SIMPLE-ROOT NEGACYCLIC CODES OF LENGTH
$2p^n\ell^m$ OVER A FINITE FIELD

ANURADHA SHARMA

Abstract. Let $p$, $\ell$ be distinct odd primes, $q$ be an odd prime power with $\gcd(q, p) = \gcd(q, \ell) = 1$, and $m$, $n$ be positive integers. In this paper, we determine all self-dual, self-orthogonal and complementary-dual negacyclic codes of length $2p^n\ell^m$ over the finite field $\mathbb{F}_q$ with $q$ elements. We also illustrate our results with some examples.

1. Introduction

Berlekamp [4, 5] introduced negacyclic codes over the finite field $\mathbb{F}_p$ with $p$ elements, where $p \geq 5$ is a prime. He also designed a decoding algorithm that can correct errors having Lee weight at most $\left\lfloor \frac{p-1}{2} \right\rfloor$. Later, Kelsch and Green [14] constructed 2-error-correcting negacyclic codes of length $\frac{3m-1}{2}$ and redundancy $2m$ over $\mathbb{F}_3$. Since then, negacyclic codes have been an interesting object of study for a long time.

Two extensively studied subclasses of negacyclic codes are that of self-dual and self-orthogonal negacyclic codes, which have beautiful underlying algebraic structures, have nice connections with unimodular lattices and the theory of Jacobi forms, and are more practical to implement. Thus the problem of determination of all self-dual and self-orthogonal negacyclic codes over finite fields is of great interest. Below we provide a brief survey of the results known in this direction.

Blackford [6] proved that simple-root self-dual negacyclic codes of length $2^am$ ($a \geq 1$, $m$ odd) over $\mathbb{F}_q$ exist if and only if $q \not\equiv -1 \pmod{2^{a+1}}$. Dinh [7, 8, 9, 10, 11] explored the existence of all self-dual cyclic and negacyclic codes of length $mp^r$ ($r \geq 1$) over the finite field $\mathbb{F}_{p^n}$ ($p$ is a prime), where $m \in \{1, 2, 3, 4, 6\}$ is an integer coprime to $p$. Guenda and Gulliver [12] examined all repeated-root cyclic and negacyclic codes of length $mp^r$ ($r \geq 1$) over $\mathbb{F}_{p^n}$, where $p$ is a prime and $m \geq 1$ is an integer with $\gcd(m, p) = 1$. When $p$ is odd, they derived necessary and sufficient conditions for the existence of self-dual negacyclic codes of length $mp^r$ over $\mathbb{F}_{p^n}$. When $m = 2m'$ with $m'$ odd,
they characterized these codes in terms of their polynomial generators, which provides simple conditions on the existence of self-dual negacyclic codes and generalizes the work of Dinh [8]. Later, Bakshi and Raka [2] listed all self-dual negacyclic codes of $2^n$ ($n \geq 1$) over $\mathbb{F}_q$, where $q$ is an odd prime power. In another paper, Bakshi and Raka [3] listed all self-dual and self-orthogonal negacyclic codes of length $2p^n$ ($n \geq 1$) over $\mathbb{F}_q$, where $p$ is an odd prime and $q$ is an odd prime power coprime to $p$. Extending this work, Sharma [19] listed all self-dual and self-orthogonal negacyclic codes of length $2^m p^n$ over $\mathbb{F}_q$, where $p$ is an odd prime power coprime to $p$, and $m,n$ are positive integers. In a subsequent work, Sharma [20] listed all self-orthogonal and complementary-dual cyclic codes of length $p^n \ell^m$ over $\mathbb{F}_q$, where $p, \ell$ are distinct odd primes, $q$ is an odd prime power with $\gcd(q,p) = \gcd(q,\ell) = 1$, and $m,n$ are positive integers. In another work, Sharma [18] provided a method to list all constacyclic codes over finite fields.

Massey [15] studied another important class of linear codes, which are called complementary-dual codes. He proved that there exist asymptotically good complementary-dual codes and also showed that these codes provide an optimum linear coding solution for the two-user binary adder channel. In another work, Yang and Massey [23] proved that a cyclic code of length $N$ over $\mathbb{F}_q$ is complementary-dual if and only if its generator polynomial $g(x)$ is self-reciprocal and all the monic irreducible factors of $g(x)$ over $\mathbb{F}_q$ have the same multiplicity in $g(x)$ as in $x^N - 1$. Later, Sendrier [17] proved that complementary-dual linear codes meet the asymptotic Gilbert–Varshamov bound using the hull dimension spectra of linear codes.

Throughout this paper, let $p, \ell$ be distinct odd primes, $q$ be an odd prime power with $\gcd(q,p) = \gcd(q,\ell) = 1$, and $m,n$ be positive integers. The main goal of this paper is to determine all self-dual, self-orthogonal and complementary-dual negacyclic codes of length $2p^n \ell^m$ over $\mathbb{F}_q$. Here we will employ techniques similar to that of Sharma [19, 20].

This paper is organized as follows: In Section 2, we state some preliminaries that are needed to derive our main results. In Section 3, we determine all negacyclic codes of length $2p^n \ell^m$ over $\mathbb{F}_q$ (Theorem 1). In Section 4, we list all self-dual, self-orthogonal and complementary-dual negacyclic codes of length $2p^n \ell^m$ over $\mathbb{F}_q$ (Theorems 2-4). To illustrate our results, we determine all self-dual, self-orthogonal and complementary-dual negacyclic codes of length 374 over $\mathbb{F}_5$. We also determine all self-orthogonal and complementary-dual negacyclic codes of length 286 over $\mathbb{F}_3$ and observe that there does not exist any self-dual negacyclic code of length 286 over $\mathbb{F}_3$.

2. Some preliminaries

In this section, we state some preliminaries that are needed to derive our main results.
Let \( \mathbb{F}_q \) denote the finite field of odd prime power order \( q \) and \( N \) be a positive integer coprime to \( q \). A negacyclic code \( C \) of length \( N \) over \( \mathbb{F}_q \) is an ideal in the principal ideal ring \( \mathbb{F}_q[x]/\langle x^N + 1 \rangle \). Further, if we represent the element \( f(x) + (x^N + 1) \in \mathbb{F}_q[x]/\langle x^N + 1 \rangle \) by the polynomial \( f(x) \in \mathbb{F}_q[x] \) of degree strictly less than \( N \), then for every non-zero negacyclic code \( C \), there exists a unique monic polynomial \( g(x) \in C \), which generates the code \( C \) and is a factor of \( x^N + 1 \) in \( \mathbb{F}_q[x] \). The polynomial \( g(x) \) is called the generator polynomial of \( C \) and we write \( C = \langle g(x) \rangle \). Conversely, each factor of \( x^N + 1 \) in \( \mathbb{F}_q[x] \) generates a negacyclic code of length \( N \) over \( \mathbb{F}_q \). Furthermore, the dual code of \( C \), denoted by \( C^\perp \), is defined as \( C^\perp = \{ a(x) \in \mathbb{F}_q[x]/\langle x^N + 1 \rangle : a(x)c^*(x) = 0 \text{ for all } c(x) \in C \} \), where \( c^*(x) = x^{\deg c(x)c(x^{-1})} \) for all \( c(x) \in C \). Note that the dual code \( C^\perp \) is also a negacyclic code of the same length \( N \) over \( \mathbb{F}_q \) and has generator polynomial \( \hat{h}(x) = h(0)^{-1}x^{\deg h(x)}h(x^{-1}) \), where \( h(x) = \frac{x^N - 1}{g(x)} \). Furthermore, the code \( C \) is said to be

- self-orthogonal if it satisfies \( C \subseteq C^\perp \).
- self-dual if it satisfies \( C = C^\perp \).
- complementary-dual if it satisfies \( C \cap C^\perp = \{0\} \).

In general, if \( f(x) \) is any monic polynomial in \( \mathbb{F}_q[x] \) and \( f(0) \) is non-zero, then the reciprocal polynomial of \( f(x) \), denoted by \( \hat{f}(x) \), is defined as \( \hat{f}(x) = f(0)^{-1}x^{\deg f(x)}f(x^{-1}) \). Further, the polynomial \( f(x) \) is said to be a self-reciprocal polynomial if it satisfies \( \hat{f}(x) = f(x) \). A pair \( g(x), h(x) \) of relatively prime monic polynomials in \( \mathbb{F}_q[x] \) is said to be a reciprocal pair if \( h(x) = \hat{g}(x) \) holds. For example, note that the polynomial \( x^N + 1 \) is a self-reciprocal polynomial in \( \mathbb{F}_q[x] \). Therefore if some polynomial \( f(x) \) divides \( x^N + 1 \) in \( \mathbb{F}_q[x] \) (note that \( f(0) \) must be non-zero), either \( f(x) = \hat{f}(x) \) holds or \( \hat{f}(x) \), \( f(x) \) form a reciprocal pair such that \( f(x)\hat{f}(x) \) divides \( x^N + 1 \) in \( \mathbb{F}_q[x] \). Then the following result is straightforward.

**Proposition 1.** Let \( \gcd(N, q) = 1 \). Let

\[
x^N + 1 = f_1(x)f_2(x) \cdots f_S(x)h_1(x)\hat{h}_1(x)h_2(x)\hat{h}_2(x) \cdots h_R(x)\hat{h}_R(x)
\]

be the factorization of \( x^N + 1 \) over \( \mathbb{F}_q \), where \( f_i(x) = \hat{f}_i(x) \) (\( 1 \leq i \leq S \)) and \( h_j(x), \hat{h}_j(x) \) (\( 1 \leq j \leq R \)) are reciprocal pairs of polynomials in \( \mathbb{F}_q[x] \).

(a) There are precisely \( 2^{S+2R} \) distinct negacyclic codes of length \( N \) over \( \mathbb{F}_q \), given by

\[
\left( f_1(x)^{e_1}f_2(x)^{e_2} \cdots f_S(x)^{e_S}h_1(x)^{\mu_1}\hat{h}_1(x)^{\kappa_1}h_2(x)^{\mu_2}\hat{h}_2(x)^{\kappa_2} \cdots h_R(x)^{\mu_R}h_R(x)^{\kappa_R} \right),
\]

where \( e_i \)'s, \( \mu_j \)'s, \( \kappa_j \)'s are either \( 0 \) or \( 1 \).

(b) There exists a self-dual negacyclic code of length \( N \) over \( \mathbb{F}_q \) if and only if no self-reciprocal polynomial divides \( x^N + 1 \) in \( \mathbb{F}_q[x] \). Furthermore, if no self-reciprocal polynomial divides \( x^N + 1 \) in \( \mathbb{F}_q[x] \), then there are
precisely \(2^R\) distinct self-dual negacyclic codes of length \(N\) over \(\mathbb{F}_q\), given by
\[
\left\langle h_1(x)^{\mu_1} \tilde{h}_1(x)^{1-\mu_1} h_2(x)^{\mu_2} \tilde{h}_2(x)^{1-\mu_2} \cdots h_R(x)^{\mu_R} \tilde{h}_R(x)^{1-\mu_R} \right\rangle,
\]
where \(\mu_j\)'s are either 0 or 1.

