Journal of Algebra, Number Theory: Advances and Applications
Volume 15, Number 1, 2016, Pages 41-64
Available at http://scientificadvances.co.in
DOI: http://dx.doi.org/10.18642/jantaa_7100121523

CONSTACYCLIC CODES OF LENGTH $p^n q^m$ OVER A FINITE FIELD

AMITA SAHNI and POONAM TRAMA SEHGAL

Centre for Advanced Study in Mathematics
Panjab University
Chandigarh 160014
India
e-mail: sahniamita05@gmail.com
poonam.sehgal@gmail.com

Abstract

Let $\mathbb{F}_\ell$ be a finite field with ℓ elements, where ℓ is an odd prime power. We explicitly determine the λ-constacyclic codes of length $p^n q^m$ over $\mathbb{F}_\ell$ and their duals in terms of the generator polynomials, where p, q are distinct odd primes coprime to ℓ. All the repeated root constacyclic codes of length $p^n q^m \ell^u$ over $\mathbb{F}_{\ell^v}$ and their duals are also characterized in terms of the generator polynomials. The number of such codes have also been found.

1. Introduction

Since 1950's cyclic and negacyclic codes have been studied extensively. These codes can be obtained from the class of constacyclic codes. Constacyclic codes form an important class of linear codes due to

2010 Mathematics Subject Classification: 11T71, 94B05, 94B15.
Keywords and phrases: constacyclic codes, generator polynomials, dual codes, cyclotomic cosets.
Received July 13, 2015

their rich algebraic structures, which are useful for efficient error detection and correction. Let $\mathbb{F}_\ell$ denote a finite field with ℓ elements. An $[N, k]$ linear code C of length N and dimension k over $\mathbb{F}_\ell$ is a k-dimensional subspace of the vector space $\mathbb{F}_\ell^N$. Elements of the subspace C are called codewords and are written as row vectors: $c = (c_0, c_1, \ldots, c_{N-1})$. A linear code C over $\mathbb{F}_\ell$ is called λ-constacyclic code if $(\lambda c_{N-1}, c_0, \ldots, c_{N-2})$ is in C for every $(c_0, c_1, \ldots, c_{N-1})$ in C. Let $\theta : \mathbb{F}_\ell^N \to \frac{\mathbb{F}_\ell[x]}{< x^N - \lambda >}$ be a map given by $\theta((c_0, c_1, \ldots, c_{N-1})) = c_0 + c_1 x + \cdots + c_{N-1}x^{N-1} \bmod (x^N - \lambda)$. One can easily check that θ is an $\mathbb{F}_\ell$-module isomorphism. We can therefore identify λ-constacyclic codes of length N over $\mathbb{F}_\ell$ with ideals in $\frac{\mathbb{F}_\ell[x]}{< x^N - \lambda >}$. If $\lambda = 1$, these codes are just cyclic codes and for $\lambda = -1$, these codes are known as negacyclic codes. If N is coprime to the characteristic of $\mathbb{F}_\ell$, a λ-constacyclic code of length N over $\mathbb{F}_\ell$ is called a simple-root λ-constacyclic code, otherwise it is called a repeated root λ-constacyclic code. Simple root λ-constacyclic codes of a given length over a finite field have been extensively studied. In [1], Bakshi and Raka have studied simple root μ-constacyclic codes of length 2^n, $n \geq 1$ over a finite field $\mathbb{F}_q$, q being an odd prime power, with order of μ a power of 2. They, then extended the results to the repeated root λ-constacyclic codes of length $2^n p^s$ over $\mathbb{F}_q$ for any non zero λ in $\mathbb{F}_q$, via an isomorphism from $\frac{\mathbb{F}_q[x]}{< x^{2^n p^s} - \lambda >}$ to $\frac{\mathbb{F}_q[x]}{< x^{2^n p^s} - \Lambda >}$, where order of Λ is the highest power of 2 occurring in the order of λ and p is the characteristic of $\mathbb{F}_q$. In [4], Chen et al. characterized the polynomial generators of constacyclic codes of length $\ell^t p^s$, where p is the characteristic of the finite field and ℓ is a prime different from p. In [5, 6, 7], Dinh obtains constacyclic codes of length $2p^s, 3p^s$, and $4p^s$ over a finite field $\mathbb{F}_{p^m}$.

In the previous work [8], the authors have studied simple-root cyclic codes of length $p^n q$ over a finite field. In [9], self-dual and self-orthogonal simple-root negacyclic codes over a finite field have been studied. Hermitian self-orthogonal constacyclic codes over a finite field and some MDS Hermitian self-orthogonal constacyclic codes are obtained in [10].

In this paper, we study λ-constacyclic codes of length $p^n q^m$ over a finite field $\mathbb{F}_\ell$, where p, q are distinct odd primes and ℓ is an odd prime power coprime to p and q such that ℓ is a primitive root modulo p^n and $q \mid (\ell - 1)$. In Section 2, the generator polynomials and the number of these codes are found. In Section 3, we consider the dual codes of these constacyclic codes. Explicit expressions for the generator polynomials of the corresponding dual codes are given. In Section 4, the repeated root constacyclic codes of length $p^n q^m \ell^u$ over a finite field $\mathbb{F}_{\ell^v}$ and their duals are determined.

2. Simple Root Constacyclic Codes of Length $p^n q^m$

Let p, q be distinct odd primes and ℓ be an odd prime power, ℓ is a primitive root modulo p^n and $q \mid (\ell - 1)$. Let λ be a non zero element of $\mathbb{F}_\ell$. Then, the order of λ, denoted by $o(\lambda) = r$, divides $(\ell - 1)$. In this section, we consider simple root λ-constacyclic codes of length $p^n q^m$ over $\mathbb{F}_\ell$, for $m, n \geq 1$.

Lemma 1. *For p, q, ℓ, r as defined above, p does not divide r.*

Proof. If p divides r, since r divides $(\ell - 1)$, we see that p divides $(\ell - 1)$, which is a contradiction as ℓ is a primitive root modulo the odd prime p.

Write $r = q^e w$, $e \geq 0$, $q \nmid w$.

Lemma 2. *There exist unique* Λ *and* β *in* $\mathbb{F}_\ell^*$ *with* $o(\Lambda) = q^e$ *and order of* β *not divisible by* p *and* q, *such that* $\lambda = \Lambda\beta^{p^n q^m}$.

Proof. Write $\ell = q^d c + 1$, $d > 0$, $q \nmid c$. Observe that $o(\lambda) = q^e w$ is a divisor of $(\ell - 1)$. Therefore, $e \leq d$ and $w \mid c$. As $p^n q^{m+d}$ and c are coprime, there exist integers a and b such that

$$ca + p^n q^{m+d} b = 1,$$

so that $\lambda = \lambda^{ca + p^n q^{m+d} b} = \lambda^{ca}(\lambda^{q^d b})^{p^n q^m} = \Lambda\beta^{p^n q^m}$, where $\Lambda = \lambda^{ca}$ and $\beta = \lambda^{q^d b}$. As $o(\lambda) = q^e w$, $e \leq d$, β has order w which is not divisible by p and q. Also $\Lambda^{q^e} = \lambda^{q^e ca} = \lambda^{q^e w(\frac{c}{w})a} = 1$ (as $w \mid c$) and $\Lambda^{q^{e-1}} = \lambda^{q^{e-1} ca} \neq 1$ (since c and a are coprime to q). Thus $o(\Lambda) = q^e$.

