On MDS Negacyclic LCD Codes

Mustafa Sarı and Mehmet Emin Köröglu

Department of Mathematics, Faculty of Art and Science
Yıldız Technical University, Esenler, Istanbul 34220, Turkey

Abstract

This paper is devoted to the study of linear codes with complementary-duals (LCD) arising from negacyclic codes over finite fields \( \mathbb{F}_q \), where \( q \) is an odd prime power. We obtain two classes of MDS negacyclic LCD codes of length \( n|\frac{q-1}{2} \), \( n|\frac{q+1}{2} \) and a class of negacyclic LCD codes of length \( n = q+1 \). Also, we drive some parameters of Hermitian negacyclic LCD codes over \( \mathbb{F}_{q^2} \) of length \( n = q^2 - 1 \) and \( n = q - 1 \). For both Euclidean and Hermitian cases the dimension of these codes are determined and for some classes the minimum distance is settled. For the other cases, by studying \( q \) and \( q^2 \)-cyclotomic classes we give lower bounds on the minimum distance.

Keywords: Linear codes, Negacyclic codes, LCD codes, Euclidean inner product, Hermitian inner product

2008 MSC: 94B15, 94B05

1. Introduction

Linear codes with complementary-duals (LCD codes), which was introduced by Massey in 1992 (see [3]), have many applications in cryptography, communication systems, data storage and consumer electronics. A linear code is called an LCD code if \( C \perp \cap C = \{0\} \), which is equivalent to \( C \perp \oplus C = \mathbb{F}_q^n \). LCD codes provides an optimum linear coding solution for binary adder channel [3] and in [4] it is shown that asymptotically good LCD codes exist. Also, in [5] Sendrier proved that LCD codes meet Gilbert-Varshamov bound. In [6] necessary and sufficient condition for a cyclic code to have a complementary dual was given by Yang and Massey. In [7] it is
shown that if $\lambda^2 \neq 1$, then any $\lambda-$constacyclic code of length $n$ over finite field $\mathbb{F}_q$ is LCD. All LCD constacyclic codes of length $2^l p^s$ are determined in [8]. The LCD condition for a certain class of quasi cyclic codes studied in [9]. In [10] a linear programming bound on the largest size of an LCD code of given length and minimum distance was developed. Guneri et al. introduced Hermitian LCD codes in [11]. In [12] a class of MDS LCD negacyclic codes of length $n \mid q - 1$ was given. Carlet and Gulle studied an applications of LCD codes against side-channel attacks, and presented particular constructions for LCD codes in [13].

In this work, we get two classes of MDS negacyclic LCD codes of length $n \mid \frac{q^2 - 1}{2}$, $n \mid \frac{q + 1}{2}$ and a class of negacyclic LCD codes of length $n = q + 1$. Also, we studied the structure of Hermitian negacyclic LCD codes over $\mathbb{F}_{q^2}$ and we drive some parameters for lengths $n = q^2 - 1$ and $n = q - 1$. For both Euclidean and Hermitian cases the dimension of these codes are determined and for some classes the minimum distance settled. For the other cases, by studying $q$ and $q^2-$cyclotomic cosets we give lower bounds on the minimum distance.

This paper is organized as follows. In Section 2 we provide some required backgrounds. In Section 3 we derive some classes of LCD codes of length $n \mid \frac{q^2 - 1}{2}$, $n \mid \frac{q + 1}{2}$ from negacyclic codes and we show that these codes are MDS. Further, by studying its defining set we determine parameters of a class of LCD codes of length $n = q - 1$. In Section 4 we handled Hermitian negacyclic LCD codes over $\mathbb{F}_{q^2}$. The last Section is devoted to conclusion.

2. Backgrounds

In this section, we will give some preliminaries which required for the subsequent sections. Let $q$ be a prime power and $\mathbb{F}_q$ be the finite field with $q$ elements. An $[n, k]_q$ linear code $C$ of length $n$ over $\mathbb{F}_q$ is a $k-$dimensional subspace of the vector space $\mathbb{F}_q^n$. The elements of $C$ are of the form $(c_0, c_1, \ldots, c_{n-1})$ and called as codewords. The Hamming weight of any $c \in C$ is the number of nonzero coordinates of $c$ and denoted by $w(c)$. The minimum distance of $C$ is defined as $d = \min \{ w(c) \mid 0 \neq c \in C \}$. An $[n, k]_q$ linear code with minimum distance $d$ is said to be MDS (maximum distance separable) if $n + 1 = k + d$. The Euclidean dual code of $C$ is defined to be

$$C^\perp = \left\{ x \in \mathbb{F}_q^n \mid \sum_{i=0}^{n-1} x_i y_i = 0, \forall y \in C \right\}.$$
A code $C$ is Euclidean self-orthogonal if $C^\perp \subset C$ and Euclidean self-dual if $C^\perp = C$. Let $\langle x, y \rangle = \sum_{i=0}^{n-1} x_i y_i^q$ be the Hermitian inner product of $x$ and $y \in \mathbb{F}_q^n$ and $C$ be a code of length $n$ over $\mathbb{F}_q$. The Hermitian dual code of $C$ is defined to be $C^{\perp H} = \left\{ x \in \mathbb{F}_q^n \middle| \sum_{i=0}^{n-1} x_i y_i^q = 0, \forall y \in C \right\}$. A code $C$ is Hermitian self-orthogonal if $C^{\perp H} \subset C$ and Hermitian self-dual if $C^{\perp H} = C$.