(c) There are precisely \(3^R\) distinct self-orthogonal negacyclic codes of length \(N\) over \(\mathbb{F}_q\), given by
\[
\left\langle f_1(x) f_2(x) \cdots f_S(x)^{\kappa_1} h_1(x)^{\mu_1} h_2(x)^{\mu_2} \tilde{h}_2(x)^{\kappa_2} \cdots h_R(x)^{\mu_R} \tilde{h}_R(x)^{\kappa_R} \right\rangle,
\]
where \((\mu_j, \kappa_j) \in \{(1, 0), (0, 1), (1, 1)\}\) for \(1 \leq j \leq R\).

(d) There are precisely \(2^{S+R}\) distinct complementary-dual negacyclic codes of length \(N\) over \(\mathbb{F}_q\), given by
\[
\left\langle f_1(x)^{\epsilon_1} f_2(x)^{\epsilon_2} \cdots f_S(x)^{\epsilon_S} h_1(x)^{\mu_1} h_2(x)^{\mu_2} \tilde{h}_2(x)^{\kappa_2} \cdots h_R(x)^{\mu_R} \tilde{h}_R(x)^{\kappa_R} \right\rangle,
\]
where \(\epsilon_i\)'s and \(\mu_j\)'s are either 0 or 1.

Proof. Proof is left to the reader. \(\square\)

From the above proposition, we see that to write down all negacyclic codes of length \(N\) over \(\mathbb{F}_q\) more explicitly, we need to factorize the polynomial \(x^N + 1\) over \(\mathbb{F}_q\). For this, we study \(q\)-cyclotomic cosets, which are as defined below:

Let \(K\) be any positive integer coprime to \(q\). For any integer \(s \geq 0\), the \(q\)-cyclotomic coset of \(s\) modulo \(K\) is defined as the set \(C_s^{(K)} = \{s, sq, sq^2, \ldots, sq^{K-1}\}\), where \(K_s\) is the least positive integer such that \(sq^{K_s} \equiv s \pmod{K}\).

The integer \(s\) is called a representative of \(C_s^{(K)}\) modulo \(K\). Note that the cardinality of \(C_s^{(K)}\) equals the multiplicative order of \(q\) modulo \(\frac{K}{\gcd(K,s)}\). A set \(S_K = \{s_1, s_2, \ldots, s_t\}\) of integers modulo \(K\) is said to be a complete set of representatives of \(q\)-cyclotomic cosets modulo \(K\) if the \(q\)-cyclotomic cosets \(C_{s_i}^{(K)}\) \((1 \leq i \leq t)\) are mutually disjoint modulo \(K\) and \(\bigcup_{i=1}^t C_{s_i}^{(K)} = \mathbb{Z}_K\), where \(\mathbb{Z}_K\) is the ring of integers modulo \(K\). Let us define \(\mathcal{S}_K = \{s \in S_K : s \equiv 1 \pmod{2}\}\). The \(q\)-cyclotomic cosets modulo \(K\) are useful in describing the factorization of \(x^K - 1\) in \(\mathbb{F}_q[x]\), as follows:

If \(\beta\) is a primitive \(K\)th root of unity in some extension field of \(\mathbb{F}_q\), then for each integer \(s \geq 0\), the polynomial \(M_s(x) = \prod_{\beta \in C_s^{(K)}} (x - \beta)\) is the minimal polynomial of \(\beta^s\) over \(\mathbb{F}_q\). From this, it is easy to observe the following:

**Lemma 1.** We have \(C_s^{(K)} = C_{-1}^{(K)}\) if and only if \(M_s(x) = \tilde{M}_1(x)\). 

Proof. Proof is trivial. \(\square\)

Moreover, if \(S_K\) is a complete set of representatives of \(q\)-cyclotomic cosets modulo \(K\), then
\[
x^K - 1 = \prod_{s \in S_K} M_s(x)
\]
is the factorization of $x^K - 1$ into monic irreducible polynomials over $\mathbb{F}_q$.

From now onwards, we focus our attention on negacyclic codes of length $N = 2p^n\ell^m$ over $\mathbb{F}_q$, where $p, \ell$ are distinct odd primes, $q$ is an odd prime power with $\gcd(q, p) = \gcd(q, \ell) = 1$, and $m, n$ are positive integers.

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

In order to write down all negacyclic codes of length $2p^n\ell^m$ over $\mathbb{F}_q$, by Proposition 1, we need to factorize the polynomial $x^{2p^n\ell^m} + 1$ over $\mathbb{F}_q$. For this, we first observe the following:

**Lemma 2.** (a) Let $\mathcal{S}_{2p^n\ell^m} = \{ s \in \mathbb{S}_{2p^n\ell^m} : s \equiv 1 \pmod{2} \}$. For each $s \in \mathcal{S}_{2p^n\ell^m}$, let $M_s(x)$ denote the minimal polynomial of $\alpha^s$ over $\mathbb{F}_q$, where $\alpha$ is a primitive $(4p^n\ell^m)$th root of unity over $\mathbb{F}_q$. Then we have $x^{2p^n\ell^m} + 1 = \prod_{s \in \mathcal{S}_{2p^n\ell^m}} M_s(x)$.

(b) All the distinct negacyclic codes of length $2p^n\ell^m$ over $\mathbb{F}_q$ are given by $\langle \prod_{s \in I} M_s(x) \rangle$, where $I$ runs over all subsets of $\mathcal{S}_{2p^n\ell^m}$.

**Proof.** Proof is trivial.

Now to obtain the set $\mathcal{S}_{2p^n\ell^m}$, we need the following lemma:

**Lemma 3.** We have

$$\mathcal{S}_{2p^n\ell^m} = \bigcup_{(s_1, s_2)} \left\{ \theta(s_1, s_2), \theta(s_1, s_2q), \ldots, \theta(s_1, s_2q^{\gamma(s_1, s_2) - 1}) \right\},$$

where the union $\bigcup_{(s_1, s_2)}$ runs over all $(s_1, s_2) \in \mathbb{S}_{2p^n} \times \mathbb{S}_{\ell^m}$, $\theta$ denotes the usual ring isomorphism given by Chinese Remainder Theorem from $\mathbb{Z}_{4p^n} \times \mathbb{Z}_{\ell^m}$ onto $\mathbb{Z}_{4p^n\ell^m}$ and $\gamma(s_1, s_2) = \gcd \left( \left| C_{s_1}^{(4p^n)} \right|, \left| C_{s_2}^{(\ell^m)} \right| \right)$ for each $s_1 \in \mathbb{S}_{4p^n}$, $s_2 \in \mathbb{S}_{\ell^m}$.

(Throughout this paper, $|A|$ denotes the cardinality of the set $A$.)

**Proof.** It follows from Proposition 3 of Sharma [18].

From the above lemma, we see that in order to determine the set $\mathcal{S}_{4p^n\ell^m}$ more explicitly, we need to determine the sets $\mathcal{S}_{4p^n}$ and $\mathcal{S}_{\ell^m}$. For this, we proceed as follows:

Let $a$ be the multiplicative order of $q$ modulo $p$. Let us write $q^a = 1 + 2p^r c'$, where $p$ does not divide $c'$ and $c \geq 1$ is an integer. With these assumptions, it is easy to see that the multiplicative orders of $q$ modulo $p^r$ and modulo $2p^r$, denoted by $O_{p^r}(q)$ and $O_{2p^r}(q)$ respectively, are given by $O_{p^r}(q) = O_{2p^r}(q) = a p^\max(0, r - c) = \lambda_r$ (say) for $1 \leq r \leq n$. Also it is easy to show that

$$O_{2p^r}(q) = \begin{cases} 
\lambda_r & \text{if } q \equiv 1 \pmod{4} \text{ or } q \equiv 3 \pmod{4} \text{ with } a \text{ even}; \\
2\lambda_r & \text{if } q \equiv 3 \pmod{4} \text{ with } a \text{ odd}.
\end{cases}$$

For $1 \leq r \leq n$, let $\delta_r = \frac{a p^r}{\lambda_r}$, where $\phi$ denotes the Euler’s phi function. Next working as in Lemma 4 of Sharma [21], we choose a primitive root $g$ modulo $p$ satisfying $g^{\delta_r - 1} \not\equiv 1 \pmod{p^r}$ and $g \equiv 1 \pmod{4}$. In view of Theorems 10.6
and 10.7 of [1], we see that the integer \( g \) is a primitive root modulo \( p^r \) and \( 2p^r \) for all \( r \geq 1 \). Further, for integers \( s, r, k \) satisfying \( \gcd(s, p) = 1 \), \( 1 \leq r \leq n \) and \( k \geq 0 \), it is easy to see that the \( q \)-cycloctic coset \( C_{sp^m-r-gk}^{(4p^n)} \) modulo \( 4p^n \) is given by

\[
C_{sp^m-r-gk}^{(4p^n)} = \begin{cases} 
\{sp^n-rg^k, sp^n-rg^kq, \ldots, sp^n-rg^{k\lambda_s-1}\}, & \text{if } q \equiv 3 \pmod{4} \text{ with both } a, s \text{ odd;} \\
\{sp^n-rg^k, sp^n-rg^kq, \ldots, sp^n-rg^{k\lambda_s-1}\}, & \text{otherwise.}
\end{cases}
\]

Then the following lemma provides all the distinct \( q \)-cycloctic cosets modulo \( 4p^n \).

**Lemma 4.**

(a) Let \( q \equiv 1 \pmod{4} \). Let \( \mathfrak{A} \) be an integer satisfying \( \mathfrak{A} \equiv 3 \pmod{4} \) and \( \mathfrak{A} \equiv 1 \pmod{p^n} \). All the distinct \( q \)-cycloctic cosets modulo \( 4p^n \) are given by \( C_0^{(4p^n)} = \{0\}, C_0^{(2p^n)} = \{p^n\}, C_2^{(4p^n)} = \{2p^n\} \) \( C_{4p^n}^{(4p^n)} = \{3p^n\} \) and \( C_{4p^n}^{(4p^n)} = \{3p^n\} \) if \( q \equiv 3 \pmod{4} \) and \( C_{4p^n}^{(4p^n)} = \{3p^n\} \) otherwise.

