta^{2k})^{p^s}.$$

Proof. As $gad(q-1, 3) = 1$, there is not any primitive $3-$th root of unity in F_q, which implies $x^2 + x + 1$ is irreducible. By this, we can deduce that $x^2 + \eta^k x + \eta^{2k}$ is irreducible, for any $k = 1, 2, ..., l$. Because if $x^2 + \eta^k x + \eta^{2k}$ is reducible, then $\eta^{-2k}(x^2 + \eta^k x + \eta^{2k}) = (\eta^{-k}x)^2 + \eta^{-k}x + 1$ is reducible. Set $x = \eta^{-k}x$, then $x^2 + x + 1$ is reducible which is a contradiction. Since $\eta = \xi^{\frac{q-1}{l}}$ be a primitive $l-$th root of unity, then η^3 is also a primitive $l-$th root of unity. Hence, the irreducible factorization of $x^{3lp^s} - 1$ over F_q is given by

$$x^{3lp^s} - 1 = (x^{3l} - 1)^{p^s} = \prod_{k=1}^{l} (x^3 - \eta^{3k})^{p^s} = \prod_{k=1}^{l} (x-\eta^k)^{p^s}(x^2 + \eta^k x + \eta^{2k})^{p^s}.$$

Lemma 4.8. Assume that $gcd(q-1, 3lp^s) = l$, then the irreducible factorization of $x^{3lp^s} - \xi^{jp^s}$, $1 \leq j \leq l-1$ over F_q as follows:
(I) When $(3, j) = 3$, i.e. $3|j$, let $j = 3k$, for some integer k. Then we have

$$x^{3lp^s} - \xi^{jp^s} = (x^{3l} - \xi^{3k})^{p^s} = (x^l - \xi^k)^{p^s}(x^{2l} + \xi^k x^l + \xi^{2k})^{p^s}.$$

(II) When $(3, j) = 1$, there must exists some integer i, $1 \leq i \leq q-1$, such that $3i = j + q - 1$ or $3i = j + 2(q-1)$. Then one of the following conclusions holds:
(i) When $3i = j + q - 1$, we have

$$\begin{aligned} x^{3lp^s} - \xi^{jp^s} &= x^{3lp^s} - \xi^{(j+q-1)p^s} \\ &= (x^{3l} - \xi^{(j+q-1)})^{p^s} \\ &= (x^{3l} - \xi^{3i})^{p^s} \\ &= (x-\xi^i)^{p^s}(x^{2l} + \xi^i x^l + \xi^{2i})^{p^s}. \end{aligned}$$

(ii) When $3i = j + 2(q-1)$, we have

$$\begin{aligned} x^{3lp^s} - \xi^{jp^s} &= x^{3lp^s} - \xi^{(j+2(q-1))p^s} \\ &= (x^{3l} - \xi^{(j+2(q-1))})^{p^s} \\ &= (x^{3l} - \xi^{3i})^{p^s} \\ &= (x-\xi^i)^{p^s}(x^{2l} + \xi^i x^l + \xi^{2i})^{p^s}. \end{aligned}$$

Proof. (I) Obviously, $gcd(l,k) = 1$. From Lemma 2.3, it's very easy to verify that $x^l - \xi^k$ is irreducible. By the proof of Lemma 4.5, we see that $x^2 + \xi^k x + \xi^{2k}$ is irreducible over F_q. Now, we suppose that δ is any root of $x^2 + \xi^k x + \xi^{2k}$ in some extended field of F_q, and e is the order of δ. Then, we have $\delta^3 = \xi^{3k}$. Further, we deduce that $\frac{e}{(e,3)} = \frac{q-1}{(q-1,3k)}$, i.e $\frac{e}{(e,3)} = \frac{q-1}{(q-1,k)}$, as $gcd(q-1,3) = 1$. By the reduction again, we get $e = \frac{(q-1)(e,3)}{(q-1,k)}$. From Lemma 2.4, we can verify that $x^{2l} + \xi^k x^l + \xi^{2k}$ is irreducible.
(II) When $(3,j) = 1$, we get that $x^3 - \xi^j$, $1 \le j \le l-1$, are all reducible, from Lemma 2.3. Therefor, there must exist some $\xi^i \in F_q^*$ is a root of $x^3 - \xi^j$, for any $j = 1, 2, ...l-1$. Then, $\xi^{3i} - \xi^j = 0$, i.e. $\xi^{3i} = \xi^j$. As $1 \le i \le q-1$ and $1 \le j \le l-1$, we deduce that $3i = j + q - 1$ or $3i = j + 2(q-1)$ and $gcd(l.i) = 1$. Next, working similar to the proof of (I), we get that conclusion (i) and conclusion (ii) hold.