Let $\alpha$ be a non-zero element of $\mathbb{F}_q$. A linear code $C$ of length $n$ over $\mathbb{F}_q$ is said to be $\alpha$-constacyclic if for any codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$ we have that $(\alpha c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. An $\alpha$-constacyclic codes of length $n$ over $\mathbb{F}_q$ correspond to the principal ideal $\langle g(x) \rangle$ of the quotient ring $\mathbb{F}_q[x]/\langle x^n - \alpha \rangle$ where $g(x)|x^n - \alpha$. The roots of the code $C$ are the roots of the polynomial $g(x)$. So, if $\beta_1, \beta_2, \ldots, \beta_{n-k}$ are the zeros of $g(x)$ in the splitting field of $x^n - \alpha$, then $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ if and only if $c(\beta_1) = c(\beta_2) = \ldots = c(\beta_{n-k}) = 0$, where $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$.

In particular, for $\alpha = 1$ the class of constacyclic codes are called cyclic codes and for $\alpha = -1$ the class of constacyclic codes are called negacyclic codes.

Let $r = \text{ord}_q(\alpha)$ and the multiplicative order of $q$ modulo $rn$ be $m$. There exists $\delta \in \mathbb{F}_q^n$ called a primitive $rn$th roots of unity, such that $\delta^n = \alpha$. Let $\zeta = \delta^r$, then $\zeta$ is a primitive $n$th root of unity. Therefore, the roots of $x^n - \alpha$ are $\{\delta, \delta^{1+r}, \ldots, \delta^{1+(n-1)r}\}$ and the roots of $x^n - \alpha^{-1}$ are $\{\delta^{-1}, \delta^{-1+r}, \ldots, \delta^{-1+(n-1)r}\}$. Define $O_{r,n}(1)$ and $O_{r,n}(-1)$ as follows:

$$
O_{r,n}(1) = \{1 + ri | 0 \leq i \leq n - 1 \} \mod rn \subseteq \mathbb{Z}_{rn},
$$

$$
O_{r,n}(-1) = \{-1 + ri | 0 \leq i \leq n - 1 \} \mod rn \subseteq \mathbb{Z}_{rn}.
$$

The defining set of the $\alpha$-constacyclic code $C$ is defined as

$$
Z = \{1 + ri \in O_{r,n}(1) | \delta^{1+ir} \text{ is a root of } C\}.
$$

(1)

Clearly, $Z \subset O_{r,n}(1)$ and the dimension of $C$ is $n - |Z|$. Let

$$
\mathbb{Z}_{rn} = \{0, 1, 2, \ldots, rn - 1\},
$$

denoting the ring of integers modulo $rn$. For any $s \in \mathbb{Z}_{rn}$, the $q$-cyclotomic coset of $s$ modulo $rn$ is defined by $C_s = \{sq^j (\mod rn) | j \in \mathbb{Z} \}$. The smallest integer in $C_s$ is called coset leader of $C_s$. Let $\pi_{(rn,q)}$ be the set of all the
coset leaders. Then, we have $C_s \cap C_t = \emptyset$ for any distinct $s$ and $t$ in $\pi_{(r_n,q)}$, and $\bigcup_{s \in \pi_{(n,q)}} C_s = \mathbb{Z}_{r_n}$. The minimal polynomial $m_s(x)$ of $\zeta$ over $\mathbb{F}_q$ is a monic polynomial of smallest degree over $\mathbb{F}_q$ with $\zeta$ as a root. This polynomial is given $m_s(x) = \prod_{i \in C_s} (x - \zeta^i) \in \mathbb{F}_q[x]$, which is irreducible over $\mathbb{F}_q$. It then follows that $x^n - \alpha = \prod_{s \in \mathcal{O}_{r_n,1}} m_s(x)$ and $x^{rn} - 1 = \prod_{s \in \pi_{(n,q)}} m_s(x)$.

Assume the generator polynomial of $C$ is $g(x) = \sum_{i=0}^{k} g_i x^i$, where $g_i \in \mathbb{F}_q$. If $g(\nu) = 0$ for some $\nu \in \mathbb{F}_q^m$, then

$$g(\nu^q) = \sum_{i=0}^{k} g_i (\nu^q)^i = \sum_{i=0}^{k} g_i (\nu^q)^i = \left( \sum_{i=0}^{k} g_i \nu^i \right)^q = (g(\nu))^q = 0.$$ 

Thus, the defining set $Z$ is a union of some $q$-cyclotomic cosets modulo $r_n$ and a union of some $q$-cyclotomic cosets modulo $rn$ is also the defining set of some $\alpha$-constacyclic code.

The following is a well known result in literature.