(b) Let \( q \equiv 3 \pmod{4} \) and \( a \) be even. All the distinct \( q \)-cycloctic cosets modulo \( 4p^n \) are given by \( C_0^{(4p^n)} = \{0\}, C_0^{(2p^n)} = \{p^n, 3p^n\} \) \( C_2^{(4p^n)} = \{2p^n\} \) \( C_{4p^n}^{(4p^n)} = \{2p^n\} \) \( C_{4p^n}^{(4p^n)} = \{2p^n\} \) \( C_{4p^n}^{(4p^n)} = \{2p^n\} \) with \( k \) running over the set \( \{0, 1, 2, \ldots, \delta_r - 1\} \) for each \( r \) \( (1 \leq r \leq n) \). As a consequence, we have

\[
\mathfrak{S}_{4p^n} = \{p^n, 3p^n\} \cup \left\{ \bigcup_{r=1}^{n} \bigcup_{k=0}^{2\delta_r-1} \{p^n-rg^k, \mathfrak{A}p^n-rg^k\} \right\}.
\]

(c) Let \( q \equiv 3 \pmod{4} \) and \( a \) be odd. All the distinct \( q \)-cycloctic cosets modulo \( 4p^n \) are given by \( C_0^{(4p^n)} = \{0\}, C_0^{(2p^n)} = \{p^n, 3p^n\} \) \( C_2^{(4p^n)} = \{2p^n\} \) \( C_{4p^n}^{(4p^n)} = \{2p^n\} \) \( C_{4p^n}^{(4p^n)} = \{2p^n\} \) with \( k \) running over the set \( \{0, 1, 2, \ldots, \delta_r - 1\} \) for each \( r \) \( (1 \leq r \leq n) \). As a consequence, we have

\[
\mathfrak{S}_{4p^n} = \{p^n\} \cup \left\{ \bigcup_{r=1}^{n} \bigcup_{k=0}^{2\delta_r-1} \{p^n-rg^k\} \right\}.
\]

**Proof.**

(a) Suppose, if possible, that there exist integers \( u, v \in \{1, \mathfrak{A}, 2, 4\} \), \( r, r' \) \( (1 \leq r, r' \leq n) \), \( k \) \( (0 \leq k \leq \delta_r - 1) \) and \( k' \) \( (0 \leq k' \leq \delta_r - 1) \) satisfying \( C_{up^n-r-gk}^{(4p^n)} = C_{vp^n-r'-gk'}^{(4p^n)} \). This holds if and only if there exists an integer \( j \) \( (0 \leq j \leq \lambda_r - 1) \) such that \( up^n-r-gk \equiv vp^n-r'-gk' \pmod{4p^n} \). This implies that \( r = r' \), which gives \( up^{k-k'} \equiv v \pmod{4p^n} \). This further implies that \( up^{k-k'} \equiv v \pmod{4p^n} \)
This implies that $\gcd(\delta, v) \equiv 1 \pmod{4}$ and $v \equiv 1 \pmod{4}$. This gives $g^{k-k'} q^j \equiv 1 \pmod{4}$. As $g \equiv 1 \pmod{4}$, we get $g^{k-k'} \equiv 1 \pmod{4}$. This implies that $\delta_r$ divides $k-k'$, as $g$ is a primitive root modulo $p'$. Since $0 \leq k, k' \leq 2\delta_r - 1$, we get $k = k'$, which gives $j = 0$. Further, these are all the distinct $q$-cyclocontic cosets modulo $4p^n$, as these contain

$$\left| C_0^{(4p^n)} \right| + \left| C_{p^n}^{(4p^n)} \right| + \left| C_{2p^n}^{(4p^n)} \right| + \left| C_{3p^n}^{(4p^n)} \right|$$

$$+ \sum_{r=1}^{\frac{n}{\delta_r}} \sum_{k=0}^{\frac{2\delta_r - 1}{\delta_r}} \left| C_{p^n - r g^k}^{(4p^n)} \right| + \sum_{r=1}^{\frac{n}{\delta_r}} \sum_{k=0}^{\frac{\delta_r - 1}{\delta_r}} \left| C_{2p^n - r g^k}^{(4p^n)} \right| + \left| C_{3p^n - r g^k}^{(4p^n)} \right|$$

$$= 4 + 4 \sum_{r=1}^{\frac{n}{\delta_r}} \sum_{k=0}^{\frac{2\delta_r - 1}{\delta_r}} \lambda_r = 4 + 4 \sum_{r=1}^{\frac{n}{\delta_r}} \lambda_r \delta_r = 4p^n \text{ elements.}$$

(b) Suppose, if possible, that there exist integers $r, r'$ ($1 \leq r, r' \leq n$), $k$ ($0 \leq k \leq 2\delta_r - 1$) and $k'$ ($0 \leq k' \leq 2\delta_r - 1$) satisfying $C_{p^n - r g^k}^{(4p^n)} = C_{p^n - r' g^{k'}}^{(4p^n)}$. Then there exists an integer $j$ ($0 \leq j \leq \lambda_r - 1$) such that $p^n - r g^k q^j \equiv p^n - r' g^{k'} \pmod{4p^n}$, which gives $r = r'$. This implies that $g^{k-k'} q^j \equiv 1 \pmod{4p^n}$, which gives $g^{k-k'} q^j \equiv 1 \pmod{4}$ and $g^{k-k'} \equiv 1 \pmod{4}$. As $g \equiv 1 \pmod{4}$, we get $q^j \equiv 1 \pmod{4}$, which implies that the integer $j$ is even, as $q \equiv 3 \pmod{4}$. From this, we obtain $g^{k-k'} q^j \equiv 1 \pmod{4}$. From this, we obtain $k = k'$ and $j = 0$, as $k, k' \leq 2\delta_r - 1$. Next working in a similar way as above, one can show that the $q$-cyclocontic cosets $C_{2p^n - r g^k}^{(4p^n)}$, $C_{3p^n - r g^k}^{(4p^n)}$, $0 \leq k \leq \delta_r - 1$ for $1 \leq r \leq n$, are also mutually disjoint modulo $4p^n$. Further, these are all the distinct $q$-cyclocontic cosets modulo $4p^n$, as these contain

$$\left| C_0^{(4p^n)} \right| + \left| C_{p^n}^{(4p^n)} \right| + \left| C_{2p^n}^{(4p^n)} \right|$$

$$+ \sum_{r=1}^{\frac{\delta_r - 1}{\delta_r}} \sum_{k=0}^{\frac{2\delta_r - 1}{\delta_r}} \left| C_{p^n - r g^k}^{(4p^n)} \right| + \sum_{r=1}^{\frac{\delta_r - 1}{\delta_r}} \sum_{k=0}^{\frac{\delta_r - 1}{\delta_r}} \left| C_{2p^n - r g^k}^{(4p^n)} \right| + \left| C_{3p^n - r g^k}^{(4p^n)} \right|$$

$$= 4 + 4 \sum_{r=1}^{\frac{\delta_r - 1}{\delta_r}} \sum_{k=0}^{\frac{2\delta_r - 1}{\delta_r}} \lambda_r = 4 + 4 \sum_{r=1}^{\frac{\delta_r - 1}{\delta_r}} \lambda_r \delta_r = 4p^n \text{ elements.}$$

(c) Here we have $O_{2p^n}(q) = O_{2p^n}(q) = \lambda_r$ and $O_{4p^n}(q) = 2\lambda_r$ for each $r \geq 1$. Now working in a similar way as in parts (a) and (b), part (c) follows. \[\square\]

Next we proceed to determine a complete set $S_{\ell_m}$ of representatives of $q$-cyclocontic cosets modulo $\ell_m$. For this, let $b$ be the multiplicative order of $q$ modulo $\ell$. Let us write $q^b = 1 + 2\ell d'$, where $\ell$ does not divide $d'$ and $d \geq 1$ is an integer. With these assumptions, the multiplicative order of $q$ modulo $\ell$,
denoted by \( O_{t'}(q) \), is given by \( O_{t'}(q) = b^{\text{max}(0,t-d)} = \mu_t \) (say) for \( 1 \leq t \leq m \). For \( 1 \leq t \leq m \), let \( \nu_t = \frac{a^{(t')}}{\mu_t} \). Let \( h \) be a primitive root modulo \( t' \) for all \( t \geq 1 \). Such an integer \( h \) always exists (for details, see Theorem 10.6 of [1]). Further, it is easy to observe that for any integer \( u \geq 0 \), the \( q \)-cyclotomic coset \( C_{\ell^m-1}^{(t')} \), is given by \( C_{\ell^m-1}^{(t')} = \{ \ell^{m-t}h^u, \ell^{m-t}h^uq, \ldots, \ell^{m-t}h^uq^{\mu_t-1} \} \). Then the following lemma provides all the distinct \( q \)-cyclotomic cosets modulo \( \ell^m \).

**Lemma 5.** All the distinct \( q \)-cyclotomic cosets modulo \( \ell^m \) are given by \( C_0^{(\ell^m)} = \{0\}, C_{\ell^m-1}^{(t')} \), with \( u \) running over the set \( \{0,1,2,\ldots,\nu_t-1\} \) for each \( t \) (\( 1 \leq t \leq m \)). As a consequence, we have

\[
S_{\ell^m} = \{0\} \cup \left\{ \bigcup_{t=1}^{\nu_t-1} \{\ell^{m-t}h^u\} \right\}.
\]

**Proof.** For proof, see Sharma et al. [22, Proposition 1]. □

In the following proposition, we explicitly determine the set \( S_{\ell^m} \).

**Proposition 2.** For \( 1 \leq r \leq n \) and \( 1 \leq t \leq m \), let \( f_{r,t} = \gcd(\lambda_r, \mu_t) \). Let \( \theta \) denote the usual ring isomorphism given by Chinese Remainder Theorem from \( \mathbb{Z}_{4p^n} \times \mathbb{Z}_{\ell^m} \) onto \( \mathbb{Z}_{4p^n \ell^m} \). Then we have the following:

(a) Let \( q \equiv 1 \pmod{4} \). Let \( A \) be an integer satisfying \( A \equiv 3 \pmod{4} \) and \( A \equiv 1 \pmod{p^n} \). Then we have

\[
\mathcal{S}_{4p^n \ell^m} = \{ \theta(p^n,0), \theta(3p^n,0) \} \cup \left( \bigcup_{r=1}^{n} \bigcup_{k=0}^{\delta_r-1} \bigcup_{t=1}^{m} \bigcup_{u=0}^{\nu_t-1} \{ \theta(p^n, \ell^{m-t}h^u), \theta(3p^n, \ell^{m-t}h^u), \theta(p^n, \ell^{m-t}h^u), \theta(3p^n, \ell^{m-t}h^u) \} \right).
\]

(b) Let \( q \equiv 3 \pmod{4} \) and \( a \) be even. Then we have

\[
\mathcal{S}_{4p^n \ell^m} = \{ \theta(p^n,0), \theta(3p^n,0) \} \cup \left( \bigcup_{r=1}^{n} \bigcup_{k=0}^{\delta_r-1} \bigcup_{t=1}^{m} \bigcup_{u=0}^{\nu_t-1} \{ \theta(p^n, \ell^{m-t}h^u), \theta(p^n, \ell^{m-t}h^u), \theta(p^n, \ell^{m-t}h^u), \theta(p^n, \ell^{m-t}h^u) \} \right).
\]

if \( b \) is even, and we have

\[
\mathcal{S}_{4p^n \ell^m} = \{ \theta(p^n,0), \theta(3p^n,0) \} \cup \left( \bigcup_{r=1}^{n} \bigcup_{k=0}^{\delta_r-1} \bigcup_{t=1}^{m} \bigcup_{u=0}^{\nu_t-1} \{ \theta(p^n, \ell^{m-t}h^u), \theta(p^n, \ell^{m-t}h^u), \theta(p^n, \ell^{m-t}h^u), \theta(p^n, \ell^{m-t}h^u) \} \right).
\]

if \( b \) is odd.
Theorem 1. Let \( q \equiv 3 \pmod{4} \) and \( a \) be odd. Then we have

\[
\mathcal{S}_{4p^n\ell^m} = \{ \theta(p^n, 0) \} \cup \left( \bigcup_{r=1}^{n} \bigcup_{k=0}^{m} \bigcup_{t=1}^{m} \bigcup_{u=0}^{m} \bigcup_{w=0}^{m} \{ \theta(p^n, \ell^m t h^u), \theta(p^n, \ell^m t h^u q^w), \theta(p^n, \ell^m t h^u q^{w+m}) \} \right)
\]

if \( b \) is even, and we have

\[
\mathcal{S}_{4p^n\ell^m} = \{ \theta(p^n, 0) \} \cup \left( \bigcup_{r=1}^{n} \bigcup_{k=0}^{m} \bigcup_{t=1}^{m} \bigcup_{u=0}^{m} \bigcup_{w=0}^{m} \{ \theta(p^n, \ell^m t h^u), \theta(p^n, \ell^m t h^u q^w) \} \right)
\]

if \( b \) is odd.