To prove the uniqueness of Λ and β, suppose that there exist another Λ_1 and β_1 satisfying $\lambda = \Lambda_1\beta_1^{p^n q^m}$, where $o(\Lambda_1) = q^e$ and order of β_1 not divisible by p and q. Therefore, $\Lambda\beta^{p^n q^m} = \Lambda_1\beta_1^{p^n q^m}$ so that $\Lambda\Lambda_1^{-1} = \beta_1^{p^n q^m}\beta^{-p^n q^m}$. But $\Lambda\Lambda_1^{-1}$ has order a power of q and $\beta_1^{p^n q^m}$ $\beta^{-p^n q^m}$ has order coprime to q. Thus

$$\Lambda\Lambda_1^{-1} = \beta_1^{p^n q^m}\beta^{-p^n q^m} = 1,$$

giving us that $\Lambda = \Lambda_1$ and $\beta_1^{p^n q^m} = \beta^{p^n q^m}$. Also $\beta = \beta^{ca + p^n q^{m+d} b} = (\beta^{p^n q^m})^{q^d b} = (\beta_1^{p^n q^m})^{q^d b} = \beta_1^{ca + p^n q^{m+d} b} = \beta_1$. This proves the lemma. $\square$

Lemma 3. *Let* λ, Λ, *and* β *be as in Lemma* 2. *Then the map*

$$\Phi : \frac{\mathbb{F}_\ell[x]}{< x^{p^n q^m} - \lambda >} \to \frac{\mathbb{F}_\ell[x]}{< x^{p^n q^m} - \Lambda >}$$

given by $f(x) \mapsto f(\beta x)$ *is a ring isomorphism.*

Proof. Clearly, Φ is a ring homomorphism and is onto. Let $f(x), g(x) \in \mathbb{F}_\ell[x]$ be such that $\Phi(f(x)) = \Phi(g(x))$. Then $f(\beta x) = g(\beta x)$ $\bmod(x^{p^n q^m} - \Lambda)$, i.e., $f(\beta x) - g(\beta x) = (x^{p^n q^m} - \Lambda)h(x)$ for some $h(x) \in \mathbb{F}_\ell[x]$. Replacing x by $\beta^{-1}x$, we get

$$\begin{aligned} f(x) - g(x) &= (\beta^{-p^n q^m} x^{p^n q^m} - \Lambda)h(\beta^{-1}x) \\ &= \beta^{-p^n q^m}(x^{p^n q^m} - \Lambda\beta^{p^n q^m})h(\beta^{-1}x) \\ &= \beta^{-p^n q^m}(x^{p^n q^m} - \lambda)h(\beta^{-1}x) \equiv 0 \bmod(x^{p^n q^m} - \lambda). \end{aligned}$$

Thus $f(x) \equiv g(x) \bmod(x^{p^n q^m} - \lambda)$ giving us that Φ is one one, as required. □

Lemma 4. $< f(x) >$ *is a* Λ*-constacyclic code of length* $p^n q^m$ *over* $\mathbb{F}_\ell$ *if and only if* $< f(\beta^{-1}x) >$ *is a* λ*-constacyclic code of length* $p^n q^m$ *over* $\mathbb{F}_\ell$.

Proof. Follows from the isomorphism in Lemma 3. □

In view of Lemma 4, it is enough to consider Λ-constacyclic codes of length $p^n q^m$ over $\mathbb{F}_\ell$, where $o(\Lambda) = q^e$ for some $e \geq 0$.

Lemma 5. $(x^{p^n q^m} - \Lambda)$ *divides* $(x^{p^n q^{m+e}} - 1)$.

Proof. Let α be a root of $(x^{p^n q^m} - \Lambda)$. Then $\alpha^{p^n q^m} = \Lambda$ and order of Λ is q^e giving us that $(\alpha^{p^n q^m})^{q^e} = \alpha^{p^n q^{m+e}} = \Lambda^{q^e} = 1$. However,

$(x^{p^n q^m} - \Lambda)$ has simple roots over $\mathbb{F}_\ell$, it follows that $(x^{p^n q^m} - \Lambda)$ divides $(x^{p^n q^{m+e}} - 1)$. □

In order to find the generator polynomials of Λ-constacyclic codes, we need to find the factorization of $(x^{p^n q^m} - \Lambda)$. For any $0 \le s < p^n q^{m+e}$, let $C_s = \{s, s\ell, \ldots, s\ell^{N_s - 1}\}$ denote the ℓ-cyclotomic coset modulo $p^n q^{m+e}$ containing s, where N_s is the least positive integer such that $s\ell^{N_s} \equiv s(\bmod p^n q^{m+e})$. Let α be a primitive $p^n q^{m+e}$-th root of unity in some extension field of $\mathbb{F}_\ell$. We know that $M_s(x) = \prod_{i \in C_s}(x - \alpha^i)$ is the minimal polynomial of α^s over $\mathbb{F}_\ell$ and

$$x^{p^n q^{m+e}} - 1 = \prod_s M_s(x),$$

where s varies over the set of representatives of all the distinct ℓ-cyclotomic cosets modulo $p^n q^{m+e}$. Let t be an integer such that $q^t \parallel (p-1)$.

Lemma 6. *Let p, q, ℓ be as defined. Then order of ℓ modulo $p^i q^j$, $0 \le i < n$ and $0 \le j < m + e$ is $q^{\max\{0, j-d-t\}}\phi(p^i)$.*

Proof. ℓ is a primitive root modulo p^n so that order of ℓ modulo p^i, $0 \le i < n$ is $\phi(p^i)$. Also $\ell = q^d c + 1$, i.e., $\ell \equiv 1(\bmod q^d)$. Therefore, order of ℓ modulo q^j is $q^{\max\{0, j-d\}}$. By Lemma 2 [8], order of ℓ modulo $p^i q^j$ is $\operatorname{lcm}[\phi(p^i), q^{\max\{0, j-d\}}]$. As $q^t \parallel (p-1)$, $\operatorname{lcm}[\phi(p^i), q^{\max\{0, j-d\}}] = q^{\max\{0, j-d-t\}}\phi(p^i)$. □

Lemma 7. *There exists an integer* a, $1 < a < p^n q^{m+e}$, $\gcd(a, pq) = 1$ *such that* a *is a primitive root modulo* q^{m+e} *and order of* a *modulo* p^n *is* $\dfrac{\varphi(p^n)}{q^t}$.