**Theorem 1.** [7, 8] (BCH bound for constacyclic codes) Let $(n, q) = 1$ and also let $\delta$ be an $rn$th root of unity with $\delta^n = \alpha$ where $\alpha \in \mathbb{F}_q^\times$ and $r$ is the multiplicative order $\alpha$ in $\mathbb{F}_q^\times$. Then, the minimum distance of an $\alpha$-constacyclic code of length $n$ over $\mathbb{F}_q$ with the defining set $Z = \{1 + rj, l \leq j \leq l + d - 2\}$ is at least $d$.

The following results are analogue to the Theorem 5 given in [16].

**Theorem 2.** Let $C = \langle g(x) \rangle$ be an $\alpha$-constacyclic code over $\mathbb{F}_q$. Then, the following statements are equivalent

1. $C$ is an LCD code.
2. $g(x)$ is self reciprocal.
3. $\delta^{-1}$ is a root of $g(x)$ for every root $\delta$ of $g(x)$ over the splitting field of $g(x)$.

Let $\Pi_{(nr,q)} \subset O_{r,n}(1)$ such that $\{C_a \cup C_{rn-a} | a \in \Pi_{(nr,q)}\}$ is a partition of $O_{r,n}(1)$. Every reversible $\alpha$-constacyclic codes of length $n$ over $\mathbb{F}_q$ is...
generated by a polynomial \( g(x) = \prod_{a \in S} \text{lcm}(m_a(x), m_{rn-a}(x)) \), where \( S \) is a nonempty subset of \( \Pi_{(nr,q)} \).

In the following, we give some preparatory about Hermitian dual of an \( \alpha \)-constacyclic code over \( \mathbb{F}_{q^2} \). For further and detailed information readers can refer to [14].

**Lemma 3.** [14]. Let \( C \) be an \( \alpha \)-constacyclic code over \( \mathbb{F}_{q^2} \), then the Hermitian dual code \( C^\perp_H \) is an \( \alpha^{-q} \)-constacyclic code generated by \( g^\perp(q)(x) = \sum_{i=0}^{k} h_i h_0^{-1} x^{k-i} \) and \( \xi_1, \ldots, \xi_k \) be the roots of \( g^\perp(x) = \sum_{i=0}^{k} h_i h_0^{-1} x^{k-i} \), then \( \xi_1^q, \ldots, \xi_k^q \) are the roots of \( g^\perp(q)(x) \).

Let \( C \) be an \( \alpha \)-constacyclic code over \( \mathbb{F}_{q^2} \) with defining set \( Z \) and let \( Z^\perp = -(O_{r,n}(1) \setminus Z) \subset O_{r,n}(-1) \) be the defining set of the code \( C_{Z^\perp} \). Then \( x^n - \alpha = \prod_{i \in O_{r,n}(1)} (x - \delta^i) = \prod_{i \in Z} (x - \delta^i) \prod_{i \in Z^\perp} (x - \delta^{-i}) = g(x) h(x) \), where \( g(x) \) is the generator polynomial of \( C_Z \). By Lemma 3, \( g^\perp(x) = \prod_{i \in Z^\perp} (x - \delta^i) \).

Hence, \( Z^\perp \) is the defining set of the Euclidean dual of \( C_Z \). So we have \( C_{Z^\perp} = C_Z^\perp \). Let \( Z = qZ^\perp = -q(O_{r,n}(1) \setminus Z) \). Then \( Z \) is the union of some \( q^2 \)-cyclotomic cosets modulo \( rn \) and \( |Z| + |Z^\perp| = n \). Also \( g^\perp(q)(x) = \prod_{i \in Z} (x - \delta^{iq}) \). Hence, \( Z \) is the defining set of \( \alpha^{-q} \)-constacyclic code \( C_Z^{\perp H} \).

**Theorem 4.** [15]. \( C^\perp_Z \) is the Hermitian dual of \( C_Z \).

An immediate result of Theorem 2 for Hermitian LCD codes we have the following.

**Theorem 5.** Let \( C = \langle g(x) \rangle \) be an \( \alpha \)-constacyclic code over \( \mathbb{F}_{q^2} \). Then, the following statements are equivalent,

1. \( C \) is an Hermitian LCD code.
2. \( g(x) \) is Hermitian self-reciprocal.
3. \( \delta^{-q} \) is a root of \( g(x) \) for every root \( \delta \) of \( g(x) \) over the splitting field of \( g(x) \).

The following Corollary is a direct result of Theorem 5.

**Corollary 6.** Hermitian LCD \( \alpha \)-constacyclic codes over \( \mathbb{F}_{q^2} \) of length \( n \) exists if and only if \( C_s = C_{-qs} \) for some \( s \in O_{r,n}(1) \), where \( C_s \) is a \( q^2 \)-cyclotomic coset modulo \( rn \).

Proof. Follows from Theorem 5. \( \square \)
3. New MDS LCD codes from negacyclic codes

In this section, we aim to derive some classes of LCD codes from negacyclic codes and show that these codes are MDS. For this aim, we first determine what the defining set $Z$ of negacyclic codes should be to satisfy $Z = -Z$ and to contain consecutive terms and then construct MDS negacyclic LCD codes from these negacyclic codes with the defining set $Z$. We commence with the length $n$ dividing $\frac{q-1}{2}$.