Proof. It follows immediately from Lemmas 3-5.

We now define \( \delta = \sum_{r=1}^{n} \delta_r, \nu = \sum_{t=1}^{m} \nu_t \) and \( \mathcal{S} = \sum_{r=1}^{n} \delta_r \nu_t \).

Theorem 1. Let \( p, \ell \) be distinct odd primes, \( q \) be an odd prime power with \( \gcd(q, p) = \gcd(q, \ell) = 1 \), and \( m, n \) be positive integers.

(a) Let \( q \equiv 1 \pmod{4} \). Let \( A \) be an integer satisfying \( A \equiv 3 \pmod{4} \) and \( A \equiv 1 \pmod{p^m} \). Then there are precisely \( 2^{2(1+\delta+\nu+3)} \) distinct negacyclic codes of length \( 2p^n\ell^m \) over \( \mathbb{F}_q \), where \( I \) runs over all subsets of

\[
\{ \theta(p^n, 0), \theta(3p^n, 0) \} \cup \left( \bigcup_{r=1}^{n} \bigcup_{k=0}^{m} \bigcup_{t=1}^{m} \bigcup_{u=0}^{m} \bigcup_{w=0}^{m} \{ \theta(p^n, \ell^m t h^u), \theta(3p^n, \ell^m t h^u), \theta(p^n, \ell^m t h^u q^w), \theta(3p^n, \ell^m t h^u q^w) \} \right).
\]

(b) Let \( q \equiv 3 \pmod{4} \) and \( a \) be even. Then there are precisely \( 2^{1+2\nu+23+23} \) distinct negacyclic codes of length \( 2p^n\ell^m \) over \( \mathbb{F}_q \) with \( I \) running over all subsets of

\[
\{ \theta(p^n, 0) \} \cup \left( \bigcup_{r=1}^{n} \bigcup_{k=0}^{m} \bigcup_{t=1}^{m} \bigcup_{u=0}^{m} \bigcup_{w=0}^{m} \{ \theta(p^n, \ell^m t h^u), \theta(p^n, \ell^m t h^u q^w) \} \right)
\]

if \( b \) is even, while there are precisely \( 2^{1+\nu+23+23} \) distinct negacyclic codes of length \( 2p^n\ell^m \) over \( \mathbb{F}_q \) with \( I \) running over all subsets of

\[
\{ \theta(p^n, 0) \} \cup \left( \bigcup_{r=1}^{n} \bigcup_{k=0}^{m} \bigcup_{t=1}^{m} \bigcup_{u=0}^{m} \bigcup_{w=0}^{m} \{ \theta(p^n, \ell^m t h^u), \theta(p^n, \ell^m t h^u q^w) \} \right)
\]
Proof. It follows immediately from Lemma 2 and Proposition 2. □

4. Self-dual, self-orthogonal and complementary-dual negacyclic codes of length $2p^n\ell m$ over $\mathbb{F}_q$

From now onwards, we will follow the same notations as in Section 3. Further, for integers $R$ and $S \geq 1$, let $[R]_S$ be the remainder obtained upon dividing $R$ by $S$. Note that $[R]_S = R$ if $0 \leq R < S$. For each $s \in S_{4p^n\ell m}$, let $C_s$ denote the $q$-cyclotomic coset of $s$ modulo $4p^n\ell m$.

In this section, we will determine all self-dual, self-orthogonal and complementary-dual negacyclic codes of length $2p^n\ell m$ over $\mathbb{F}_q$ by considering the following cases separately: (i) $q \equiv 1 \pmod{4}$, (ii) $q \equiv 3 \pmod{4}$ with $a$ even, and (iii) $q \equiv 3 \pmod{4}$ with $a$ odd. For this, we need the following lemma:

Lemma 6 ([19]). Let $1 \leq r \leq n$ and $1 \leq t \leq m$ be fixed integers. Then we have the following:

(a) There exist integers $y_r$ and $z_t$ satisfying $q \equiv g^{y_r\delta_r} \pmod{p'}$ and $q \equiv h^{z_t\epsilon_t} \pmod{\ell'}$ with gcd$(y_r, \lambda_r) = \gcd(z_t, \mu_t) = 1$.

(b) Suppose that there exists an integer $j$ satisfying $g^{s'-s'}q' \equiv -1 \pmod{p'}$ for some integers $s, s' (0 \leq s, s' \leq \delta_r - 1)$. Then we have

$$s' = \left\{ \begin{array}{ll} \left[ s + \frac{\delta_r}{s} \right] \delta_r & \text{if } a \text{ is odd;} \\ s & \text{if } a \text{ is even.} \end{array} \right.$$
SIMPLE-ROOT NEGACYCLIC CODES OF LENGTH $2p^n\ell^m$

(Noe that when $a$ is odd, each $\lambda_r$ is odd. This implies that each $\delta_r$ is even, as $\phi(p^r) = \lambda_r\delta_r$ is even for each $r$.)

(c) Suppose that there exists an integer $k$ satisfying $h^{u-u'}q^k \equiv -1 \pmod{\ell^t}$ for some integers $u, u'$ ($0 \leq u, u' \leq \nu_t - 1$). Then we have

$$u' = \begin{cases} 
[u + \frac{\phi}{2}\nu]_\nu & \text{if } b \text{ is odd}; \\
u & \text{if } b \text{ is even}.
\end{cases}$$

(Note that when $b$ is odd, each $\mu_t$ is odd. This implies that each $\nu_t$ is even, as $\phi(\ell^t) = \mu_t\nu_t$ is even for each $t$.)

Proof. For proof, see Sharma [19, Lemma 8]. □

Next we make the following observation:

Remark 1. Note that $x^{2\nu_t\ell^m} + 1 = x^{2p^n\ell^m} + 1$. From this, it follows that for every $s \in S_{4p^n\ell^m}$, there exists $t \in S_{4p^n\ell^m}$ such that $\hat{M}_s(x) = M_t(x)$ (or equivalently, $C_{-s} = C_t$ by Lemma 1).

4.1. $q \equiv 1 \pmod{4}$

Throughout this subsection, let $q \equiv 1 \pmod{4}$, and $A$ be an integer satisfying $A \equiv 3 \pmod{4}$ and $A \equiv 1 \pmod{p^n}$. Then in the following theorem, we list all the self-dual, self-orthogonal and complementary-dual negacyclic codes of length $2p^n\ell^m$ over $\mathbb{F}_q$.

Theorem 2. Let $q \equiv 1 \pmod{4}$, and $A$ be an integer satisfying $A \equiv 3 \pmod{4}$ and $A \equiv 1 \pmod{p^n}$. There are precisely

- $2^{1+\delta+\nu+\delta}$ distinct self-dual negacyclic codes
  $$\left\langle \prod_{j \in J} M_j(x) \prod_{k \in \hat{S}_{4p^n\ell^m} \setminus J} \hat{M}_k(x) \right\rangle$$
  of length $2p^n\ell^m$ over $\mathbb{F}_q$,

- $3^{1+\delta+\nu+\delta}$ distinct self-orthogonal negacyclic codes
  $$\left\langle \prod_{j \in J} M_j(x) \prod_{j' \in J'} \hat{M}_{j'}(x) \right\rangle$$
  of length $2p^n\ell^m$ over $\mathbb{F}_q$,

- $2^{1+\delta+\nu+\delta}$ distinct complementary-dual negacyclic codes
  $$\left\langle \prod_{j \in J} M_j(x) \hat{M}_j(x) \right\rangle$$
  of length $2p^n\ell^m$ over $\mathbb{F}_q$, where

- $\delta$ is the number of integers $r$ such that $b_r = 1$.

- $\nu$ is the number of integers $r$ such that $a_r = 1$.

- $\lambda_r$ is the number of integers $r$ such that $\lambda_r = 1$.

- $\delta_r$ is the number of integers $r$ such that $\delta_r = 1$.

- $\mu_t$ is the number of integers $t$ such that $\mu_t = 1$.

- $\nu_t$ is the number of integers $t$ such that $\nu_t = 1$.
with \( J, J' \) running over all subsets of \( \mathcal{S}_{4p^n \ell^m} \) \( \subseteq \mathcal{S}_{4p^n \ell^m} \), where
\[
\mathcal{S}_{4p^n \ell^m} = \{ (p^n, 0) \} \cup \bigcup_{r=1}^n \bigcup_{t=1}^m \bigcup_{k=0}^{\ell-1} \bigcup_{u=0}^{\delta_r-1} \{ \theta(p^n, \ell^m-t h^u), \theta(p^n-r g^k, 0), \theta(p^n-g^k, \ell^m-t h^u q^w) \}.
\]

To prove this theorem, we need to prove the following lemma:

**Lemma 7.** For \( 1 \leq r \leq n \) and \( 1 \leq t \leq m \), let \( 0 \leq k \leq \delta_r - 1 \), \( 0 \leq u \leq \nu_t - 1 \) and \( 0 \leq w \leq f_{r,t} - 1 \) be fixed integers. Further for each \( r \) and \( t \), let \( y_r \) and \( z_t \) be as chosen in Lemma 6(a) with \( y_r^{-1} \) and \( z_t^{-1} \) as the multiplicative inverses of \( y_r \) and \( z_t \) modulo \( \lambda_r \) and \( \mu_t \), respectively. Then we have

\[
\begin{align*}
(a) \quad & C_{-\theta(p^n, 0)} = C_{\theta(3p^n, 0)}, \\
(b) \quad & C_{-\theta(p^n, \ell^m-t h^u)} = \begin{cases} 
C_{\theta(3p^n, \ell^m-t h^u)} & \text{if } b \text{ is odd;} \\
C_{\theta(3p^n, \ell^m-t h^u)} & \text{if } b \text{ is even,}
\end{cases} \\
(c) \quad & C_{-\theta(p^n-r g^k, 0)} = \begin{cases} 
C_{\theta(3p^n-r g^k, 0)} & \text{if } a \text{ is odd;} \\
C_{\theta(3p^n-r g^k, 0)} & \text{if } a \text{ is even,}
\end{cases} \\
(d) \quad & C_{-\theta(p^n-g^k, \ell^m-t h^u q^w)} = \begin{cases} 
C_{\theta(3p^n-g^k, \ell^m-t h^u q^w, r)} & \text{if both } a, b \text{ are even;}
C_{\theta(3p^n-g^k, \ell^m-t h^u q^w, r)} & \text{if } a \text{ is even and } b \text{ is odd;}
C_{\theta(3p^n-g^k, \ell^m-t h^u q^w, r)} & \text{if } a \text{ is odd and } b \text{ is even;}
C_{\theta(3p^n-g^k, \ell^m-t h^u q^w, r)} & \text{if both } a, b \text{ are odd,}
\end{cases}
\end{align*}
\]