Proof. Since $\gcd(p^n, q^{m+e}) = 1$, there exist integers u and v such that $p^n u + q^{m+e} v = 1$. Let g be a primitive root modulo q^{m+e}. Also, ℓ is a primitive root modulo p^n. Let $1 \leq a < p^n q^{m+e}$ be such that $a \equiv g p^n u + \ell^{q^t} q^{m+e} v (\bmod p^n q^{m+e})$. Observe that $a \equiv g p^n u (\bmod q^{m+e})$ $\equiv g(1 - q^{m+e} v) (\bmod q^{m+e}) \equiv g (\bmod q^{m+e})$ is a primitive root modulo q^{m+e}. Similarly, $a \equiv \ell^{q^t} (\bmod p^n)$ so that order of a modulo p^n is $\dfrac{\phi(p^n)}{q^t}$. □

Theorem 1. *Let* p, q, ℓ *be as defined and* a *be an integer as in Lemma* 7. *Then* ℓ*-cyclotomic cosets modulo* $p^n q^{m+e}$ *are given by*

$$C_0 = \{0\},$$

for $0 \leq i < n$, $0 \leq j \leq m + e$, $0 \leq k < \phi(q^{m+e-j-\gamma_j})$

$$C_{a^k p^i q^j} = \left\{ a^k p^i q^j, a^k p^i q^j \ell, \ldots, a^k p^i q^j \ell^{q^{\gamma_j} \phi(p^{n-i}) - 1} \right\},$$

and for $0 \leq j < m + e$, $0 \leq k < \phi(q^{m+e-j-\theta_j})$

$$C_{a^k p^n q^j} = \left\{ a^k p^n q^j, a^k p^n q^j \ell, \ldots, a^k p^n q^j \ell^{q^{\theta_j - 1}} \right\},$$

where $\gamma_j = \max\{0, m + e - j - d - t\}$ *and* $\theta_j = \max\{0, m + e - j - d\}$.

Proof. By Lemma 6, we have order of ℓ modulo $p^{n-i}q^{m+e-j}$ is $q^{\gamma_j}\phi(p^{n-i})$ for $0 \le i < n$, $0 \le j \le m+e$. Thus, $a^k p^i q^j \ell^{q^{\gamma_j}\phi(p^{n-i})} \equiv a^k p^i q^j (\bmod p^n q^{m+e})$ and the cyclotomic coset containing $a^k p^i q^j$ is $C_{a^k p^i q^j} = \left\{a^k p^i q^j, a^k p^i q^j \ell, \ldots, a^k p^i q^j \ell^{q^{\gamma_j}\phi(p^{n-i})-1}\right\}$. Also order of ℓ modulo q^{m+e-j} is θ_j so that $a^k p^n q^j \ell^{q^{\theta_j}} \equiv a^k p^n q^j (\bmod p^n q^{m+e})$ and the cyclotomic coset containing $a^k p^n q^j$ is $C_{a^k p^n q^j} = \left\{a^k p^n q^j, a^k p^n q^j \ell, \ldots, a^k p^n q^j \ell^{q^{\theta_j-1}}\right\}$. We show that these cosets are pairwise disjoint. For $0 \le i < n$, $0 \le j \le m+e$, $o \le k, h < \phi(q^{m+e-j-\gamma_j})$, let $a^k p^i q^j \in C_{a^h p^i q^j}$. Then there exists s, $0 \le s < q^{\gamma_j}\phi(p^{n-i})$ such that $a^k p^i q^j \equiv a^h p^i q^j \ell^s$ $(\bmod p^n q^{m+e})$, i.e., $a^{k-h} \equiv \ell^s (\bmod p^{n-i} q^{m+e-j})$. Thus $a^{k-h} \equiv \ell^s (\bmod p^{n-i})$ and $a \equiv \ell^{q^t} (\bmod p^{n-i})$ implying that $\ell^{q^t(k-h)} \equiv \ell^s (\bmod p^{n-i})$. Since ℓ is a primitive root modulo p^{n-i}, we get $q^t(k-h) \equiv s (\bmod \phi(p^{n-i}))$ so that q^t divides s. Write $s = q^t s'$. Now $a^{k-h} \equiv \ell^s (\bmod q^{m+e-j})$ or $a^{k-h} \equiv \ell^{q^t s'} (\bmod q^{m+e-j})$. Also a is a primitive root modulo q^{m+e-j} and ℓ has order q^{θ_j} modulo q^{m+e-j} so that order of ℓ^{q^t} modulo q^{m+e-j} is q^{γ_j}. Therefore, $\ell^{q^t} \equiv a^{\frac{\phi(q^{m+e-j})}{q^{\gamma_j}} r} (\bmod q^{m+e-j})$ for some integer r. Thus $a^{k-h} \equiv a^{\phi(q^{m+e-j-\gamma_j})rs'} (\bmod q^{m+e-j})$ giving us that $k-h \equiv \phi(q^{m+e-j-\gamma_j})rs' (\bmod \phi(q^{m+e-j}))$. Hence $\phi(q^{m+e-j-\gamma_j})$ divides $k-h$ for $0 \le k, h < \phi(q^{m+e-j-\gamma_j})$, showing that $k = h$. Similarly, for $0 \le j < m+e$ if $a^k p^n q^j \in C_{a^h p^n q^j}$ for some $0 \le k, h < \phi(q^{m+e-j-\theta_j})$. Then there exists s, $0 \le s < q^{\theta_j}$ such that $a^k p^n q^j \equiv a^h p^n q^j \ell^s (\bmod p^n$

q^{m+e}), i.e., $a^{k-h} \equiv \ell^s (\bmod q^{m+e-j})$. Again a is a primitive root modulo q^{m+e-j} and ℓ has order q^{θ_j} modulo q^{m+e-j} so that $\ell \equiv a^{\phi(q^{m+e-j-\theta_j})r}$ $(\bmod q^{m+e-j})$. Thus $a^{k-h} \equiv a^{\phi(q^{m+e-j-\theta_j})rs} (\bmod q^{m+e-j})$ giving us that $k - h \equiv \phi(q^{m+e-j-\theta_j})rs (\bmod \phi(q^{m+e-j}))$. Hence $\phi(q^{m+e-j-\theta_j})$ divides $(k-h)$ for $0 \le k, h < \phi(q^{m+e-j-\theta_j})$ implying $k = h$. Thus, the cyclotomic cosets are pairwise disjoint. Finally, these are all the cyclotomic cosets mod $p^n q^{m+e}$ because counting cardinalities

$$|C_0| + \sum_{i=0}^{n-1} \sum_{j=0}^{m+e} \sum_{k=0}^{\phi(q^{m+e-j-\gamma_j})-1} |C_{a^k p^i q^j}| + \sum_{j=0}^{m+e-1} \sum_{k=0}^{\phi(q^{m+e-j-\theta_j})-1} |C_{a^k p^n q^j}|$$