From above lemmas , we get the following theory immediately.

Theorem 4.9. Assume that $gcd(q-1, 3lp^s) = l$, and let $\eta = \xi^{\frac{q-1}{l}}$ be a primitive $l-$th root of unity in F_q. For any element λ of F_q^* and $\lambda-$constacyclic code C of length $3lp^s$ over F_q, one of the following cases holds:
(I) If $\lambda \in \langle \xi^l \rangle$, then there exists $c_1 \in F_q^*$ such that $c_1^{3lp^s}\lambda = 1$, and we have

$$C = \langle \prod_{k=1}^{l} (x - c_1^{-1}\eta^k)^{\varepsilon_k}(x^2 + c_1^{-1}\eta^k x + c_1^{-2}\eta^{2k})^{\tau_k} \rangle,$$

$$C^{\perp} = \langle \prod_{k=1}^{l} (x - c_1\eta^{-k})^{p^s-\varepsilon_k}(x^2 + c_1\eta^{-k} x + c_1^2\eta^{-2k})^{p^s-\tau_k} \rangle,$$

where $0 \le \varepsilon_k, \tau_k \le p^s$, for any $k = 1, 2, ..., l$.
(II) If $\lambda \in \xi^{jp^s}$, $1 \le j \le l-1$, then there exists $c_2 \in F_q^*$ such that $c_2^{3lp^s}\lambda = \xi^{jp^s}$, and one of the following holds:
(i) When $(3,j) = 3$, i.e. $3|j$, let $j = 3k$, for some integer k. we have

$$C = \langle (x^l - c_2^{-1}\xi^k)^{\varepsilon_k}(x^{2l} + c_2^{-1}\xi^k x^l + c_2^{-2}\xi^{2k})^{\tau_k} \rangle,$$

$$C^{\perp} = \langle (x^l - c_2\xi^{-k})^{p^s-\varepsilon_k}(x^{2l} + c_2\xi^{-k} x^l + c_2^2\xi^{-2k})^{p^s-\tau_k} \rangle,$$

where $o \le \varepsilon_k, \tau_k \le p^s$.
(ii) When $(3,j) = 1$, there must exists some integer i, $1 \le i \le q-1$, such that $3i = j + q - 1$ or $3i = j + 2(q-1)$. Then one of the following conclusions holds:
(a) When $3i = j + q - 1$, we have

$$C = \langle (x - c_2^{-1}\xi^i)^{\varepsilon_i}(x^{2l} + c_2^{-1}\xi^i x^l + c_2^{-2}\xi^{2i})^{\tau_i} \rangle,$$

$$C^{\perp} = \langle (x - c_2\xi^{-i})^{p^s-\varepsilon_i}(x^{2l} + c_2\xi^{-i}x^l + c_2^2\xi^{-2i})^{p^s-\tau_i}\rangle.$$

where $0 \leq \varepsilon_i, \tau_i \leq p^s$.
(b) When $3i = j + 2(q-1)$, we have

$$C = (x - c_2^{-1}\xi^i)^{\varepsilon_i}(x^{2l} + c_2^{-1}\xi^i x^l + c_2^{-2}\xi^{2i})^{\tau_i},$$

$$C^{\perp} = (x - c_2\xi^{-i})^{p^s-\varepsilon_i}(x^{2l} + c_2\xi^{-i}x^l + c_2^2\xi^{-2i})^{p^s-\tau_i},$$

where $0 \leq \varepsilon_i, \tau_i \leq p^s$.

4.4 All constacyclic codes of length $3lp^s$ over F_q when $d = 3l$

In the section, we assume that $d = gcd(3lp^s, q-1) = 3l$, namely $3l|q-1$. Clearly, there exists an element $\gamma = \xi^{\frac{q-1}{3l}} \in F_q^*$, which is a primitive $3l-$th root of unity. Further, Due to $l|q-1$, and $3|q-1$, it's easy to know that $\eta = \xi^{\frac{q-1}{l}}$ and $\beta = \xi^{\frac{q-1}{3}}$ are primitive $l-$th and $3-$th root of unity respectively.