with \( \tilde{u}_r = \left[u + \frac{w}{2}\right]_{v_r}, k^* = \left[k + \frac{v_r}{2}\right]_{\delta_r}, \tilde{w}_{r,t} = \left[w + \frac{\nu_t}{2}\right]_{f_{r,t}}, \)

\[
\begin{align*}
\tilde{w}_{r,t} &= \begin{cases} 
\frac{w + \lambda_r - z_r^{-1}(\mu_t + 1)}{2} & \text{if } 0 \leq u \leq \frac{w}{2} - 1, \\
\frac{w + \lambda_r - z_r^{-1}(\mu_t + 1)}{2} & \text{if } \frac{w}{2} \leq u \leq \nu_t - 1,
\end{cases} \\
\tilde{w}_{r,t} &= \begin{cases} 
\frac{w + \mu_t + y_r^{-1}(\lambda_r - 1)}{2} & \text{if } 0 \leq k \leq \frac{\delta_r}{2} - 1, \\
\frac{w + \mu_t + y_r^{-1}(\lambda_r - 1)}{2} & \text{if } \frac{\delta_r}{2} \leq k \leq \delta_r - 1,
\end{cases} \\
\tilde{w}_{r,t} &= \begin{cases} 
\frac{w + y_r^{-1}(\lambda_r + 1) - z_r^{-1}(\mu_t + 1)}{2} & \text{if } 0 \leq k \leq \frac{\delta_r}{2} - 1, 0 \leq u \leq \frac{w}{2} - 1; \\
\frac{w + y_r^{-1}(\lambda_r + 1) - z_r^{-1}(\mu_t + 1)}{2} & \text{if } 0 \leq k \leq \frac{\delta_r}{2} - 1, \frac{w}{2} \leq u \leq \nu_t - 1; \\
\frac{w + y_r^{-1}(\lambda_r + 1) - z_r^{-1}(\mu_t + 1)}{2} & \text{if } \frac{\delta_r}{2} \leq k \leq \delta_r - 1, 0 \leq u \leq \frac{w}{2} - 1; \\
\frac{w + y_r^{-1}(\lambda_r + 1) - z_r^{-1}(\mu_t + 1)}{2} & \text{if } \frac{\delta_r}{2} \leq k \leq \delta_r - 1, \frac{w}{2} \leq u \leq \nu_t - 1.
\end{cases}
\end{align*}
\]

**Proof.** (a) By Remark 1, there exists an element \( j \in \mathcal{S}_{4p^n \ell^m} \) such that
\[
C_{-\theta(p^n, 0)} = C_j.
\]
By Proposition 2(a), we write \( j = \vartheta(j_1, j_2) \), where \((j_1, j_2)\) is either of the type \((\vartheta p^n, 0)\) or \((\vartheta p^n, \ell_m t h^u)\) or \((\vartheta g^{n-r} g^k, 0)\) or \((\vartheta g^{n-r} g^k, \ell_m t h^u q^w)\) with \( \vartheta \in \{1, 3\}, \varrho \in \{1, A\}, 0 \leq u \leq \nu t - 1, 0 \leq k \leq \delta_r - 1, 0 \leq w \leq f_{r,t} - 1, 1 \leq r \leq n \) and \( 1 \leq t \leq m \). That is, we have \( C_{-\vartheta(p^n, 0)} \equiv C_{\vartheta(j_1, j_2)} \), which holds if and only if there exists an integer \( v \geq 0 \) satisfying \( \theta(j_1, j_2) \equiv -\theta(p^n, 0) q^v \pmod{4p^n \ell_m} \). This is equivalent to \( j_1 \equiv -p^q q^v \pmod{4p^n} \) and \( j_2 \equiv 0 \pmod{\ell_m} \), which gives \( j_1 = 3p^n, v = 0 \) and \( j_2 = 0 \). This proves (a).

(b) By Remark 1, there exists an element \( s \in \mathbb{G}_{4p^n \ell_m} \) such that

\[
C_{-\vartheta(p^n, \ell_m t h^u)} = C_s.
\]

By Proposition 2(a), we write \( \varrho = \vartheta(s_1, s_2) \), where \((s_1, s_2)\) is either of the type \((\vartheta p^n, 0)\) or \((\vartheta p^n, \ell_m t h^u)\) or \((\vartheta g^{n-r} g^k, 0)\) or \((\vartheta g^{n-r} g^k, \ell_m t h^u q^w)\) with \( \vartheta \in \{1, 3\}, \varrho \in \{1, A\}, 0 \leq u' \leq \nu t - 1, 0 \leq k' \leq \delta_r - 1, 0 \leq w \leq f_{r,t} - 1, 1 \leq r \leq n \) and \( 1 \leq t' \leq m \). Now \( C_{-\vartheta(p^n, \ell_m t h^u)} = C_{\vartheta(s_1, s_2)} \) holds if and only if each \( \vartheta \) exists an integer \( Y \geq 0 \) satisfying \( -\vartheta(p^n, \ell_m t h^u) q^Y \equiv \varrho(s_1, s_2) \pmod{4p^n \ell_m} \). This gives \( s_1 \equiv -p^q q^Z \pmod{4p^n} \) and \( s_2 \equiv -\ell_m t h^u q^Y \pmod{\ell_m} \). From this, we obtain \( s_1 = 3p^n \). Also note that \( \text{gcd}(s_2, \ell_m) = \text{gcd}(-\ell_m t h^u q^Y, \ell_m) = \ell_m t \) implies that \( j_2 \) must be of the form \( \ell_m t h^u \), where \( 0 \leq u' \leq \nu t - 1 \). This further implies \( h^{u'-v} q^Y \equiv -1 \pmod{\ell t} \). By Lemma 6(c), we get \( u' = \left[ u + \frac{a_2}{2} \right] \), if \( b \) is odd and \( u' = u \) if \( b \) is even, which proves (b).

(c) By Remark 1, there exists an element \( \epsilon \in \mathbb{G}_{4p^n \ell_m} \) such that

\[
C_{-\vartheta(p^n, \ell_m t h^u)} = C_{\epsilon}.
\]

By Proposition 2(a), we write \( \epsilon = \vartheta(\epsilon_1, \epsilon_2) \), where \((\epsilon_1, \epsilon_2)\) is either of the type \((\vartheta p^n, 0)\) or \((\vartheta p^n, \ell_m t h^u)\) or \((\vartheta g^{n-r} g^k, 0)\) or \((\vartheta g^{n-r} g^k, \ell_m t h^u q^w)\) with \( \vartheta \in \{1, 3\}, \varrho \in \{1, A\}, 0 \leq u \leq \nu t - 1, 0 \leq k' \leq \delta_r - 1, 0 \leq w \leq f_{r,t} - 1, 1 \leq r' \leq n \) and \( 1 \leq t' \leq m \). This holds if and only if there exists an integer \( Z \geq 0 \) satisfying \( -\vartheta(p^n, \ell_m t h^u) q^Z \equiv \vartheta(\epsilon_1, \epsilon_2) \pmod{4p^n \ell_m} \), which gives \( \epsilon_1 \equiv -p^q q^Z \pmod{4p^n} \) and \( \epsilon_2 \equiv 0 \pmod{\ell_m} \). From this, it follows that \( \epsilon_2 = 0 \) and \( \epsilon_1 \) must be of the form \( g^{n-r} g^k \), where \( \varrho \in \{1, A\} \) and \( 0 \leq k' \leq \delta_r - 1 \). This gives \( g^{k-k'} q^Z \equiv -q \pmod{4p^n} \), which gives \( g^{k-k'} q^Z \equiv -q \pmod{4} \) and \( g^{k-k'} q^Z \equiv -q \pmod{4p^n} \). As \( g \equiv q \equiv 1 \pmod{4} \) and \( A \equiv 3 \pmod{4} \), we must have \( \varrho = A \). Since \( A \equiv 1 \pmod{2} \), we get \( g^{k-k'} q^Z \equiv -1 \pmod{4p^n} \), which, by Lemma 6(b), implies that \( k' = \left[ k + \frac{a_2}{2} \right] \), if \( a \) is odd and \( k' = k \) if \( a \) is even.

(d) By Remark 1, there exists an element \( \Delta \in \mathbb{G}_{4p^n \ell_m} \) such that

\[
C_{-\vartheta(p^n, \ell_m t h^u q^w)} = C_{\Delta}.
\]

By Proposition 2(a), we write \( \Delta = \vartheta(\Delta_1, \Delta_2) \), where \((\Delta_1, \Delta_2)\) is either of the type \((\vartheta p^n, 0)\) or \((\vartheta p^n, \ell_m t h^u)\) or \((\vartheta g^{n-r} g^k, 0)\) or \((\vartheta g^{n-r} g^k, \ell_m t h^u q^w)\) with \( \vartheta \in \{1, 3\}, \varrho \in \{1, A\}, 0 \leq u' \leq \nu t - 1, 0 \leq k' \leq \delta_r - 1, 0 \leq w' \leq f_{r,t} - 1, 1 \leq r' \leq n \) and \( 1 \leq t' \leq m \). From this, we see that there exists an integer \( \varphi \geq 0 \) satisfying

\[
-\theta(p^{n-r} g^k, \ell_m t h^u q^w) q^\varphi \equiv \theta(\Delta_1, \Delta_2) \pmod{4p^n \ell_m}.
\]
Let us write \( q^2 = \theta(q^{r_1}, q^{r_2}) \), where \( \varphi \equiv \varphi_1 \pmod{\lambda_0}, \varphi \equiv \varphi_2 \pmod{\mu_0} \) with \( 0 \leq \varphi_1 < \lambda_0 \) and \( 0 \leq \varphi_2 < \mu_0 \). Using this, we see that the congruence (1) is equivalent to the following system of congruences:

\[
\begin{align*}
\Delta_1 & \equiv -p^n - r^k q^{\varphi_1} \pmod{4 p^n} \\
\Delta_2 & \equiv -\ell^m - t h^{u} q^{u} \pmod{\ell^m} 
\end{align*}
\]

As \( \gcd(\Delta_1, 4 p^n) = p^n - r \) and \( \gcd(\Delta_2, \ell^m) = \ell^{m - t} \), we must have \( \Delta_1 = g p^n - r g^{k'} \) and \( \Delta_2 = \ell^{m - t} h^{u} q^{w} \), where \( g \in \{ 1, \mathfrak{A} \} \), \( 0 \leq k' \leq \delta_t - 1 \), \( 0 \leq u' \leq \nu_t - 1 \) and \( 0 \leq w' \leq f_{r,t} - 1 \). In view of this, (2) gives \( g^{k'} q^{w'} \equiv -g \pmod{4 \ell'} \) and \( h^{u} w' q^{w} w' \equiv -1 \pmod{\ell'} \). From this, we have \( g^{k'} q^{w'} \equiv -g \pmod{\ell'} \), which holds only if \( g = \mathfrak{A} \), as \( q \equiv g \equiv 1 \pmod{4} \) and \( \mathfrak{A} \equiv 3 \pmod{4} \). From this and using the fact that \( \mathfrak{A} \equiv 1 \pmod{p^n} \), we obtain \( g^{k'} q^{w'} \equiv -1 \pmod{\ell'} \) and \( h^{u} w' q^{w} w' \equiv -1 \pmod{\ell'} \). Now working in a similar way as in Lemma 7 of Sharma [20] and using Lemma 6(a), part (d) follows immediately.