3.1. New MDS negacyclic LCD codes of length $n$, where $n | \frac{q-1}{2}$

Let $q$ be an odd prime power and let $n | \frac{q-1}{2}$, where $n \geq 3$. It is then clear that $q \equiv 1 \mod 2n$ and so each $q$-cyclotomic coset modulo $2n$ has exactly one element, that is, $C_{1+2j} = \{1 + 2j\}$ for all $0 \leq j \leq n-1$. We also have:

**Lemma 7.** For all $0 \leq j \leq n-1$, $-C_{1+2j} = C_{1+2(n-j-1)}$. Moreover, if $n$ is odd and $j = \frac{n-1}{2}$, then $-C_{1+2j} = C_{1+2j}$.

**Proof.** $-(1 + 2j) \equiv 2n - (1 + 2j) = 1 + 2(n-j-1) \mod 2n$. If $n$ is odd and $j = \frac{n-1}{2}$, then $j = n - j - 1$. 

We give in the following the number of LCD negacyclic codes of length $n$ without proof.

**Corollary 8.** If $n$ is even, the number of nontrivial LCD negacyclic codes of length $n$ is $2 \left(2^{\frac{n-2}{2}} - 1\right)$. If $n$ is odd, the number of nontrivial LCD negacyclic codes of length $n$ is $2 \left(2^{\frac{n-1}{2}} - 1\right)$.

For odd $n$, we define the defining set $Z_1 = \bigcup_{i=0}^{l} C_{1+2(\frac{n-1}{2}+i)}$, where $0 \leq l \leq \frac{n-3}{2}$. For even $n$, we define the defining set $Z_2 = \bigcup_{i=0}^{k} C_{1+2(\frac{n}{4}+i)} \cup C_{1+2(\frac{n}{4}-i)}$, where $0 \leq k \leq \frac{n-4}{2}$. By Lemma 7, it is immediate that $-Z_1 = Z_1$ and $-Z_2 = Z_2$ for each $0 \leq l \leq \frac{n-3}{2}$ and $0 \leq k \leq \frac{n-4}{2}$, respectively. Now we are ready to introduce two classes of new LCD negacyclic codes of length $n$ which are MDS.

**Theorem 9.** Let $q$ be an odd prime power and let $n | \frac{q-1}{2}$ such that $n \neq 1$. For even $n$, a class of MDS negacyclic LCD codes with the parameters $[n, n-2\lambda, 2\lambda + 1]_q$, where $1 \leq \lambda \leq \frac{n-2}{2}$, exists. For odd $n$, a class of MDS negacyclic LCD codes with the parameters $[n, n-2\lambda-1, 2(\lambda+1)]_q$, where $0 \leq \lambda \leq \frac{n-3}{2}$, exists.
Table 1: Some MDS negacyclic LCD codes obtained from Theorem 9

| q  | n  | λ       | MDS Negacyclic LCD Codes          |
|----|----|---------|-----------------------------------|
| 7  | 3  | 0       | [3, 2, 2]_{7}                      |
| 9  | 4  | 1       | [4, 2, 3]_{9}                      |
| 11 | 5  | 0 ≤ λ ≤ 1 | [5, 4 − 2λ, 2 (λ + 1)]_{11}       |
| 13 | 6  | 1 ≤ λ ≤ 2 | [6, 6 − 2λ, 2λ + 1]_{13}         |
| 17 | 8  | 1 ≤ λ ≤ 3 | [8, 8 − 2λ, 2λ + 1]_{17}         |
| 17 | 4  | 1       | [4, 2, 3]_{17}                     |
| 19 | 9  | 0 ≤ λ ≤ 3 | [9, 8 − 2λ, 2 (λ + 1)]_{19}       |
| 19 | 3  | 0       | [3, 2, 2]_{19}                     |

Proof. Let \( n \) be even and let \( C \) be a negacyclic code of length \( n \) having the defining set \( Z_2 \) over \( \mathbb{F}_q \). Clearly, \( Z_2 \) consists of \( 2\lambda \) consecutive terms, where \( 1 ≤ \lambda ≤ \frac{n−2}{2} \) and so, by Theorem 1, \( C \) has at least minimum distance \( 2\lambda + 1 \). By the dimension of \( C \) and the definition of MDS codes, \( C \) has desired parameters and is MDS.

Let \( n \) be odd and let \( C \) be a negacyclic code of length \( n \) having the defining set \( Z_1 \) over \( \mathbb{F}_q \). It is easy to see that \( Z_1 \) consists of \( 2\lambda + 1 \) consecutive terms, where \( 0 ≤ \lambda ≤ \frac{n−3}{2} \). Therefore, by Theorem 1, \( C \) has at least minimum distance \( 2\lambda + 2 \). By the dimension of \( C \) and the definition of MDS codes, \( C \) has desired parameters and is MDS.

Example 10. We present some parameters of MDS negacyclic LCD codes obtained by Theorem 9 in Table 1.