From Lemma 3.1, we get that the $F_q^* = \langle\xi\rangle = \langle\xi^{3l}\rangle \cup \xi^{p^s}\langle\xi^{3l}\rangle \cup \xi^{2p^s}\langle\xi^{3l}\rangle \cup ... \cup \xi^{(3l-1)p^s}\langle\xi^{3l}\rangle$. Therefore, any element λ of F_q^* belongs to exactly one of the cosets, i.e. there is a unique integer j, $0 \leq j \leq 3l-1$, such that $\lambda \in \xi^{jp^s}\langle\xi^{3l}\rangle$, namely $\lambda-$constacyclic codes are equivalent to $\xi^{jp^s}-$constacyclic codes. Hence, we just need to determine $\xi^{jp^s}-$constacyclic codes, where $0 \leq j \leq 3l-1$.

Lemma 4.10. Let$d = gcd(3lp^s, q-1) = 3l$ and $\gamma = \xi^{\frac{q-1}{3l}}$. Then irreducible factorization of $x^{3lp^s} - 1$ over F_q as follow:

$$x^{3lp^s} - 1 = \prod_{i=0}^{3l-1}(x - \gamma^i)^{p^s}.$$

Proof. proof is trivial.

Lemma 4.11. Let $\eta = \xi^{\frac{q-1}{l}}$ and $\beta = \xi^{\frac{q-1}{3}}$. Then the irreducible factorization of $x^{3lp^s} - \xi^{jp^s}$ over F_q as follows:
(I) when $gcd(3l, j) = l$, we have

$$x^{3lp^s} - \xi^{jp^s} = (x^{3l} - \xi^{tl})^{p^s} = \prod_{i=0}^{l-1}(x^3 - \xi^t\eta^i)^{p^s},$$

where $t = 1$ or 2.
(II) when $gcd(3l, j) = 3$, we have

$$x^{3lp^s} - \xi^{jp^s} = (x^{3l} - \xi^{3k})^{p^s} = \prod_{i=0}^{2}(x^l - \xi^k\beta^i)^{p^s},$$

where k is some integer such that $j = 3k$.
(III) Otherwise, we can see that $gcd(3l, j) = 1$. Then we have

$$x^{3lp^s} - \xi^{jp^s} = (x^{3l} - \xi^j)^{p^s}$$

.

Proof. (I) As $gcd(3l, j) = l$ and $1 \leq j \leq 3l-1$, we have $j = tl$, where $t = 1, 2$. Obviously, $\eta = \xi^{\frac{q-1}{l}}$ is a primitive $l-$th root of unity in F_q. Therefor, we get

$$x^{3lp^s} - \xi^{jp^s} = (x^{3l} - \xi^{tl})^{p^s} = \prod_{i=0}^{l-1}(x^3 - \xi^t\eta^i)^{p^s},$$

Next, we prove that the polynomial $x^3 - \xi^t\eta^i$, for any $i = 0, 1, 2, ..., l-1$, is irreducible in $F_q[x]$. Firstly, we know that the multiplicative order of $\xi^t\eta^i = \xi^{t+\frac{i(q-1)}{l}}$, $t = 1, 2$, is $e_i = \frac{q-1}{(q-1, t+\frac{i(q-1)}{l}}$. As $3|q-1$ but $gcd(3, t) = 1$ and $gcd(3, l) = 1$, we get that $(3, t + \frac{i(q-1)}{l}) = 1$. Thus, 3 divides e_i but not $\frac{q-1}{e_i} = (q-1, t + \frac{i(q-1)}{l})$. From Lemma 2.3, we get the polynomial $x^3 - \xi^t\eta^i$, for any $i = 0, 1, 2, ..., l-1$, is irreducible in $F_q[x]$. In the same way, we have conclusions (II) and (III) hold.

In the following theorem, we determine all constacyclic codes of length $3lp^s$ over F_q and their dual codes, when $d = gcd(3lp^s, q-1) = 3l$.