$$= 1 + \sum_{i=0}^{n-1} \sum_{j=0}^{m+e} \sum_{k=0}^{\phi(q^{m+e-j-\gamma_j})-1} q^{\gamma_j} \phi(p^{n-i}) + \sum_{j=0}^{m+e-1} \sum_{k=0}^{\phi(q^{m+e-j-\theta_j})-1} q^{\theta_j}$$

$$= 1 + \sum_{i=0}^{n-1} \phi(p^{n-i}) \sum_{j=0}^{m+e} q^{\gamma_j} \phi(q^{m+e-j-\gamma_j}) + \sum_{j=0}^{m+e-1} q^{\theta_j} \phi(q^{m+e-j-\theta_j})$$

$$= 1 + (p^n - 1) \left\{ \sum_{j=0}^{m+e} \phi(q^{m+e-j}) \right\} + \sum_{j=0}^{m+e-1} \phi(q^{m+e-j})$$

$$= 1 + (p^n - 1)(q^{m+e}) + (q^{m+e} - 1) = p^n q^{m+e}.$$

□

We choose α, a primitive $p^n q^{m+e}$-th root of unity in some extension field of $\mathbb{F}_\ell$ such that $\alpha^{p^n q^m} = \Lambda$. Thus,

$$(x^{p^n q^{m+e}} - 1) = M_0(x) \prod_{\substack{0 \le i < n \\ 0 \le j \le m+e \\ 0 \le k < \phi(q^{m+e-j-\gamma_j})}} M_{a^k p^i q^j}(x) \prod_{\substack{0 \le j \le m+e \\ 0 \le k < \phi(q^{m+e-j-\theta_j})}} M_{a^k p^n q^j}(x). \tag{2.1}$$

Theorem 2. *For any* s, $0 \le s < p^n q^{m+e}$, *the irreducible polynomial* $M_s(x)$ *divides* $(x^{p^n q^m} - \Lambda)$ *if and only if* $q^e \mid (s-1)$.

Proof. $M_s(x)$ divides $(x^{p^n q^m} - \Lambda)$ if and only if α^s is a root of $(x^{p^n q^m} - \Lambda)$, i.e., if and only if $\alpha^{p^n q^m s} = \Lambda$ or $\Lambda^s = \Lambda$ which is true if and only if $s \equiv 1(\bmod q^e)$ (as $o(\Lambda) = q^e$). □

Lemma 8. $M_{a^k p^i q^j}(x)$ *divides* $(x^{p^n q^m} - \Lambda)$ *if and only if* $j = 0$ *and* $a^k p^i \equiv 1(\bmod q^e)$.

Proof. By Theorem 2, $M_{a^k p^i q^j}(x)$ divides $(x^{p^n q^m} - \Lambda)$ if and only if $a^k p^i q^j \equiv 1(\bmod q^e)$ implying that $j = 0$ and $a^k p^i \equiv 1(\bmod q^e)$.

Let order of p modulo q^e be f. Write $\phi(q^e) = ff_1$. Also a is a primitive root modulo q^e so that $p \equiv a^{f_1 r}(\bmod q^e)$, for some integer r, $\gcd(r, f) = 1$.

Theorem 3. *The factorization of* $(x^{p^n q^m} - \Lambda)$ *over* $\mathbb{F}_\ell$ *into monic irreducible factors is given by*

(i) *For* $e = 0$,

$$(x^{p^n q^m} - \Lambda) = (x^{p^n q^m} - 1) = M_0(x) \prod_{i=0}^{n-1} \prod_{j=0}^{m} \prod_{k \in S_{i,j}} M_{a^k p^i q^j}(x) \prod_{j=0}^{m-1} \prod_{k \in S_{n,j}} M_{a^k p^n q^j}(x),$$

where for $0 \le i < n$, $0 \le j \le m$,

$$S_{i,j} = \left\{s,\ 0 \le s < \phi(q^{\min\{m-j,\, d+t\}})\right\}, \tag{2.2}$$

and for $0 \le j < m$,

$$S_{n,j} = \left\{s,\ 0 \le s < \phi(q^{\min\{m-j,\, d\}})\right\}. \tag{2.3}$$

(ii) *For* $1 \leq e \leq t$,

$$(x^{p^n q^m} - \Lambda) = \prod_{i=0}^{m} \prod_{k \in S_i} M_{a^k p^i}(x),$$

where for $0 \leq i < n$,

$$S_i = \left\{ s\phi(q^e);\ 0 \leq s < q^{\min\{m, d+t-e\}} \right\}, \tag{2.4}$$

and

$$S_n = \left\{ s\phi(q^e);\ 0 \leq s < q^{\min\{m, d-e\}} \right\}. \tag{2.5}$$

(iii) *For* $e > t$,

$$(x^{p^n q^m} - \Lambda) = \prod_{i=0}^{n} \prod_{k \in S'_i} M_{a^k p^i}(x),$$

where for $0 \leq i < n$,

$$S'_i = \left\{ f_1(sf - ir);\ 0 \leq s < q^{\min\{m, d+t-e\}} \right\} \bmod \phi(q^{m+e-\gamma_0}), \tag{2.6}$$

and

$$S'_n = \left\{ f_1(sf - nr);\ 0 \leq s < q^{\min\{m, d-e\}} \right\} \bmod \phi(q^{m+e-\theta_0}). \tag{2.7}$$

Proof. (i) If $e = 0$, the result follows from (2.1).

(ii) If $1 \leq e \leq t$, we have $p \equiv 1(\bmod q^e)$. Thus, Lemma 8 implies that $M_{a^k p^i}(x)$ divides $(x^{p^n q^m} - \Lambda)$ if and only if $a^k \equiv 1(\bmod q^e)$. Also a is a primitive root modulo q^e so that $k \equiv 0(\bmod \phi(q^e))$. Thus, $k = s\phi(q^e)$ for $0 \leq s < q^{m-\gamma_0}$ in case $0 \leq i < n$ and $k = s\phi(q^e)$ for $0 \leq s < q^{m-\theta_0}$ in case $i = n$. Thus in both the cases, $M_{a^k p^i}(x)$ divides $(x^{p^n q^m} - \Lambda)$ if and only if $k \in S_i$.

(iii) If $e > t$, we have $p \equiv a^{f_1 r}(\bmod q^e)$, where $f_1 = \dfrac{\phi(q^e)}{f}$ and f is the order of p modulo q^e. Thus $a^k p^i \equiv 1(\bmod q^e)$ if and only if $a^k a^{f_1 ri} \equiv 1(\bmod q^e)$, i.e., $k + if_1 r \equiv 0(\bmod \phi(q^e))$ or $k \equiv if_1 r(\bmod ff_1)$. Thus, $M_{a^k p^i}(x)$ divides $(x^{p^n q^m} - \Lambda)$ if and only if $k \in S_i'$.