3.2. New MDS negacyclic LCD codes of length \( n \), where \( n|\frac{q+1}{2} \)

Let \( q \) be an odd prime power and let \( n|\frac{q+1}{2} \) such that \( n ≥ 3 \). In this case, since \( q \equiv -1 \mod 2n \), each \( q \)-cyclotomic coset modulo \( 2n \) has at most two elements. We give all \( q \)-cyclotomic cosets modulo \( 2n \).

Lemma 11. All \( q \)-cyclotomic cosets modulo \( 2n \) are as follow:

1. If \( n \) is even, then each cyclotomic coset has exactly two elements, i.e. \( C_{1+2j} = \{1 + 2j, 1 + 2(n−1 − j)\} \) for all \( 0 ≤ j ≤ \frac{n}{2} − 1 \).
2. If \( n \) is odd, then each cyclotomic coset has exactly two elements except one, i.e. \( C_{1+2j} = \{1 + 2j, 1 + 2(n−1 − j)\} \) for all \( 0 ≤ j ≤ \frac{n−3}{2} \) but \( C_{1+2j} = \{1 + 2j\} \) for \( j = \frac{n−1}{2} \).
Proof. Since \( q \equiv -1 \mod 2n \), we get \( q(1+2j) \equiv -1-2j = 1+2(n-1-j) \mod 2n \). If \( n \) is odd and \( j = \frac{n-1}{2} \), \( j = n-1-j \) and so \( C_{1+2j} = \{1+2j\} \). □

The following is immediately concluded from Lemma 11 and we omit the proof.

**Corollary 12.** For all \( q \)-cyclotomic cosets modulo \( 2n \) containing \( 1+2j \), \(-C_{1+2j} = C_{1+2j} \).

We define the defining sets \( Z_1 \) and \( Z_2 \) with respect to the cases of \( n \) as follow: If \( n \) is even, \( Z_1 = \bigcup_{j=l}^{n-1} C_{1+2j} \) where \( 1 \leq l \leq \frac{n}{2} - 1 \). If \( n \) is odd, \( Z_2 = \bigcup_{j=k}^{n^2} C_{1+2j} \) where \( 1 \leq k \leq \frac{n-1}{2} \). Then, by Lemma 11, we get \( Z_1 = \{1+2l, 1+2(l+1), \ldots, 1+2(\frac{n}{2}-l), \ldots, 1+2(n-1-l)\} \) and \( Z_2 = \{1+2k, 1+2(k+1), \ldots, 1+2(\frac{n-1}{2}), \ldots, 1+2(n-1-k)\} \) where \( 1 \leq l \leq \frac{n}{2} - 1 \) and \( 1 \leq k \leq \frac{n-1}{2} \), respectively. So, \( Z_1 \) comprise exactly \( n-2l \) consecutive terms and \( Z_2 \) consists of exactly \( n-2k \) consecutive terms. Moreover, Corollary 12 implies that \(-Z_1 = Z_1 \) and \(-Z_2 = Z_2 \). We at present willing to derive new MDS negacyclic LCD codes of length \( n \) dividing \( q+1 \).

**Theorem 13.** Let \( q \) be an odd prime power and let \( n | \frac{q+1}{2} \) such that \( n \neq 1 \). For even \( n \), a family of MDS negacyclic LCD codes with the parameters \([n, 2l, n-2l+1]_q\), where \( 1 \leq l \leq \frac{n}{2} - 1 \), exists. For odd \( n \), a family of MDS negacyclic LCD codes with the parameters \([n, 2k, n-2k+1]_q\), where \( 1 \leq k \leq \frac{n-1}{2} \), exists.

**Proof.** If \( n \) is even, take \( C \) as a negacyclic code of length \( n \) having the defining set \( Z_1 \) over \( \mathbb{F}_q \). Clearly, \( Z_1 \) consists of \( n-2l \) consecutive terms, where \( 1 \leq l \leq \frac{n}{2} - 1 \) and so, by Theorem 1, \( C \) has at least minimum distance \( n-2l+1 \). By the dimension of \( C \) and the definition of MDS codes, \( C \) has desired parameters and is MDS.

If \( n \) is odd, take \( C \) as a negacyclic code of length \( n \) having the defining set \( Z_2 \) over \( \mathbb{F}_q \). It is easy to see that \( Z_2 \) consists of \( n-2k \) consecutive terms, where \( 1 \leq k \leq \frac{n-1}{2} \). Therefore, by Theorem 1, \( C \) has at least minimum distance \( n-2k+1 \). By the dimension of \( C \) and the definition of MDS codes, \( C \) has desired parameters and is MDS. □

**Example 14.** We present some parameters of MDS negacyclic LCD codes obtained by Theorem 13 in Table 2.
Table 2: Some MDS negacyclic LCD codes obtained from Theorem 13

| q | n | l, k | MDS Negacyclic LCD Codes |
|---|---|------|------------------------|
| 5 | 3 | 1    | \([3, 2, 2]_5\)         |
| 7 | 4 | 1    | \([4, 2, 3]_7\)         |
| 9 | 5 | 1 ≤ k ≤ 2 | \([5, 2k, 5 - 2k + 1]_9\) |
| 11| 6 | 1 ≤ l ≤ 2 | \([6, 2l, 6 - 2l + 1]_{11}\) |
| 11| 3 | 1    | \([3, 2, 2]_{11}\)       |
| 13| 7 | 1 ≤ k ≤ 3 | \([7, 2k, 7 - 2k + 1]_{13}\) |
| 17| 9 | 1 ≤ k ≤ 4 | \([9, 2k, 9 - 2k + 1]_{17}\) |
| 17| 3 | 1    | \([3, 2, 2]_{17}\)       |
| 19| 10| 1 ≤ l ≤ 4 | \([10, 2l, 10 - 2l + 1]_{19}\) |
| 19| 5 | 1 ≤ k ≤ 2 | \([5, 2k, 5 - 2k + 1]_{19}\) |