Theorem 4.12. Assume that $gcd(3lp^s, q-1) = 3l$, let $\gamma = \xi^{\frac{q-1}{3l}}, \eta = \xi^{\frac{q-1}{l}}$ and $\beta = \xi^{\frac{q-1}{3}}$ be primitive $3l-$th, $l-$th and $3-$th root of unity in f_q respectively. For any element λ of F_q^* and $\lambda-$ constcyclic codes C of length $3lp^s$ over F_q. One of the following holds:
(I) If $\lambda \in \langle \xi^{3l} \rangle$, then there exists $d_1 \in F_q^*$ such that $d_1^{3lp^s}\lambda = 1$, and we have

$$C = \langle \prod_{i=0}^{3l-1}(x - d_1^{-1}\gamma^i)^{\varepsilon_i} \rangle,$$

$$C^{\perp} = \langle \prod_{i=0}^{3l-1}(x - d_1\gamma^{-i})^{p^s-\varepsilon_i} \rangle,$$

where $0 \leq \varepsilon_i \leq p^s$, for any $i = 0, 1, 2, ..., 3l-1$.
(II) If $\lambda \in \xi^{jp^s}\langle \xi^{3l} \rangle$, $1 \leq j \leq 3l-1$, then there exist $d_2 \in F_q^*$ such that $d_2^{3lp^s}\lambda = \xi^{jp^s}$, and one of the following holds:
(i) when $gcd(3l, j) = l$, we have

$$C = \langle \prod_{i=0}^{l-1}(x^3 - d_2^{-3}\xi^t\eta^i)^{\varepsilon_i} \rangle,$$

$$C^{\perp} = \langle \prod_{i=0}^{l-1}(x^3 - d_2^3\xi^{-t}\eta^{-i})^{p^s-\varepsilon_i} \rangle,$$

where $0 \leq \varepsilon_i \leq p^s$, for any $i = 0, 1, 2, ..., l-1$.
(ii) when $gcd(3l, j) = 3$, we have

$$C = \langle \prod_{i=0}^{2}(x^l - d_2^{-l}\xi^k\beta^i)^{\varepsilon_i} \rangle,$$

$$C^{\perp} = \langle \prod_{i=0}^{2} (x^l - d_2^l \xi^{-k} \beta^{-i})^{p^s - \varepsilon_i} \rangle,$$

where $0 \leq \varepsilon_i \leq p^s$ for $i = 0, 1, 2$. And k is some integer such that $j = 3k$.
(iii) When $gcd(3l, j) = 1$. Then we have

$$C = \langle (x^{3l} - d_2^{-3l} \xi^j)^{\varepsilon} \rangle,$$

$$C^{\perp} = \langle (x^{3l} - d_2^{3l} \xi^{-j})^{p^s - \varepsilon} \rangle,$$

where $0 \leq \varepsilon \leq p^s$.

5 All self-dual cyclic codes of length $3lp^s$ over F_q

In section 4, we have given the generator polynomials of all the constacyclic codes and their dual codes of length $3lp^s$ over F_q. Further, we more detailed determine all the self-dual cyclic(negacyclic) codes of length $3lp^s$ over F_q, in this section.

It's well known that there exist self-dual cyclic codes of length N over F_q if and only if N is even and the characteristic of F_q is $p = 2$ [10, 11]. Therefore, we get that self-dual cyclic codes of length $3lp^s$ over F_q exist only when $p = 2$, in this paper. What's more, when $p = 2$, cyclic codes are the same with negacyclic codes of length $3l2^s$ over F_{2^m}. Therefore, aim to obtain self-dual cyclic and negacyclic codes, we just need to work on cyclic(negacyclic) codes.