Theorem 4. *Let p, q, ℓ be as defined and Λ be a non zero element of $\mathbb{F}_\ell$ with $o(\Lambda) = q^e$. The generator polynomials of Λ-constacyclic codes of length $p^n q^m$ over $\mathbb{F}_\ell$ are given by*:

(i) *For $e = 0$, the Λ-constacyclic codes of length $p^n q^m$ over $\mathbb{F}_\ell$ are given by*

$$\left\langle (M_0(x))^{\delta_0} \prod_{i=0}^{n-1} \prod_{j=0}^{m+e} \prod_{k \in S_{i,j}} (M_{a^k p^i q^j}(x))^{\delta_{i,j,k}} \prod_{j=0}^{m+e-1} \prod_{k \in S_{n,j}} (M_{a^k p^n q^j}(x))^{\delta_{n,j,k}} \right\rangle,$$

where $S_{i,j}$ is as defined in (2.2) *and* (2.3).

(ii) *For $1 \le e \le t$, the Λ-constacyclic codes of length $p^n q^m$ over $\mathbb{F}_\ell$ are given by*

$$\left\langle \prod_{i=0}^{n} \prod_{k \in S_i} (M_{a^k p^i}(x))^{\delta_{i,k}} \right\rangle,$$

where S_i is as in (2.4) *and* (2.5).

(iii) *For $e > t$, the Λ-constacyclic codes of length $p^n q^m$ over $\mathbb{F}_\ell$ are given by*

$$\left\langle \prod_{i=0}^{n} \prod_{k \in S_i'} (M_{a^k p^i}(x))^{\delta_{i,k}} \right\rangle,$$

where S_i' is as in (2.6) *and* (2.7).

Here δ_0, $\delta_{i,j,k}$, and $\delta_{i,k}$ takes value 0 *or* 1 *for each relevant i, j, k.*

Theorem 5. *There are precisely* 2^{ζ} *number of* λ*-constacyclic codes of length* $p^n q^m$ *over* $\mathbb{F}_\ell$, *where*

(i) *For* $e = 0$,

$$\zeta = \begin{cases} q^m(n+1), & m \le d, \\ q^d(nq^{m-d}+1) + \phi(q^d)(m-d), & d < m \le d+t, \\ q^d(nq^t+1) + \phi(q^d)\{m-d+nq^t(m-d-t)\}, & m > d+t. \end{cases}$$

(ii) *For* $e \ge 1$,

$$\zeta = \begin{cases} q^m(n+1), & m \le d-e, \\ q^{d-e}(nq^{m-d+e}+1), & d-e < m \le d-e+t, \\ q^{d-e}(nq^t+1), & m > d-e+t. \end{cases}$$

3. Dual Codes

In this section, we investigate the dual codes of Λ-constacyclic codes of length $p^n q^m$ over $\mathbb{F}_\ell$. Let C be a Λ-constacyclic code of length $p^n q^m$ over $\mathbb{F}_\ell$ generated by $g(x)$. Let $h(x) = \dfrac{(x^{p^n q^m} - \Lambda)}{g(x)}$ be the check polynomial. It is well known that the dual code $C^{\perp}$ of C is a Λ^{-1}-constacyclic code of length $p^n q^m$ over $\mathbb{F}_\ell$ and has generator polynomial $h^*(x)$, where $h^*(x) = h(0)^{-1} x^{\deg h(x)} h(\frac{1}{x})$ is the reciprocal polynomial of $h(x)$. Note that $h^*(x)$ is a monic polynomial and divides $(x^{p^n q^m} - \Lambda^{-1})$.

Lemma 9. *If C_s denotes the ℓ-cyclotomic coset mod $p^n q^{m+e}$ containing s, then*

$$-1 \in C_{a^{\frac{\phi(q^{m+e-\gamma_0})}{2}}}.$$

Proof. Let $-1 \in C_{a^k}$ for some k, $0 \le k < \phi(q^{m+e-\gamma_0})$. Then there exists an integer s, $0 \le s < q^{\gamma_0}\phi(p^n)$ such that $a^k \ell^s \equiv -1 (\text{mod } p^n q^{m+e})$. Thus $a^k \ell^s \equiv -1 (\text{ mod } p^n)$ and $a^k \ell^s \equiv -1 (\text{ mod } p^{m+e})$. Since $a \equiv \ell^t$ $(\text{ mod } p^n)$ we get $\ell^{kq^t+s} \equiv -1 (\text{ mod } p^n)$ or $\ell^{2(kq^t+s)} \equiv 1 (\text{ mod } p^n)$. Since ℓ is a primitive root modulo p^n, we have $2(kq^t + s) \equiv 0 (\text{ mod } \phi(p^n))$, i.e., $s \equiv -kq^t (\text{ mod } \frac{\phi(p^n)}{2})$ giving us that s is divisible by q^t. Write $s = q^t s'$. Also $a^k \ell^s \equiv -1 (\text{ mod } q^{m+e})$, i.e., $a^k \ell^{q^t s'} \equiv -1 (\text{ mod } q^{m+e})$. Now a is a primitive root modulo q^{m+e} and ℓ has order $q^{\theta_0} \text{ mod } q^{m+e}$, so that ℓ^{q^t} has order $q^{\gamma_0} \text{ mod } q^{m+e}$. Thus $\ell^t \equiv a^{\phi(q^{m+e-\gamma_0})r} (\text{ mod } q^{m+e})$ for some integer r. Hence $a^k a^{\phi(q^{m+e-\gamma_0})rs'} \equiv -1 (\text{ mod } q^{m+e})$ or $a^{2(k+\phi(q^{m+e-\gamma_0})rs')} \equiv 1 (\text{ mod } q^{m+e})$ giving us that $k \equiv -\phi(q^{m+e-\gamma_0})rs'$ $(\text{ mod } \frac{\phi(q^{m+e})}{2})$. Therefore $\frac{\phi(q^{m+e-\gamma_0})}{2}$ divides k for $0 \le k < \phi(q^{m+e-\gamma_0})$ showing us that $k = 0$ or $k = \frac{\phi(q^{m+e-\gamma_0})}{2}$. If $k = 0$, then $\ell^s \equiv -1 (\text{ mod } p^n q^{m+e})$ for some s. Thus $\ell^s \equiv -1 (\text{ mod } q)$, whereas $\ell \equiv 1 (\text{ mod } q)$ and q is an odd prime giving us a contradiction. Thus $k \ne 0$ and $-1 \in C_{\frac{\phi(q^{m+e-\gamma_0})}{2}}$. □

Lemma 10. *For* $0 \le i < n$, $0 \le j \le m + e$, $0 \le k < \phi(q^{m+e-j-\gamma_j})$,

$$-C_{a^k p^i q^j} = C_{a^{k'} p^i q^j},$$

where

$$k' = \begin{cases} k + \dfrac{\phi(q^{m+e-j-\gamma_j})}{2}; & 0 \le k < \dfrac{\phi(q^{m+e-j-\gamma_j})}{2}, \\ k - \dfrac{\phi(q^{m+e-j-\gamma_j})}{2}; & \dfrac{\phi(q^{m+e-j-\gamma_j})}{2} \le k < \phi(q^{m+e-j-\gamma_j}), \end{cases} \tag{3.1}$$

and for $0 \le j \le m + e$, $0 \le k < \phi(q^{m+e-j-\theta_j})$

$$-C_{a^k p^n q^j} = C_{a^{k''} p^n q^j},$$

where

$$k'' = \begin{cases} k + \dfrac{\phi(q^{m+e-j-\theta_j})}{2}; & 0 \le k < \dfrac{\phi(q^{m+e-j-\theta_j})}{2}, \\ k - \dfrac{\phi(q^{m+e-j-\theta_j})}{2}; & \dfrac{\phi(q^{m+e-j-\theta_j})}{2} \le k < \phi(q^{m+e-j-\theta_j}). \end{cases} \tag{3.2}$$