3.3. New negacyclic LCD codes of length \(n = q + 1\)

Let \(q\) be an odd prime power and let \(n = q + 1\) such that \(4|n\). In this subsection, we derive negacyclic codes of length \(q + 1\) which do not have to be MDS. It follows from \(q \not\equiv 1 \mod 2(q + 1)\) and \(q^2 \equiv 1 \mod 2(q + 1)\) that each \(q\)-cyclotomic coset modulo \(2n\) has at most two elements.

Suppose \(q(1 + 2j) \equiv (1 + 2j) \mod 2(q + 1)\) for some \(0 ≤ j ≤ n - 1\). Since \((q - 1, q + 1) = 2\) and \(1 ≤ 1 + 2j ≤ 2n - 1\), we get \(2j = q\), which is a contradiction. This implies that each \(q\)-cyclotomic coset modulo \(2(q + 1)\) has precisely two elements. We give an exact characterization for all \(q\)-cyclotomic coset modulo \(2n\).

Lemma 15. All \(q\)-cyclotomic cosets modulo \(2(q + 1)\) are as follow:

1. \(C_{1 + 2j} = \{1 + 2j, 1 + 2(\frac{q - 1}{2} - j)\}\) for all \(0 ≤ j ≤ \frac{q - 3}{4}\).
2. \(C_{1 + 2j} = \{1 + 2j, 1 + 2(n + \frac{q - 1}{2} - j)\}\) for all \(\frac{q + 1}{2} ≤ j ≤ \frac{3q - 1}{4}\).

Proof. If \(0 ≤ j ≤ \frac{q - 3}{4}\), then \(j < \frac{q - 1}{2}\). Since \(2qj \equiv -2j \mod 2n\), \(q(1 + 2j) \equiv q - 2j = 1 + 2(\frac{q - 1}{2} - j) \mod 2n\). If \(\frac{q + 1}{2} ≤ j ≤ \frac{3q - 1}{4}\), then \(j > \frac{q - 1}{2}\) and so \(q(1 + 2j) \equiv 1 + 2(n + \frac{q - 1}{2} - j) \mod 2n\). The union of all \(q\)-cyclotomic cosets presented here gives the set \(O_{2q+1}(1)\) and so proof is completed.

Lemma 16. For all \(0 ≤ j ≤ \frac{q - 3}{4}\), \(-C_{1 + 2j} = C_{1 + 2(\frac{q + 1}{2} + j)}\).

Proof. See that \(-(1 + 2j) \equiv 1 + 2(n - j - 1) \mod 2n\). By Lemma the first part of [13], we need to find \(k\) satisfying \(n + \frac{q + 1}{2} - k = n - j - 1\). Then, \(k = \frac{q + 1}{2} + j\).
Table 3: Some negacyclic LCD codes obtained from Theorem 17

| $q$ | $n$ | $1 \leq \lambda \leq \frac{q-3}{4}$ | Negacyclic LCD Codes |
|-----|-----|-----------------------------------|----------------------|
| 19  | 20  | $4\lambda, \geq 11 - 2\lambda_{19}$ |
| 23  | 24  | $4\lambda, \geq 13 - 2\lambda_{23}$ |

As a result of Lemma 16, one can see that $C_{1+2j} \neq -C_{1+2j}$ for all $0 \leq j \leq n-1$. We define the defining set $Z$ to be $Z = \bigcup_{j=l}^{3q+1} C_{1+2j}$, where $1 \leq l \leq \frac{q-3}{4}$. Then, by Lemma 15 we get

$$Z = \left\{ 1 + 2l, 1 + 2(l + 1), \ldots, 1 + 2 \left( \frac{q-1}{2} - l \right), 1 + 2 \left( \frac{q+1}{2} + l \right), 1 + 2 \left( \frac{q+3}{2} + l \right), \ldots, 1 + 2(q - l) \right\}.$$

Clearly, $Z$ contains $\frac{q+1}{2} - 2l$ consecutive terms and $|Z| = q + 1 - 4l$. These facts provide us to derive a class of LCD negacyclic codes.

**Theorem 17.** Assume that $q$ is an odd prime power and $n = q + 1$ such that $4|n$. Then, a class of LCD negacyclic codes with parameters

$$\left[ q + 1, 4\lambda, d \geq \frac{q + 3}{2} - 2\lambda \right]_q$$

where $1 \leq \lambda \leq \frac{q-3}{4}$, exists.