Let $x^{3lp^s} - 1 = (x^{3l} - 1)^{p^s} = f_1(x)^{p^s} f_2(x)^{p^s} \cdots f_a(x)^{p^s} h_1(x)^{p^s} h_1^*(x)^{p^s} \cdots h_j(x)^{p^s} h_b^*(x)^{p^s}$ be the irreducible factorization of $x^{3lp^s} - 1$, where $f_i(x)$, $1 \leq i \leq a$, is monic irreducible self-reciprocal polynomial over F_q, $h_j(x)$ and its reciprocal polynomial $h_j^*(x)$, $1 \leq j \leq b$, are also monic irreducible polynomial over F_q. Further, for any cyclic code $C = \langle g(x) \rangle$ of length $3lp^s$ over F_q, we suppose that

$$g(x) = f_1(x)^{\tau_1} f_2(x)^{\tau_2} \cdots f_a(x)^{\tau_a} h_1(x)^{\delta_1} h_1^*(x)^{\sigma_1} \cdots h_b(x)^{\delta_b} h_1^*(x)^{\sigma_b},$$

where $0 \leq \tau_i, \delta_j, \sigma_k \leq p^s$. Then, we have

$$h(x) = f_1(x)^{p^s - \tau_1} f_2(x)^{p^s - \tau_2} \cdots f_a(x)^{p^s - \tau_a} h_1(x)^{p^s - \delta_1} h_1^*(x)^{p^s - \sigma_1} \cdots h_b(x)^{p^s - \delta_b} h_1^*(x)^{p^s - \sigma_b},$$

Therefore,

$$h^*(x) = f_1(x)^{p^s - \tau_1} f_2(x)^{p^s - \tau_2} \cdots f_a(x)^{p^s - \tau_a} h_1(x)^{p^s - \sigma_1} h_1^*(x)^{p^s - \delta_1} \cdots h_b(x)^{p^s - \sigma_b} h_1^*(x)^{p^s - \delta_b},$$

If C is a self-dual cyclic code, we get the following theorem.

Theorem 5.1. With the above notations, we have that C is a self-dual cyclic code if and only if $2\tau_i = p^s$, $0 \leq i \leq a$, and $\delta_j + \sigma_j = p^s$, $0 \leq j \leq b$.

Proof. C is a self-dual cyclic code if and only if $g(x) = h^*(x)$, i.e. $2\tau_i = p^s$, $0 \leq i \leq a$, and $\delta_j + \sigma_j = p^s$, $0 \leq j \leq b$.

According to this theorem, we see that it's enough to determine the irreducible factorization of $x^{3lp^s} - 1$ as above. And if we do this, we can give all the self-dual cyclic codes immediately.

Similar to the definition of reciprocal polynomials, we give the following definition.

Definition 5.2. Let $C_s = (s, sq, ...sq^{f-1})$ be any $q-$cyclotomic coset modulo l, then

$$C_s^* = (-s, -sq, ... - sq^{f-1})$$

is said to be the reciprocal coset of C_s. And C_s is called self-reciprocal if $C_s = C_s^*$.

Obviously, C_s^* is still a $q-$cyclotomic coset modulo l. And the reciprocal polynomial of the minimal polynomial of C_s is the minimal polynomial of C_s^*. Hence, the minimal polynomial of C_s is also self-reciprocal if C_s is self-reciprocal.

Lemma 5.3. When $q \equiv 1(mod 3)$, For the $q-$cyclotomic coset, which have been described in Lemma 2.1, one of the following holds:
(I) If $f = ord_l(q)$ is even, we have

$$B_0^* = B_0, B_l^* = B_{-l}, B_{g^k}^* = B_{-g^k}, B_{3g^k}^* = B_{3g^k},$$

where $0 \leq k \leq e-1$.
(II) If $f = ord_l(q)$ is odd, we have

$$B_0^* = B_0, B_l^* = B_{-l}, B_{g^k}^* = B_{-g^k}, B_{3g^{k'}}^* = B_{-3g^{k'}}$$

where $\{B_{3g^k}\} = \{B_{3g^{k'}}\} \bigcup \{B_{-3g^{k'}}\}$ and $0 \leq k \leq e-1$, $0 \leq k^{'} \leq \frac{e}{2} - 1$.

Proof. (I) Obviously, we only need to prove $B_{3g^k}^* = B_{3g^k}$. If $f = ord_l(q)$ is even, we deduce that $q^{\frac{f}{2}} \equiv -1(modl)$. According to this, we get there exist i, j, $0 \leq i, j \leq f-1$, and $|j-i| = \frac{f}{2}$, such that $3g^k q^i \equiv -3g^k q^j (mod 3l)$, for any $3g^k q^i \in B_{3g^k}$, $0 \leq k \leq e-1$. Therefore, we have $B_{3g^k}^* = B_{3g^k}$, for any $k = 0, 1, ...e-1$.
(II) In the same way with Lemma 2.1, we get $B_0, B_l, B_{-l}, B_{g^k}, B_{-g^k}, B_{3g^{k'}}$ and $B_{-3g^{k'}}$, $0 \leq k \leq e-1$, $0 \leq k^{'} \leq \frac{e}{2} - 1$, are all the distinct $q-$cyclotomic coset modulo $3l$. Next, the result is obvious.