Remark 1. Let C be a Λ-constacyclic code of length $p^n q^m$ over $\mathbb{F}_\ell$ with generator polynomial $g(x) = \prod_s (M_s(x))^{\delta_s}$, where s takes the relevant values as given in Theorem 4. Then $h(x) = \prod_s (M_s(x))^{1-\delta_s}$ and $h^*(x) = \prod_s (M_s^*(x))^{1-\delta_s} = \prod_s (M_{-s}(x))^{1-\delta_s} = \prod_s (M_s(x))^{1-\delta_{-s}}$. Thus, the dual code $C^\perp$ is a Λ^{-1}-constacyclic code of length $p^n q^m$ over $\mathbb{F}_\ell$ with generator polynomial $h^*(x) = \prod_s (M_s(x))^{1-\delta_{-s}}$.

Theorem 6. *Let C be a Λ-constacyclic code of length $p^n q^m$ over $\mathbb{F}_\ell$ with generator polynomial as given in Theorem 4. Then the dual code $C^\perp$ is a Λ^{-1}-constacyclic code of length $p^n q^m$ over $\mathbb{F}_\ell$ with generator polynomial $h^*(x)$ given by the following*:

(i) *For* $e = 0$,

$$h^*(x) = (M_0(x))^{1-\delta_0} \prod_{i=0}^{n-1} \prod_{j=0}^{m+e} \prod_{k \in S_{i,j}} (M_{a^k p^i q^j}(x))^{1-\delta_{i,j,k'}} \prod_{j=0}^{m+e-1} \prod_{k \in S_{n,j}} (M_{a^k p^n q^j}(x))^{1-\delta_{n,j,k''}};$$

(ii) *For* $1 \leq e \leq t$,

$$h^*(x) = \prod_{i=0}^{n-1} \prod_{k \in S_i} (M_{a^k p^i}(x))^{1-\delta_{i,k'}} \prod_{k \in S_n} (M_{a^k p^n}(x))^{1-\delta_{n,k''}};$$

(iii) *For* $e > t$,

$$h^*(x) = \prod_{i=0}^{n-1} \prod_{k \in S_i'} (M_{a^k p^i}(x))^{1-\delta_{i,k'}} \prod_{k \in S_n'} (M_{a^k p^n}(x))^{1-\delta_{n,k''}},$$

where k' *and* k'' *are as in* (3.1) *and* (3.2), *respectively.*

Proof. Follows easily from Lemma 10 and Remark 1. □

Now we consider a λ-constacyclic code of length $p^n q^m$ over $\mathbb{F}_\ell$, where $o(\lambda) = q^e w$, $q \nmid w$. We have seen that λ-constacyclic codes of length $p^n q^m$ over $\mathbb{F}_\ell$ are isomorphic to Λ-constacyclic codes of length $p^n q^m$ over $\mathbb{F}_\ell$, where $\lambda = \Lambda\beta^{p^n q^m}$, $o(\Lambda) = q^e$, under the mapping

$$\Phi : \frac{\mathbb{F}_\ell[x]}{< x^{p^n q^m} - \lambda >} \to \frac{\mathbb{F}_\ell[x]}{< x^{p^n q^m} - \Lambda >},$$

given by $f(x) \mapsto f(\beta x)$. Moreover, by Lemma 4, $< f(x) >$ is a Λ-constacyclic code of length $p^n q^m$ over $\mathbb{F}_\ell$ if and only if $< f(\beta^{-1} x) >$ is a λ-constacyclic code of length $p^n q^m$ over $\mathbb{F}_\ell$.

Theorem 7. *For any* Λ*-constacyclic code of length* $p^n q^m$ *over* $\mathbb{F}_\ell$

$$(\Phi^{-1}(C))^\perp = \Phi^{-1}(C^\perp).$$

Proof. Let C be a Λ-constacyclic code of length $p^n q^m$ over $\mathbb{F}_\ell$ generated by $g(x)$. Write $g(x)h(x) = x^{p^n q^m} - \Lambda$. Then $g(\beta^{-1}x)h(\beta^{-1}x) = \beta^{-p^n q^m}(x^{p^n q^m} - \lambda)$ so that $\Phi^{-1}(C)$ is generated by $g(\beta^{-1}x)$. Thus, $(\Phi^{-1}(C))^\perp$ is generated by $h^*(\beta^{-1}x)$, i.e.,

$$(\Phi^{-1}(C))^\perp =< h^*(\beta^{-1}x) > . \tag{3.3}$$

On the other hand, $C^\perp =< h^*(x) >$. By Lemma 3, we obtain that

$$\Phi^{-1}(C^\perp) =< h^*(\beta^{-1}x) > . \tag{3.4}$$

The result follows from (3.3) and (3.4). □

Example 1. Take $p = 13$, $q = 3$, $\ell = 7$, $m = 2$, and $n = 1$. Then $d = 1$, $t = 1$. Thus $0 \le e \le 1$ and $a = 83$.

(i) For $e = 0$, $\Lambda = 1$, we have

$$(x^{117} - 1) = M_0(x)\prod_{j=0}^{2}\prod_{k=0}^{\phi(3^{2-j})-1} M_{83^k * 3^j}(x)\prod_{j=0}^{1}\prod_{k=0}^{\phi(3)-1} M_{83^k * 13 * 3^j}(x),$$

where

$M_0(x) = x - 1,$

$M_1(x) = x^{12} + 2x^{11} + x^{10} - x^8 + 4x^6 + 4x^5 + 3x^4 + 5x^3 - x^2 - x + 2,$

$M_{83}(x) = x^{12} - x^{11} + 5x^10 - x^9 + 3x^8 + x^7 + 2x^6 + 5x^4 + x^2 + 4x + 4,$

$M_{83^2}(x) = M_{103} = x^{12} + 4x^{11} + 4x^{10} + 5x^8 + 4x^6 + x^5 + 5x^4 + 5x^3 + 5x^2 + 3x + 2,$

$M_{83^3}(x) = M_8(x) = x^{12} + 3x^{11} + 3x^{10} - x^9 + 5x^8 + 2x^7 + 2x^6 + 3x^4 + 4x^2 + x + 4,$