**Proof of Theorem 2.** It follows from Lemmas 1 and 7, and Proposition 1. □

### 4.2. \( q \equiv 3 \pmod{4} \) and \( a \) is even

Throughout this subsection, let \( q \equiv 3 \pmod{4} \) and \( a \) be even.

As \( \gcd(a, p) = \gcd(b, \ell) = 1 \), we write \( a = \hat{a} \ell^{a_1} \) and \( b = \hat{b} p^{b_1} \), where \( \gcd(\hat{a}, \ell) = \gcd(\hat{b}, p) = 1 \) and \( a_1 \geq 0, b_1 \geq 0 \) are integers. Let \( f = \gcd(\hat{a}, \hat{b}) \). Note that \( \gcd(f, p) = \gcd(f, \ell) = 1 \). Then we make the following observation:

**Lemma 8.** If both \( a, b \) are even, then the following hold:

(i) \( \lambda + \mu \equiv 0 \pmod{2 f_{r,t}} \) if and only if \( a + b \equiv 0 \pmod{2 f} \).

(ii) \( \omega_{r,t} = \left\lfloor \frac{\lambda + \mu}{2} \right\rfloor_{f_{r,t}} = w \) if and only if \( a + b \equiv 0 \pmod{2 f} \).

**Proof.** Proof is trivial. □

In the following theorem, we prove the non-existence of self-dual negacyclic codes of length \( 2 p^\ell \ell^m \) over \( \mathbb{F}_q \), and list all the self-orthogonal and complementary-dual negacyclic codes of length \( 2 p^\ell \ell^m \) over \( \mathbb{F}_q \).

**Theorem 3.** Let \( q \equiv 3 \pmod{4} \) and \( a \) be even. Then there does not exist any self-dual negacyclic code of length \( 2 p^\ell \ell^m \) over \( \mathbb{F}_q \).

A. When \( b \) is odd and \( a \equiv 2 \pmod{4} \), there are precisely

- **3** \( \frac{3}{2} + \frac{3}{2} \) distinct self-orthogonal negacyclic codes

\[
\left\langle \prod_{i \in I} M_i(x) \prod_{j \in J} M_j(x) \prod_{j' \in J'} \overline{M}_{j'}(x) \right\rangle
\]

of length \( 2 p^\ell \ell^m \) over \( \mathbb{F}_q \), and

- **2** \( \frac{3}{2} + \frac{3}{2} \) distinct complementary-dual negacyclic codes

\[
\left\langle \prod_{i \in I} M_i(x) \prod_{j \in J} M_j(x) \overline{M}_{j}(x) \right\rangle
\]

B. When \( b \) is odd and \( a \equiv 0 \pmod{4} \), there are precisely

- **3** \( \frac{3}{2} + \frac{3}{2} \) distinct self-orthogonal negacyclic codes

\[
\left\langle \prod_{i \in I} M_i(x) \prod_{j \in J} M_j(x) \prod_{j' \in J'} \overline{M}_{j'}(x) \right\rangle
\]

of length \( 2 p^\ell \ell^m \) over \( \mathbb{F}_q \), and

- **2** \( \frac{3}{2} + \frac{3}{2} \) distinct complementary-dual negacyclic codes

\[
\left\langle \prod_{i \in I} M_i(x) \prod_{j \in J} M_j(x) \overline{M}_{j}(x) \right\rangle
\]
of length $2^{n \ell m}$ over $\mathbb{F}_q$, with $I$ running over all subsets of $\mathcal{S}_{4p^{n \ell m}}$ and $J, J'$ running over all subsets of $\mathcal{S}_{4p^{n \ell m}}$ satisfying $J \cup J' = \mathcal{S}_{4p^{n \ell m}}$, where

$$\mathcal{S}_{4p^{n \ell m}} = \{ \theta(p^n, 0) \} \cup \left( \bigcup_{r=1}^{n} \bigcup_{k=0}^{2^r-1} \{ \theta(p^{n-r} g^k, 0) \} \right)$$

and

$$\mathcal{S}_{4p^{n \ell m}} = \left( \bigcup_{r=1}^{n} \bigcup_{k=0}^{m} \bigcup_{t=1}^{2^r-1} \bigcup_{w=0}^{2^t-1} \{ \theta(p^n, \ell^{m-t} h^w), \theta(p^{n-r} g^k, \ell^{m-t} h^w q^w) \} \right).$$

B. When $b$ is odd and $a \equiv 0 \pmod{4}$, there are precisely

- $3^{d+\frac{b}{2}+\delta}$ distinct self-orthogonal negacyclic codes
  $$\left\langle M_{\theta(p^n, 0)}(x) \prod_{j \in J} M_j(x) \prod_{j \in J'} \tilde{M}_j(x) \right\rangle$$

of length $2^{n \ell m}$ over $\mathbb{F}_q$, and

- $2^{1+\delta+\frac{b}{2}+\delta}$ distinct complementary-dual negacyclic codes
  $$\left\langle M_{\theta(p^n, 0)}(x)^\ast \prod_{j \in J} M_j(x) \tilde{M}_j(x) \right\rangle$$

of length $2^{n \ell m}$ over $\mathbb{F}_q$, with $i \in \{0, 1\}$ and $J, J'$ running over all subsets of $\mathcal{S}_{4p^{n \ell m}}$ satisfying $J \cup J' = \mathcal{S}_{4p^{n \ell m}}$, where

$$\mathcal{S}_{4p^{n \ell m}} = \left( \bigcup_{r=1}^{n} \bigcup_{k=0}^{m} \bigcup_{t=1}^{2^r-1} \bigcup_{w=0}^{2^t-1} \{ \theta(p^n, \ell^{m-t} h^w), \theta(p^{n-r} g^k, \ell^{m-t} h^w q^w) \} \right).$$

C. Let $b$ be even and $a \equiv 2 \pmod{4}$.

(i) When $\frac{w+b}{k} \equiv 0 \pmod{f}$, we have $\tilde{w}_{r,t} = \left[ w + \frac{\lambda r + \mu t}{2} \right]_{f_r,t} = w$ for $0 \leq w \leq f_{r,t} - 1$, where $1 \leq r \leq n$ and $1 \leq t \leq m$.

When $b \equiv 2 \pmod{4}$, we have the following:

- There is only one self-orthogonal negacyclic code of length $2^{n \ell m}$ over $\mathbb{F}_q$, namely the zero code.

- There are precisely $2^{1+2\delta+2^n+2\delta}$ distinct complementary-dual negacyclic codes $\left\langle \prod M_j(x) \right\rangle$ of length $2^{n \ell m}$ over $\mathbb{F}_q$ with $I$ running over all subsets of

$$\{ \theta(p^n, 0) \} \cup \left( \bigcup_{r=1}^{n} \bigcup_{k=0}^{m} \bigcup_{t=1}^{2^r-1} \bigcup_{w=0}^{2^t-1} \{ \theta(p^{n-r} g^k, 0), \theta(p^n, \ell^{m-t} h^w) \} \right).$$
\( \theta(p^n, \ell^{m-t}h^uw), \theta(p^{n-r}g^k, \ell^{m-t}h^uw) \) \).

When \( b \equiv 0 \) (mod \( 4 \)), there are precisely

- \( 3^s \) distinct self-orthogonal negacyclic codes

\[
\left\langle \prod_{i \in \mathcal{S}_4p^n \ell^m} M_i(x) \prod_{j \in J} M_j(x) \prod_{j' \in J'} \overline{M}_{j'}(x) \right\rangle
\]

of length \( 2^{p^n \ell^m} \) over \( \mathbb{F}_q \), and

- \( 2^{1+\nu+2\nu+2\delta} \) distinct complementary-dual negacyclic codes

\[
\left\langle \prod_{i \in I} M_i(x) \prod_{j \in J} M_j(x) \overline{M}_j(x) \right\rangle
\]

of length \( 2^{p^n \ell^m} \) over \( \mathbb{F}_q \),

with \( I \) running over all subsets of \( \mathcal{S}_4p^n \ell^m \) and \( J, J' \) running over all subsets of \( \mathcal{S}_4p^n \ell^m \) satisfying \( J \cup J' = \mathcal{S}_4p^n \ell^m \), where

\[
\mathcal{S}_4p^n \ell^m = \{ \theta(p^n, 0) \}
\]

\[
\cup \left( \bigcup_{r=1}^{n} \bigcup_{\nu=0}^{m} \bigcup_{t=1}^{2\nu-1} \bigcup_{f_{r,t}=1}^{m} \{ \theta(p^{n-r}g^k, 0), \theta(p^{n-r}g^k, \ell^{m-t}h^uw) \} \right)
\]

and

\[
\widetilde{\mathcal{S}_4p^n \ell^m} = \left( \bigcup_{t=1}^{\nu-1} \bigcup_{u=0}^{1} \left\{ \theta(p^n, \ell^{m-t}h^uw) \right\} \right).
\]

(ii) When \( \frac{\mu}{f_r} \neq 0 \) (mod \( f \)), we have \( \tilde{w}_{r,t} = \left[ w + \frac{\lambda + \mu}{f_r} \right]_{f_{r,t}} \neq w \) for \( 0 \leq w \leq f_{r,t} - 1 \), where \( 1 \leq r \leq n \) and \( 1 \leq t \leq m \). Further, for \( 1 \leq r \leq n \) and \( 1 \leq t \leq m \), let \( w_{r,t}^{(1)}, w_{r,t}^{(2)}, \ldots, w_{r,t}^{(f_{r,t})} \) be the distinct integers satisfying \( \{ 0, 1, 2, \ldots, f_{r,t} - 1 \} = \bigcup_{j=1}^{f_{r,t}} \{ w_{r,t}^{(j)}, \tilde{w}_{r,t}^{(j)} \} \).