**Proof.** Let $C$ be a negacyclic codes of length $q + 1$ with defining set $Z$ over $\mathbb{F}_q$. The parameters of $C$ are followed from that $Z$ involve in $\frac{q+1}{2} - 2\lambda$ consecutive terms and $|Z| = q + 1 - 4\lambda$.

**Example 18.** We list some parameters of negacyclic LCD codes acquired by Theorem 17 in Table 3.

4. Negacyclic Hermitian LCD Codes

In this section, we use negacyclic codes of lengths $n = q - 1$ and $n = q^2 + 1$ to construct Hermitian LCD codes over $\mathbb{F}_{q^2}$, where $q$ is an odd prime power. To accomplish this task, we have to determine the defining set $Z$ of negacyclic codes with the restriction $Z = -qZ$ and the number of consecutive terms. At first, we need to determine $q^2$–cyclotomic coset modulo $2n$. Basics about Hermitian dual of an $\alpha$–constacyclic code over $\mathbb{F}_{q^2}$ can be found in [14].
4.1. Negacyclic MDS Hermitian LCD codes of length $n = q - 1$

In this subsection, we use negacyclic codes of lengths $n = q - 1$ to construct Hermitian LCD codes, where $q$ is an odd prime power. Since $(q - 1) \mid (q^2 - 1)$ and gcd $(q - 1, q + 1) = 2$ we have $q^2 = 1 + 2 (q - 1) \frac{(q + 1)}{2} \equiv 1 \pmod{2(q - 1)}$. This means that each $q^2$-cyclotomic coset modulo $2n$ has only one element. We define the defining set $Z$ as

$$Z = \left\{ \begin{array}{ll}
\frac{q-3}{4} & \text{if } q \equiv 1 \pmod{4}, \\
\bigcup_{j=l}^{(q-3)/4} C_{1+2j} \cup -qC_{1+2j}, & \text{where } \frac{q-1}{4} \leq l \leq \frac{q-3}{2} \\
\bigcup_{j=l}^{(q-3)/4} C_{1+2j} \cup -qC_{1+2j}, & \text{where } \frac{q-3}{4} \leq l \leq \frac{q-3}{2}
\end{array} \right. \quad \text{if } q \equiv 3 \pmod{4}.$$}

**Lemma 19.** Let $n = q - 1$. Then for all $0 \leq j \leq \frac{q-3}{2}$, we have that $-qC_{1+2j} = C_{1+2j}(-q)$.

**Proof.** Observe that $-q(1 + 2j) = 2(q - 1) - q(1 + 2j) = 1 + 2 \left( \frac{(q-3)}{2} - qj \right)$. \qed

As a result of Lemma 19 we have the following.

**Lemma 20.** Let $n = q - 1$.

1. If $q \equiv 1 \pmod{4}$, then for all $\frac{q-1}{4} \leq j \leq \frac{q-3}{2}$ we have that $-qC_{1+2j} \neq C_{1+2j}$.
2. If $q \equiv 3 \pmod{4}$, then for $j = \frac{q-3}{4}$ we have $-qC_{1+2j} = C_{1+2j}$ and for all $\frac{q-3}{4} < j \leq \frac{q-3}{2}$ we have $-qC_{1+2j} \neq C_{1+2j}$.

**Proof.**

1. Contrary to the assumption for some $j$ suppose that $-qC_{1+2j} = C_{1+2j}$. Then by Lemma 19 we have that

$$-q(1 + 2j) \equiv 1 + 2j \pmod{2(q - 1)}.$$}

Therefore, we have $(q + 1)(1 + 2j) \equiv 0 \pmod{2(q - 1)}$. This means that $\frac{q-1}{2} \mid (1 + 2j)$. But $\frac{q-1}{2} < \frac{q+1}{2} \leq 1 + 2j \leq q - 2 < q - 1$. Hence, there is no $j$ such that $\frac{q-1}{4} \leq j \leq \frac{q-3}{2}$.

2. For the second part, similar to the proof of first part we have $\frac{q-1}{2} \mid (1 + 2j)$. This is possible only when $1 + 2j = \frac{q-1}{2}$. Then we get $j = \frac{q-3}{4}$. \qed
Table 4: Some negacyclic Hermitian LCD codes obtained from Theorem 21

| $q$ | $n$ | $l$ | Negacyclic Hermitian LCD Codes |
|-----|-----|-----|-------------------------------|
| 7   | 6   | $1 \leq l \leq 2$ | $[6, 5 - 2l, d \geq 6 - 2l]_{7_2}$ |
| 11  | 10  | $2 \leq l \leq 4$ | $[10, 8 - 2l, d \geq 10 - 2l]_{7_2}$ |
| 13  | 13  | $3 \leq l \leq 5$ | $[12, 12 - 2l, d \geq 13 - 2l]_{13_2}$ |

By Lemma 19 and 20 the cardinality of the defining set $\mathbb{Z}$ is

$$\begin{cases} 
\text{if } q \equiv 1 \mod 4, \text{ then } |\mathbb{Z}| = 2 \left( \frac{q-3}{2} - l + 1 \right), & \frac{q-1}{4} \leq l \leq \frac{q-3}{2} \\
\text{if } q \equiv 3 \mod 4, \text{ then } |\mathbb{Z}| = 2 \left( \frac{q-3}{2} - l + \frac{1}{2} \right), & \frac{q-3}{4} \leq l \leq \frac{q-3}{2} 
\end{cases}$$

The following is immediate from Lemma 19 and 20.