$M_{83^4}(x) = M_{79}(x) = x^{12} + x^{11} + 2x^{10} + 3x^8 + 4x^6 + 2x^5 - x^4 + 5x^3 + 3x^2 + 5x + 2,$

$$M_{83^5}(x) = M_5(x) = x^{12} + 5x^{11} - x^{10} - x^9 - x^8 + 4x^7 + 2x^6 - x^4 + 2x^2 + 2x + 4,$$

$$M_3(x) = x^{12} + 2x^{11} + 4x^{10} + x^9 + 2x^8 + 4x^7 + x^6 + 2x^5 + 4x^4 + x^3 + 2x^2 + 4x + 1,$$

$$M_{3*83}(x) = M_{15} = x^{12} + 4x^{11} + 2x^{10} + x^9 + 4x^8 + 2x^7 + x^6 + 4x^5 + 2x^4 + x^3 + 4x^2 + 2x + 1,$$

$$M_9(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

$$M_{13}(x) = x^3 + 5,$$

$$M_{83*13}(x) = M_{26}(x) = x^3 + 3,$$

$$M_{13*3}(x) = M_{39}(x) = x + 5,$$

$$M_{13*3*83}(x) = M_{78}(x) = x + 3.$$

(ii) For $e = 1$, $\Lambda = 2, 4$. For $\Lambda = 2$, we have

$$(x^{117} - 2) = M_1^{(2)}(x) M_{83^2}^{(2)}(x) M_{83^4}^{(2)}(x) M_{13}^{(2)}(x),$$

where

$$M_1^{(2)}(x) = x^{36} + 2x^{33} + x^{30} - x^{24} + 4x^{18} + 4x^{15} + 3x^{12} + 5x^9 - x^6 - x^3 + 2,$$

$$M_{83^2}^{(2)}(x) = M_{220}(x) = x^{36} + 4x^{33} + 4x^{30} + 5x^{24} + 4x^{18} + x^{15} + 5x^{12} + 5x^9 + 5x^6 + 3x^3 + 2,$$

$$M_{83^4}^{(2)}(x) = M_{313}(x) = x^{36} + x^{33} + 2x^{30} + 3x^{24} + 4x^{18} + 2x^{15} - x^{12} + 5x^9 + 3x^6 + 5x^3 + 2,$$

$$M_{13}^{(2)}(x) = x^9 + 5.$$

For $\Lambda = 4$, we have

$$(x^{117} - 4) = M_1^{(4)}(x) M_{83^2}^{(4)}(x) M_{83^4}^{(4)}(x) M_{13}^{(4)}(x),$$

where

$$M_1^{(4)}(x) = x^{36} + 5x^3 - x^{30} - x^{27} - x^{24} + 4x^{21} + 2x^{18} - x^{12} + 2x^6 + 2x^3 + 4,$$

$$M_{83^2}^{(4)}(x) = M_{220}^{(4)}(x) = x^{36} - x^{33} + 5x^{30} - x^{27} + 3x^{24} + x^{21} + 2x^{18} + 5x^{12} + x^6 + 4x^3 + 4,$$

$$M_{83^4}^{(4)}(x) = M_{313}^{(4)}(x) = x^{36} + 3x^{33} + 3x^{30} - x^{27} + 5x^{24} + 2x^{21} + 2x^{18} + 3x^{12} + 4x^6 + x^3 + 4,$$

$$M_{13}^{(4)}(x) = x^9 + 3.$$

Thus, the following table gives the number and the generator polynomials of the λ-constacyclic codes of length 117 over $\mathbb{F}_7$:

λ	$o(\lambda)$	Λ	β	e	2^{ζ}	$g(x)$
1	1	1	1	0	2^{14}	$(M_0(x))^{\delta_0}\prod_{j=0}^{2}\prod_{k=0}^{\phi(3^{2-j})-1}(M_{83^k*3j}(x))^{\delta_{0,j,k}}\prod_{j=0}^{1}\prod_{k=0}^{\phi(3)-1}(M_{83^k*13*3j}(x))^{\delta_{1,j,k}}$
2	3	2	1	1	2^4	$\left(M_1^{(2)}(x)\right)^{\delta_{0,0}}\left(M_{83^2}^{(2)}(x)\right)^{\delta_{0,2}}\left(M_{83^4}^{(2)}(x)\right)^{\delta_{0,4}}\left(M_{13}^{(2)}(x)\right)^{\delta_{1,0}}$
3	6	4	-1	1	2^4	$\left(M_1^{(4)}(-x)\right)^{\delta_{0,0}}\left(M_{83^2}^{(4)}(-x)\right)^{\delta_{0,2}}\left(M_{83^4}^{(4)}(-x)\right)^{\delta_{0,4}}\left(M_{13}^{(4)}(-x)\right)^{\delta_{1,0}}$
4	3	4	1	1	2^4	$\left(M_1^{(4)}(x)\right)^{\delta_{0,0}}\left(M_{83^2}^{(4)}(x)\right)^{\delta_{0,2}}\left(M_{83^4}^{(4)}(x)\right)^{\delta_{0,4}}\left(M_{13}^{(4)}(x)\right)^{\delta_{1,0}}$
5	6	2	-1	1	2^4	$\left(M_1^{(2)}(-x)\right)^{\delta_{0,0}}\left(M_{83^2}^{(2)}(-x)\right)^{\delta_{0,2}}\left(M_{83^4}^{(2)}(-x)\right)^{\delta_{0,4}}\left(M_{13}^{(2)}(-x)\right)^{\delta_{1,0}}$
6	2	1	-1	0	2^{14}	$(M_0(-x))^{\delta_0}\prod_{j=0}^{2}\prod_{k=0}^{\phi(3^{2-j})-1}(M_{83^k*3j}(-x))^{\delta_{0,j,k}}\prod_{j=0}^{1}\prod_{k=0}^{\phi(3)-1}(M_{83^k*13*3j}(-x))^{\delta_{1,j,k}}$

where $\delta_{i,j,k}$, $\delta_{i,k}$ takes value 0 or 1.

4. Repeated Root Constacyclic Codes of Length $p^n q^m \ell^u$ over $\mathbb{F}_{\ell^v}$

In this section, we consider repeated root constacyclic codes of length $p^n q^m \ell^u$ over $\mathbb{F}_{\ell^v}$. Let $\lambda \in \mathbb{F}_{\ell^v}^*$ be an arbitrary element with $o(\lambda) = q^e w$. Then there exist unique Λ and β in $\mathbb{F}_{\ell^v}^*$ with $o(\Lambda) = q^e$ and $o(\beta)$ not divisible by p and q, such that $\lambda = \Lambda\beta^{p^n q^m}$ (see Lemma 1). Also $\gcd(\ell, \ell^v - 1) = 1$, so that there exists a unique integer b such that $b\ell^u \equiv 1(\bmod(\ell^v - 1))$, i.e., $b\ell^u \equiv 1(\bmod q^{d'})$, for $q^{d'} \| (\ell^v - 1)$. Now $\gcd(b, q) = 1$. Therefore, the order of Λ^b is equal to the order of Λ in $\mathbb{F}_{\ell^v}$. Also if $v = 1$, then $b = 1$.