Lemma 5.4. If $q \equiv 2(mod 3)$ and f is even, For the $q-$cyclotomic coset, which have been described in Lemma 2.1, one of the following holds:
(I) When $f = 2t$ and t is even, we have

$$B_0^* = B_0, B_l^* = B_l, B_{g^k}^* = B_{-g^k}, B_{3g^k}^* = B_{3g^k},$$

where $\{B_{g^{k'}}\} = \{B_{g^k}\} \bigcup \{B_{-g^k}\}$,$0 \leq k \leq e-1$ and $0 \leq k^{'} \leq 2e-1$.
(II) When $f = 2t$ and t is odd, we have

$$B_0^* = B_0, B_l^* = B_l, B_{g^{k'}}^* = B_{g^{k'}}, B_{3g^k}^* = B_{3g^k},$$

where $0 \leq k \leq e-1$ and $0 \leq k^{'} \leq 2e-1$.

Proof. (I) In the same way with Lemma 2.1, we get $B_0, B_l, B_{g^k}, B_{-g^k}$ and B_{3g^k} , $0 \leq k \leq e-1$, are all the distinct $q-$cyclotomic coset modulo $3l$. Next, We first prove that $B_l^* = B_l$, i.e. $\{l, lq\}^* = \{l, lq\}$. As $q \equiv 2(mod 3)$, i.e $q \equiv -1(mod 3)$, then $lq \equiv -l(mod 3)$. Since $gcd(3, l) = 1$, we have $lq \equiv -l(mod 3l)$, which implies $B_l^* = B_l$. Otherwise, similar to the proof in (II) of Lemma 5.3, we get the other results immediately.

(II) According to (I), it's obvious that we only need to prove $B^*_{g^{k'}} = B_{g^{k'}}$. As t is odd, we have $q^t \equiv -1(mod 3)$. Since $q^t \equiv -1(mod l)$ and $gcd(3,l) = 1$, we get $q^t \equiv -1(mod 3l)$. Then, we deduce that there exist i, j, $0 \leq i, j \leq f-1$, and $|j-i| = t$, such that $g^{k'} q^i \equiv -g^{k'} q^j (mod 3l)$, for any $g^{k'} q^i \in B_{k'}$, $0 \leq k' \leq 2e-1$, i.e. $B^*_{g^{k'}} = B_{g^{k'}}$.

Lemma 5.5. If $q \equiv 2(mod 3)$ and f is odd, For the $q-$cyclotomic coset, which have been described in Lemma 2.1, we have

$$B^*_0 = B_0, B^*_l = B_l, B^*_{g^{k'}} = B_{-g^{k'}}, B^*_{3g^{k'}} = B_{-3g^{k'}},$$

where $\{B_{g^k}\} = \{B_{g^{k'}}\} \bigcup \{B_{-g^{k'}}\}$, $\{B_{3g^k}\} = \{B_{3g^{k'}}\} \bigcup \{B_{-3g^{k'}}\}$ and $0 \leq k \leq e-1$, $0 \leq k' \leq \frac{e}{2} - 1$.

From the above lemmas, we can give all the self-dual cyclic(negacyclic) codes of length $3l2^s$ over F_{2^m} and its enumeration in the following theorem.