When \( b \equiv 2 \) (mod \( 4 \)), there are precisely

- \( 3^s \) distinct self-orthogonal negacyclic codes

\[
\left\langle \prod_{i \in \mathcal{S}_4p^n \ell^m} M_i(x) \prod_{j \in J} M_j(x) \prod_{j' \in J'} \overline{M}_{j'}(x) \right\rangle
\]

of length \( 2^{p^n \ell^m} \) over \( \mathbb{F}_q \), and

- \( 2^{1+\nu+2\nu+2\delta} \) distinct complementary-dual negacyclic codes

\[
\left\langle \prod_{i \in I} M_i(x) \prod_{j \in J} M_j(x) \overline{M}_j(x) \right\rangle
\]

of length \( 2^{p^n \ell^m} \) over \( \mathbb{F}_q \).
with $I$ running over all subsets of $\mathcal{S}_{4p_n^e}^*$ and $J, J'$ running over all subsets of $\mathcal{S}_{4p_n^e}^*$ satisfying $J \cup J' = \mathcal{S}_{4p_n^e}^*$, where
\[
\mathcal{S}_{4p_n^e}^* = \{\theta(p^n, 0)\} \cup \bigcup_{r=1}^{n} \bigcup_{t=1}^{m} \bigcup_{k=0}^{2\delta_r-1} \bigcup_{u=0}^{\ell^t} \{\theta(p^n, \ell^{m-t} h^u), \theta(p^n, \ell^{m-2} h^u q), \theta(p^n, \ell^{m-3} h^u q^{(1)})\}
\]
and
\[
\mathcal{S}_{4p_n^e}^* = \left( \bigcup_{r=1}^{n} \bigcup_{t=1}^{m} \bigcup_{k=0}^{2\delta_r-1} \bigcup_{u=0}^{\ell^t} \{\theta(p^n, \ell^{m-t} h^u), \theta(p^n, \ell^{m-2} h^u q), \theta(p^n, \ell^{m-3} h^u q^{(1)})\} \bigg) \right).
\]
When $b \equiv 0 \pmod{4}$, there are precisely
- $3^{r+3}$ distinct self-orthogonal negacyclic codes
- $2^{n+r2^r+3}$ distinct complementary-dual negacyclic codes
of length $2p^e q^m$ over $\mathbb{F}_q$, and

when $b \equiv 0 \pmod{4}$, running over all subsets of $\mathcal{S}_{4p_n^e}^*$ and $J, J'$ running over all subsets of $\mathcal{S}_{4p_n^e}^*$ satisfying $J \cup J' = \mathcal{S}_{4p_n^e}^*$, where
\[
\mathcal{S}_{4p_n^e}^* = \{\theta(p^n, 0)\} \cup \bigcup_{r=1}^{n} \bigcup_{t=1}^{m} \bigcup_{k=0}^{2\delta_r-1} \bigcup_{u=0}^{\ell^t} \{\theta(p^n, \ell^{m-t} h^u), \theta(p^n, \ell^{m-2} h^u q), \theta(p^n, \ell^{m-3} h^u q^{(1)})\}
\]
and
\[
\mathcal{S}_{4p_n^e}^* = \left( \bigcup_{r=1}^{n} \bigcup_{t=1}^{m} \bigcup_{k=0}^{2\delta_r-1} \bigcup_{u=0}^{\ell^t} \{\theta(p^n, \ell^{m-t} h^u), \theta(p^n, \ell^{m-2} h^u q), \theta(p^n, \ell^{m-3} h^u q^{(1)})\} \bigg) \right).
\]

D. Let $b$ be even and $a \equiv 0 \pmod{4}$.
(i) When $b \equiv 2 \pmod{4}$, there are precisely
- $3^{r+3}$ distinct self-orthogonal negacyclic codes
of length $2p^e q^m$ over $\mathbb{F}_q$, and
Lemma 9. For $1 \leq r \leq n$ and $1 \leq t \leq m$, let $0 \leq u \leq \nu_t - 1$, $0 \leq k \leq 2\delta_r - 1$ and $0 \leq w \leq f_{r,t} - 1$ be fixed integers. For each $r$ and $t$, let $y_r$ and $z_t$ be as chosen in Lemma 6(a) with $y_r^{-1}$ and $z_t^{-1}$ as the multiplicative inverses of $y_r$ and $z_t$ modulo $\lambda_r$ and $\mu_t$, respectively. Then we have

(a) $C_{\theta(p^n,0)} = C_{\theta(p^n,0)}$

(b) $C_{\theta(p^n-g^k,0)} = \begin{cases} C_{\theta(p^n-g^k,0)} & \text{if } a \equiv 0 \pmod{4}; \\ C_{\theta(p^n-g^k,0)} & \text{if } a \equiv 2 \pmod{4}; \end{cases}$
(c) for $s \in \{0, 1\}$,

$$C_{-\theta(p^n, \ell^m-t h^n q^v)} = \begin{cases} 
C_{\theta(p^n, \ell^m-t h^n q^v)} & \text{if } b \equiv 0 \mod 4; \\
C_{\theta(p^n, \ell^m-t h^n q^v)} & \text{if } b \equiv 2 \mod 4; \\
C_{\theta(p^n, \ell^m-t h^n q^v)} & \text{if } b \text{ is odd},
\end{cases}$$

with $\hat{s} = \lfloor s + \frac{1}{2} \rfloor$ for $s \in \{0, 1\}$, $k_r = [k + \delta_r]_{2\delta_r}$, $\hat{u}_t = \left[ u + \frac{\mu_r}{2} \right]_{\mu_t}$, where

$$\hat{w}_{r,t} = \left[ w + \frac{\lambda_r+\mu_r}{2} \right]_{fr,t},$$

$$\bar{w}_{r,t} = \left\{ \begin{array}{ll}
\left[ w + \frac{y_r^{-1}(\lambda_r+2)+\mu_r}{2} \right]_{fr,t} & \text{if } 0 \leq k \leq \delta_r - 1; \\
\left[ w + \frac{y_r^{-1}(\lambda_r-2)+\mu_r}{2} \right]_{fr,t} & \text{if } \delta_r \leq k \leq 2\delta_r - 1,
\end{array} \right.$$
By Proposition 2(b), we write \( \epsilon = \theta(\epsilon_1, \epsilon_2) \), where \((\epsilon_1, \epsilon_2)\) is either of the form \((p^n, 0)\) or \((p^n, \ell^{m-t} h' q^t)\) or \((p^n-r' \ell^{m-t} g', 0)\) or \((p^n-r' \ell^{m-t} g\ell^{m-t} h' q^t, 0)\) with \(0 \leq u \leq \nu_1 - 1, 0 \leq k' \leq 2\delta_r - 1, 0 \leq w \leq f_{r', t} - 1, 1 \leq \ell' \leq n, 1 \leq t \leq m, \) and \(s = 0\) if \(b\) is odd and \(s \in \{0, 1\}\) if \(b\) is even. That is, we have \(C_{-\theta(p^n-r' \ell^{m-t} g, 0)} = C_{\theta(\epsilon_1, \epsilon_2)}\), which holds if and only if there exists an integer \(Y \geq 0\) such that \(\theta(\epsilon_1, \epsilon_2) = \theta(p^n-r' \ell^{m-t} g, 0) q^Y\) (mod \(4p^n \ell^m\)). This is equivalent to \(e_1 = -p^n-r' \ell^{m-t} g q^Y\) (mod \(4p^n\)) and \(e_2 = 0\) (mod \(\ell^m\)), from which we see that \(\epsilon_1\) must be of the form \(p^n-r' \ell^{m-t} g\) for some \(k' (0 \leq k' \leq 2\delta_r - 1)\) and \(e_2 = 0\). This gives \(g^{k-k'} q^Y \equiv -1\) (mod \(4p^n\)), which implies \(g^{k-k'} q^Y \equiv -1\) (mod \(4p^n\)). (c) When \(b\) is odd, we have \(s = 0\). Here working in a similar way as in Lemma 7(b), one can show that \(C_{-\theta(p^n, \ell^{m-t} h' q^t, 0)} = C_{\theta(p^n, \ell^{m-t} h' q^t, 0)}\), where \(u = [u + \frac{H_i}{2}]\), for each \(u\).

Next let \(b\) be even. Here \(s \in \{0, 1\}\). By Remark 1, we see that there exists an element \(\zeta \in \mathbb{S}_{p^n \ell^{m-t} h} h' q^t\) such that \(C_{-\theta(p^n, \ell^{m-t} h' q^t, 0)} = C_{\zeta}\). By Proposition 2(b), we write \(\zeta = \theta(\zeta_1, \zeta_2)\), where \((\zeta_1, \zeta_2)\) is either of the form \((p^n, 0)\) or \((p^n, \ell^{m-t} h' q^t)\) or \((p^n-r' \ell^{m-t} g, 0)\) or \((p^n-r' \ell^{m-t} g\ell^{m-t} h' q^t, 0)\) with \(0 \leq u' \leq \nu_1 - 1, 0 \leq k' \leq 2\delta_r - 1, 0 \leq w \leq f_{r', t} - 1, 1 \leq \ell' \leq n, 1 \leq t \leq m\), and \(s' \in \{0, 1\}\). That is, we have \(C_{-\theta(p^n-r' \ell^{m-t} g, 0)} = C_{\theta(\zeta_1, \zeta_2)}\), which holds if and only if there exists an integer \(Z \geq 0\) such that \(\theta(\zeta_1, \zeta_2) = -\theta(p^n-r' \ell^{m-t} g, 0) q^Z\) (mod \(4p^n \ell^m\)). This gives \(\zeta_1 = -p^n q^Z\) (mod \(4p^n\)) and \(\zeta_2 = -\ell^{m-t} h' q^t q^Z\) (mod \(\ell^m\)), which implies that \(\zeta_1 = p^n, Z \equiv 1\) (mod 2) and \(\zeta_2 = \ell^{m-t} h' q^t q^Z\), where \(0 \leq u' \leq \nu_1 - 1\) and \(s' \in \{0, 1\}\). This further gives \(h' q^t q^Z \equiv -1\) (mod \(\ell^t\)). By Lemma 6(c), we must have \(u' = u\), which implies that \(s - s' + Z \equiv \frac{u}{\mu_t}\) (mod \(\mu_t\)), or equivalently, \(Z \equiv s' - s + \frac{u}{\mu_t}\) (mod \(\mu_t\)). As \(\mu_t\) is even and \(Z \equiv 1\) (mod 2), we must have \(s - s' + \frac{u}{\mu_t} \equiv 1\) (mod 2). This gives \(s' \equiv s + \frac{u}{\mu_t}\) (mod 2), from which it follows that \(s' = s\) if \(b \equiv 2\) (mod 4) and \(s' = [s + 1]_2 = s\) if \(b \equiv 0\) (mod 4).

(d) Working in a similar way as above and as in Lemma 7(d), part (d) follows.

Proof of Theorem 2. It follows immediately from Lemmas 1 and 9, and Proposition 1.

4.3. \(q \equiv 3\) (mod 4) and \(a\) is odd

Throughout this subsection, let \(q \equiv 3\) (mod 4) and \(a\) be odd. In the following theorem, we observe that there does not exist any self-dual negacyclic
code of length $2p^n\ell^m$ over $\mathbb{F}_q$. We also determine all the self-orthogonal and complementary-dual negacyclic codes of length $2p^n\ell^m$ over $\mathbb{F}_q$.

**Theorem 4.** Let $q \equiv 3 \pmod{4}$ and $a$ be odd. Then there does not exist any self-dual negacyclic code of length $2p^n\ell^m$ over $\mathbb{F}_q$.