Lemma 11. *Let λ, Λ, and β be as defined above. Then the map*

$$\Phi : \frac{\mathbb{F}_{\ell^v}[x]}{< x^{p^n q^m \ell^u} - \lambda >} \to \frac{\mathbb{F}_{\ell^v}[x]}{< x^{p^n q^m \ell^u} - \Lambda >}$$

given by

$$f(x) \mapsto f(\beta^b x)$$

is a ring isomorphism.

Proof. Similar to Lemma 3. □

Lemma 12. *$< f(x) >$ is a Λ-constacyclic code of length $p^n q^m \ell^u$ over $\mathbb{F}_{\ell^v}$ if and only if $< f(\beta^{-b} x) >$ is a λ-constacyclic code of length $p^n q^m \ell^u$ over $\mathbb{F}_{\ell^v}$.*

Theorem 8. *With notations as above, let*

$$(x^{p^n q^m} - \Lambda^b) = f_1(x) f_2(x) \cdots f_s(x)$$

be the factorization of $x^{p^n q^m} - \Lambda^b$ *into irreducible factors over* $\mathbb{F}_{\ell^v}$ *given in Theorem* 4. *Then*

$$\left\langle (f_1(\beta^{-b}x))^{\epsilon_1}(f_2(\beta^{-b}x))^{\epsilon_2}\cdots(f_s(\beta^{-b}x))^{\epsilon_s}\right\rangle,$$

$$0 \le \epsilon_i \le \ell^u \text{ for each } i, \quad 1 \le i \le s,$$

are precisely all the repeated-root λ*-constacyclic codes of length* $p^n q^m \ell^u$ *over* $\mathbb{F}_{\ell^v}$.

Proof. As $f(x)$ varies over all the divisors of $(x^{p^n q^m \ell^u} - \Lambda)$ over $\mathbb{F}_{\ell^v}$, $< f(x) >$ are precisely all the Λ-constacyclic codes of length $p^n q^m \ell^u$ over $\mathbb{F}_{\ell^v}$. Now,

$$x^{p^n q^m \ell^u} - \Lambda = x^{p^n q^m \ell^u} - \Lambda^{b\ell^u} = \left(x^{p^n q^m} - \Lambda^b\right)^{\ell^u}$$

$$= (f_1(x)f_2(x)\cdots f_s(x))^{\ell^u} = (f_1(x))^{\ell^u}(f_2(x))^{\ell^u}\cdots(f_s(x))^{\ell^u}.$$

Thus, $\langle (f_1(x))^{\epsilon_1}(f_2(x))^{\epsilon_2}\cdots(f_s(x))^{\epsilon_s}\rangle$, $0 \le \epsilon_i \le \ell^u$, $1 \le i \le s$ are precisely all the repeated-root Λ-constacyclic codes of length $p^n q^m \ell^u$ over $\mathbb{F}_{\ell^v}$. The theorem now follows from Lemma 12. □

Corollary 1. *There are precisely* $(\ell^u + 1)^{\zeta}$ *number of repeated root* λ*-constacyclic codes of length* $p^n q^m \ell^u$ *over* $\mathbb{F}_{\ell^v}$, *where*

(i) *For* $e = 0$,

$$\zeta = \begin{cases} q^m(n+1), & m \le d', \\ q^{d'}(nq^{m-d'}+1) + \phi(q^{d'})(m-d'), & d' < m \le d'+t, \\ q^{d'}(nq^t+1) + \phi(q^{d'})\{m-d'+nq^t(m-d'-t)\}, & m > d'+t. \end{cases}$$

(ii) *For* $e \geq 1$,

$$\zeta = \begin{cases} q^m(n+1), & m \leq d' - e, \\ q^{d'-e}(nq^{m-d'+e}+1), & d' - e < m \leq d' - e + t, \\ q^{d'-e}(nq^t+1), & m < d' - e + t. \end{cases}$$

Theorem 9. *Let C be a Λ-constacyclic code of length $p^n q^m \ell^u$ over $\mathbb{F}_{\ell^v}$ with generator*

$$\prod_{i=1}^{s} (f_i(x))^{\epsilon_i}, \quad 0 \leq \epsilon_i \leq \ell^u.$$

Then $C^\perp$ is a Λ^{-1}-constacyclic code $p^n q^m \ell^u$ over $\mathbb{F}_{\ell^v}$ generated by

$$\prod_{i=1}^{s} (f_i^*(x))^{\ell^u - \epsilon_i}.$$

Let C be a Λ-constacyclic code of length $p^n q^m \ell^u$ over $\mathbb{F}_{\ell^v}$ generated by

$$g(x) = \prod_{i=1}^{s} (f_i(x))^{\epsilon_i}, \quad 0 \leq \epsilon_i \leq \ell^u.$$

As $g(x)h(x) = x^{p^n q^m \ell^u} - \Lambda$, so that $C^\perp =< h^*(x) >$. Let Φ be as defined in Lemma 11, then $\Phi^{-1}(C^\perp) =< h^*(\beta^{-b}x) >$. Also, $g(\beta^{-b}x)h(\beta^{-b}x) = \beta^{-bp^n q^m \ell^u}(x^{p^n q^m \ell^u} - \lambda)$ and $\Phi^{-1}(C) =< g(\beta^{-b}x) >$, so that $(\Phi^{-1}(C))^\perp =< h^*(\beta^{-b}x) >$. Consequently, we have proved the following:

Theorem 10. $(\Phi^{-1}(C))^\perp = \Phi^{-1}(C^\perp)$ *for all Λ-constacyclic codes C of length $p^n q^m \ell^u$ over $\mathbb{F}_{\ell^v}$.*

References

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

[2] T. Blackford, Negacyclic duadic codes, Finite Fields Appl. 14(4) (2008), 930-943.

[3] T. Blackford, Isodual constacyclic codes, Finite Fields Appl. 24 (2013), 29-44.

[4] Bocong Chen, Yun Fan, Liren Lin and Hongwei Liu, Constacyclic codes over finite fields, Finite Fields Appl. 18(6) (2012), 1217-1231.

[5] H. Q. Dinh, Repeated-root constacyclic codes of length $2p^s$, Finite Fields Appl. 18(1) (2012), 133-143.

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

[7] H. Q. Dinh, On repeated-root constacyclic codes of length $4p^s$, Asian-European J. Math. 06, 1350020 (2013), [25 pages].

[8] A. Sahni and P. T. Sehgal, Minimal cyclic codes of length $p^n q$, Finite Fields Appl. 18 (2012), 1017-1036.

[9] A. Sahni and P. T. Sehgal, Enumeration of self dual and self orthogonal negacyclic codes over finite fields, Advances in Mathematics of Communications 9(4) (2015) 437-447.

[10] A. Sahni and P. T. Sehgal, Hermitian self-orthogonal constacyclic codes over finite fields, Journal of Discrete Mathematics 985387 (2014), [7 pages].

■