Theorem 5.6. let $l \neq 3$ be an odd prime, $p = 2$, $f = ord_l(2^m)$, and $e = \frac{l-1}{f}$. Then, for cyclic(negacyclic) self-dual codes of length $3l2^s$ over F_{2^m}, we have
(I) When $q \equiv 1(mod 3)$, one of the following hold:
(i) If $f = ord_l(q)$ is even, then there exist $(2^s+1)^{e+1}$ cyclic self-dual codes of length $3l2^s$ over F_{2^m}. And they are given by

$$\langle (x-1)^{2^{s-1}} B_l(x)^{\delta} B_{-l}(x)^{2^s-\delta} \prod_{k=0}^{e-1} B_{g^k}(x)^{\delta_k} B_{-g^k}(x)^{2^s-\delta_k} B_{3g^k}(x)^{2^{s-1}} \rangle,$$

where $0 \leq \delta, \delta_k \leq 2^s$, for any $0 \leq k \leq e$.
(ii) If $f = ord_l(q)$ is odd, then there exist $(2^s+1)^{\frac{3e}{2}+1}$ cyclic self-dual codes of length $3l2^s$ over F_{2^m}. And they are given by

$$\langle (x-1)^{2^{s-1}} B_l(x)^{\delta} B_{-l}(x)^{2^s-\delta} \prod_{k=0}^{e-1} B_{g^k}(x)^{\delta_k} B_{-g^k}(x)^{2^s-\delta_k} \prod_{k=0}^{\frac{e}{2}-1} B_{3g^k}(x)^{\sigma_k} B_{-3g^k}(x)^{2^s-\sigma_k} \rangle,$$

where $0 \leq \delta, \delta_k, \sigma_k \leq 2^s$, for any $0 \leq k \leq e$.
(II) When $q \equiv 2(mod 3)$, we have
(i) If $f = 2t$ and t is even, then there exist $(2^s+1)^e$ cyclic self-dual codes of length $3l2^s$ over F_{2^m}. And they are given by

$$\langle (x-1)^{2^{s-1}} B_l(x)^{2^{s-1}} \prod_{k=0}^{e-1} B_{g^k}(x)^{\delta_k} B_{-g^k}(x)^{2^s-\delta_k} B_{3g^k}(x)^{2^{s-1}} \rangle,$$

where $0 \leq \delta_k \leq 2^s$, for any $0 \leq k \leq e$.
(ii) if $f = 2t$ and t is odd, then there exists only one cyclic self-dual codes of length $3l2^s$ over F_{2^m}. And they are given by

$$\langle (x-1)^{2^{s-1}} B_l(x)^{2^{s-1}} \prod_{k=0}^{2e-1} B_{g^{k'}}(x)^{2^{s-1}} \prod_{k=0}^{e-1} B_{3g^k}(x)^{2^{s-1}} \rangle.$$

(*iii*) If f is odd, then there exist $(2^s+1)^e$ cyclic self-dual codes of length $3l2^s$ over F_{2^m}. And they are given by

$$\langle (x-1)^{2^{s-1}} B_l(x)^{2^{s-1}} \prod_{k'=0}^{\frac{e}{2}-1} B_{g^{k'}}(x)^{\delta_{k'}} B_{-g^{k'}}(x)^{2^s-\delta_{k'}} B_{3g^{k'}}(x)^{\sigma_{k'}} B_{-3g^{k'}}(x)^{2^s-\sigma_{k'}} \rangle.$$

where $0 \leq \delta_{k'}, \sigma_{k'} \leq 2^s$, for any $0 \leq k \leq e$.

Acknowledgments

The authors would like to thank the referees for their helpful comments and a very meticulous reading of this manuscript.

References

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

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

[3] H.Q. Dinh, Repeated-root constacyclic codes of length $2p^s$, Finite Fields Appl. 18 (2012) 940-950.

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

[5] H.Q. Dinh, Structure of repeated-root cyclic codes and negacyclic codes of length $6p^s$ and their duals, Contemp. Math. 609 (2014) 69-87.

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

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

[8] Anuradha Sharma, Repeated-root constacyclic codes of length l^tp^s and their duals codes, Cryptogr. Commun. 7 (2015) 229-255.

[9] B. Chen, H.Q. Dinh, H.Liu, Repeated-root constacyclic codes of length $2l^mp^s$, Finite Fields Appl. 33 (2015) 137-159.

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

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

[12] H.Q. Dinh, On the lineare odering of some classess of negacyclic and cyclic codes and their distance distributions, Finite Fields Appl. 14 (2008) 22-40.

[13] H.Q. Dinh, Constacyclic codes of length p^s over $F_{p^m}+uF_{p^m}$, J. Algebra 324 (2010) 940-950.

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

[15] 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.

[16] David M. Burton, Elementary Number Theory, Tata McGraw-Hill, 2006.

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