A. When $b$ is odd, there are precisely

- $3\frac{m}{2}^{\delta_2} + \nu_2 + 1$ distinct self-orthogonal negacyclic codes

\[
\left\langle M_{\theta(p^n, 0)}(x) \prod_{j \in J} M_j(x) \prod_{j' \in J'} \overline{M}_{j'}(x) \right\rangle
\]

of length $2p^n\ell^m$ over $\mathbb{F}_q$, and

- $2^{1+\frac{m}{2}^{\delta_2} + \nu_2 + 1}$ distinct complementary-dual negacyclic codes

\[
\left\langle M_{\theta(p^n, 0)}(x)^i \prod_{j \in J} M_j(x) \overline{\hat{M}}_{j}(x) \right\rangle
\]

of length $2p^n\ell^m$ over $\mathbb{F}_q$, with $i \in \{0, 1\}$ and $J, J'$ running over all subsets of $\tilde{S}_{4p^n\ell^m}$ satisfying $J \cup J' = \tilde{S}_{4p^n\ell^m}$, where

\[
\tilde{S}_{4p^n\ell^m} = \left\{ \bigcup_{r=1}^{m} \bigcup_{t=1}^{\ell^m-t+1} \bigcup_{k=0}^{p^n-r-1} \bigcup_{u=0}^{\ell^m-t} \bigcup_{w=0}^{r+q^w} \{ \theta(p^n-r g^k, 0), \theta(p^n, \ell^m-t h^u), \theta(p^n-r g^k+q^w, \ell^m-t h^u q^w) \} \right\}
\]

B. When $b \equiv 2 \pmod{4}$, there are precisely

- $3\frac{m}{2}^{\delta_2} + 2\nu_2 + 1$ distinct self-orthogonal negacyclic codes

\[
\left\langle \prod_{i \in I} M_i(x) \prod_{j \in J} M_j(x) \prod_{j' \in J'} \overline{M}_{j'}(x) \right\rangle
\]

of length $2p^n\ell^m$ over $\mathbb{F}_q$, and

- $2^{1+\frac{m}{2}^{\delta_2} + 2\nu_2 + 1}$ distinct complementary-dual negacyclic codes

\[
\left\langle \prod_{i \in I} M_i(x) \prod_{j \in J} M_j(x) \overline{\hat{M}}_{j}(x) \right\rangle
\]

of length $2p^n\ell^m$ over $\mathbb{F}_q$, with $I$ running over all subsets of $\tilde{S}_{4p^n\ell^m}$ and $J, J'$ running over all subsets of $\tilde{S}_{4p^n\ell^m}$ satisfying $J \cup J' = \tilde{S}_{4p^n\ell^m}$, where

\[
\tilde{S}_{4p^n\ell^m} = \{ \theta(p^n, 0) \} \cup \left( \bigcup_{t=1}^{\ell^m} \bigcup_{u=0}^{\ell^m-t} \{ \theta(p^n, \ell^m-t h^u), \theta(p^n, \ell^m-t h^u q) \} \right)
\]
Lemma 10.

\[ \mathcal{S}_{4^\nu \ell m} = \left( \bigcup_{t=1}^{m} \bigcup_{k=0}^{\frac{1}{2}\nu_t-1} \{ \theta(p^n-r g^k, 0), \theta(p^n-r g^k, \ell_m t_h u q^w) \} \right) \]

C. When \( b \equiv 0 \pmod{4} \), there are precisely

- \( 3^{\frac{1}{2}+\nu+\delta} \) distinct self-orthogonal negacyclic codes
  
  \[ \left\langle M_{\theta(p^n, 0)}(x) \prod_{j \in J} M_j(x) \prod_{j' \in J'} \overline{M}_{j'}(x) \right\rangle \]
  
  of length \( 2p^n \ell m \) over \( \mathbb{F}_q \), and

- \( 2^{1+\frac{1}{2}+\nu+\delta} \) distinct complementary-dual negacyclic codes
  
  \[ \left\langle M_{\theta(p^n, 0)}(x)^{\prime} \prod_{j \in J} M_j(x) \overline{M}_{j}(x) \right\rangle \]
  
  of length \( 2p^n \ell m \) over \( \mathbb{F}_q \),

with \( i \in \{0, 1\} \) and \( J, J' \) running over all subsets of \( \mathcal{S}_{4^\nu \ell m} \) satisfying

\[ J \cup J' = \mathcal{S}_{4^\nu \ell m}, \text{ where} \]

\[ \mathcal{S}_{4^\nu \ell m} = \left( \bigcup_{t=1}^{m} \bigcup_{k=0}^{\frac{1}{2}\nu_t-1} \{ \theta(p^n-r g^k, 0), \theta(p^n, \ell_m t_h u), \theta(p^n-r g^k, \ell_m t_h u q^w) \} \right). \]

To prove this theorem, we need to prove the following lemma:

Lemma 10. For \( 1 \leq r \leq n \) and \( 1 \leq t \leq m \), let \( 0 \leq u \leq \nu_t-1 \) and \( 0 \leq k \leq \delta_r-1 \) be fixed integers. For each \( r, t \), let \( y_r \) and \( z_t \) be as chosen in Lemma 6(a) with \( y_r^{-1} \) and \( z_t^{-1} \) as the multiplicative inverses of \( y_r \) and \( z_t \) modulo \( \lambda_r \) and \( \mu_t \), respectively. For \( 1 \leq r \leq m \) and \( 1 \leq t \leq n \), let \( w \) be an integer satisfying \( 0 \leq w \leq \ell_m t_h - 1 \), where \( \theta = 1 \) if \( b \) is odd and \( \theta = 2 \) if \( b \) is even. Then we have

\( C_{\theta(p^n, \ell_m t_h t u)} \) can be calculated as follows:

- For \( s \in \{0, 1\} \),
  
  \[ C_{\theta(p^n, \ell_m t_h u q^w)} = \begin{cases} 
  C_{\theta(p^n, \ell_m t_h u q^w)} & \text{if } \theta = 0 \pmod{4}; \\
  C_{\theta(p^n, \ell_m t_h u q^w)} & \text{if } \theta = 2 \pmod{4}; \\
  C_{\theta(p^n, \ell_m t_h u q^w)} & \text{if } \theta \text{ is odd}; \\
  C_{\theta(p^n, \ell_m t_h u q^w)} & \text{if } \theta \text{ is even};
  \end{cases} \]

- For \( \theta \neq 0 \pmod{4} \),
  
  \[ C_{\theta(p^n-r g^k, \ell_m t_h u q^w)} = \begin{cases} 
  C_{\theta(p^n-r g^k, \ell_m t_h u q^w)} & \text{if } \theta \text{ is odd}; \\
  C_{\theta(p^n-r g^k, \ell_m t_h u q^w)} & \text{if } \theta \text{ is even};
  \end{cases} \]

For \( \theta \neq 0 \pmod{4} \),

\[ \mathcal{S}_{4^\nu \ell m} = \left( \bigcup_{t=1}^{m} \bigcup_{k=0}^{\frac{1}{2}\nu_t-1} \{ \theta(p^n-r g^k, 0), \theta(p^n-r g^k, \ell_m t_h u q^w) \} \right). \]
with \( s = [s + 1]_2 \) for each \( s \in \{0, 1\} \), \( \hat{u}_t = [u + \frac{u}{2}]_\nu_t \), \( k^*_t = [k + \frac{\nu_t}{2}]_\delta_r \), where

\[
\hat{w}_{r,t} = \begin{cases} 
   \frac{w + (\lambda_r + 1)\nu_t^{-1} - (\mu_r + 1)\nu_t^{-1}}{2} & \text{if } 0 \leq k \leq \frac{\nu_t}{2} - 1 \text{ and } 0 \leq u \leq \frac{\nu_t}{2} - 1; \\
   \frac{w + (\lambda_r - 1)\nu_t^{-1} - (\mu_r + 1)\nu_t^{-1}}{2} & \text{if } \frac{\nu_t}{2} \leq k \leq \delta_r - 1 \text{ and } 0 \leq u \leq \frac{\nu_t}{2} - 1; \\
   \frac{w + (\lambda_r + 1)\nu_t^{-1} - (\mu_r - 1)\nu_t^{-1}}{2} & \text{if } 0 \leq k \leq \frac{\delta_r}{2} - 1 \text{ and } \frac{\delta_r}{2} \leq u \leq \nu_t - 1; \\
   \frac{w + (\lambda_r - 1)\nu_t^{-1} - (\mu_r - 1)\nu_t^{-1}}{2} & \text{if } \frac{\delta_r}{2} \leq k \leq \delta_r - 1 \text{ and } \frac{\delta_r}{2} \leq u \leq \nu_t - 1;
\end{cases}
\]

for \( 0 \leq w \leq f_{r,t} - 1 \) and \( \hat{w}_{r,t} \equiv w + \frac{\mu_r + 1)\nu_t^{-1}}{2} \pmod{f_{r,t}} \) and \( \hat{w}_{r,t} \equiv w + \frac{\mu_r + 2}{2} \pmod{2} \) for \( 0 \leq w \leq 2f_{r,t} - 1 \). (Note that the integer \( \hat{w}_{r,t} \) exists uniquely by Chinese Remainder Theorem.)

Proof. Working in a similar way as in Lemmas 7 and 9, the result follows. \( \square \)

Proof of Theorem 4. It follows immediately from Lemmas 1 and 10, and Proposition 1. \( \square \)

4.4. Examples

1. To list all self-dual, self-orthogonal and complementary-dual negacyclic codes of length 374 over \( \mathbb{F}_5 \), let \( p = 11, \ell = 17, q = 5 \) and \( m = n = 1 \). Here we have \( a = 5, b = 16, g = 13 \) and \( h = 5 \) so that \( f = \gcd(a, b) = 1 \). As \( q \equiv 1 \pmod{4} \), by Theorem 2, we see that there are precisely
   - 64 distinct self-dual negacyclic codes
     \[
     \left\langle \prod_{j \in J} M_j(x) \prod_{k \in \tilde{S}_{748} \setminus J} \overline{M}_k(x) \right\rangle
     \]
     of length 374 over \( \mathbb{F}_5 \),
   - 729 distinct self-orthogonal negacyclic codes
     \[
     \left\langle \prod_{j \in J} M_j(x) \prod_{j' \in J'} M_{j'}(x) \right\rangle
     \]
     of length 374 over \( \mathbb{F}_5 \),
   - 64 distinct complementary-dual negacyclic codes
     \[
     \left\langle \prod_{j \in J} M_j(x) \overline{M}_{j'}(x) \right\rangle
     \]
     of length 374 over \( \mathbb{F}_5 \),

with \( J, J' \) running over all subsets of \( \tilde{S}_{748} \) satisfying \( J \cup J' = \tilde{S}_{748} \), where \( \tilde{S}_{748} = \{1, 187, 221, 409, 629, 715\} \).

2. Now we will list all self-orthogonal and complementary-dual negacyclic codes of length 286 over \( \mathbb{F}_3 \). For this, we take \( p = 11, \ell = 13, q = 3 \) and \( n = \)}
Here we have $a = 5$, $b = 3$, $g = 13$, and $h = 2$ with $f = \gcd(a, b) = 1$. As $q \equiv 3 \pmod{4}$ and both $a, b$ are odd, by Theorem 4, we see that there does not exist any self-dual negacyclic code of length 286 over $\mathbb{F}_3$. Further by Theorem 4(A) again, we see that there are precisely

- 2187 distinct self-orthogonal negacyclic codes

$$\langle M_{143}(x) \prod_{j \in J} M_j(x) \prod_{j' \in J'} \hat{M}_{j'}(x) \rangle$$

of length 286 over $\mathbb{F}_3$, and

- 256 distinct complementary-dual negacyclic codes

$$\langle M_{143}(x)^i \prod_{j \in J} M_j(x) \hat{M}_j(x) \rangle$$

of length 286 over $\mathbb{F}_3$,

with $i \in \{0, 1\}$ and $J, J'$ running over all subsets of $\tilde{S}_{572}$ satisfying $J \cup J' = \tilde{S}_{572}$, where $\tilde{S}_{572} = \{1, 145, 221, 275, 353, 365, 495\}$.

References


[18] A. Sharma, Constacyclic codes over finite fields, Communicated for publication.


[20] , Self-orthogonal and complementary-dual cyclic codes of length $p^n \ell^m$ over a finite field, Communicated for publication.


Department of Mathematics
Indian Institute of Technology Delhi
New Delhi 110016, India
E-mail address: anuradha@maths.iitd.ac.in