**Theorem 21.** Let $q$ be an odd prime power and $n = q - 1$.

1. If $q \equiv 1 \mod 4$, then we have negacyclic Hermitian LCD codes over $\mathbb{F}_{q^2}$ of parameters $[q - 1, q - 1 - 2l, d \geq q - 2l]_{q^2}$, where $\frac{q-1}{4} \leq l \leq \frac{q-3}{2}$.
2. If $q \equiv 3 \mod 4$, then we have negacyclic Hermitian LCD codes over $\mathbb{F}_{q^2}$ of parameters $[q - 1, q - 2 - 2l, d \geq q - 1 - 2l]_{q^2}$, where $\frac{q-3}{4} \leq l \leq \frac{q-3}{2}$.

If we choose the smallest value of $l$, then for both cases we have the following.

**Theorem 22.** Let $q$ be an odd prime power and $n = q - 1$. Then we have negacyclic MDS Hermitian LCD codes over $\mathbb{F}_{q^2}$ of parameters $[q - 1, \frac{q-1}{2}, \frac{q+1}{2}]_{q^2}$.

**Proof.** If we pick $l$ as the smallest value in Theorem 21 then for both cases of $q$ we get the desired result.

---

4.2. Negacyclic Hermitian LCD codes of length $n = q^2 + 1$

In this subsection, we use negacyclic codes of lengths $n = q^2 + 1$ to construct Hermitian LCD codes, where $q$ is an odd prime power. The following is similar to the Lemma 4.1 from [17].

**Lemma 23.** Let $n = q^2 + 1$. Then, the $q^2$-cyclotomic cosets modulo $2n$ containing odd integers from 1 to $2n$ are $C_{1+2j} = \{1 + 2j, n - 1 - 2j\}$, $0 \leq j < \frac{n-2}{4}$, $C_{1+2j} = \{1 + 2j\}$, $j = \frac{n-2}{4}$, $C_{1+2j} = \{1 + 2j, 3n - 1 - 2j\}$, $n < j < \frac{3n-2}{4}$, and $C_{1+2j} = \{1 + 2j\}$, $j = \frac{3n-2}{4}$. 

12
Table 5: Some negacyclic MDS Hermitian LCD codes obtained from Theorem 22

| $q$ | $n$ | Negacyclic MDS Hermitian LCD Codes |
|-----|-----|-----------------------------------|
| 5   | 4   | $[4, 2, 3]_{5^2}$                |
| 7   | 6   | $[6, 3, 4]_{7^2}$                |
| 11  | 10  | $[10, 5, 6]_{11^2}$              |
| 13  | 12  | $[12, 6, 7]_{13^2}$              |

We define the defining set $\mathcal{Z}$ as $\mathcal{Z} = \mathcal{Z}_1 \cup \mathcal{Z}_2 \cup \mathcal{Z}_3 \cup \mathcal{Z}_4$, where $\mathcal{Z}_1 = \bigcup_{j=l}^{q^2-1} C_{1+2j}$, $q - 1 \leq l \leq \frac{q^2-1}{4}$, $\mathcal{Z}_2 = -q\mathcal{Z}_1$, $\mathcal{Z}_3 = C_{\frac{q^2+1}{2}}$ and $\mathcal{Z}_4 = -q\mathcal{Z}_3$. It is shown by Kai et al. in [17] that $\mathcal{Z}_1 \cap \mathcal{Z}_2 = \emptyset$. Also, if $q \equiv 1 \mod 4$, then $\mathcal{Z}_3 \cap \mathcal{Z}_4 = \emptyset$, and if $q \equiv 3 \mod 4$, then $\mathcal{Z}_3 = \mathcal{Z}_4$. Hence, the cardinality of the defining set $\mathcal{Z}$ is

$$
\begin{cases}
\text{if } q \equiv 1 \mod 4, & |\mathcal{Z}| = 4 \left(\frac{q^2-1}{4} - 2l\right) + 1, \quad q - 1 \leq l \leq \frac{q^2-1}{4} \\
\text{if } q \equiv 3 \mod 4, & |\mathcal{Z}| = 4 \left(\frac{q^2-1}{4} - 2l\right) + 2, \quad q - 1 \leq l \leq \frac{q^2-1}{4}
\end{cases}
$$

and obviously for both cases $\mathcal{Z}$ contains $2 \left(\frac{q^2-1}{4} - l + 1\right) + 1 = \frac{q^2+5}{2} - 2l$ consecutive terms. Now, we are ready to give the following result.

**Theorem 24.** Let $q$ be an odd prime power and $n = q^2 + 1$.

1. If $q \equiv 1 \mod 4$, then we have negacyclic Hermitian LCD codes over $\mathbb{F}_{q^2}$ of parameters $\left[q^2 + 1, 4l - 3, d \geq \frac{q^2+5}{2} - 2l\right]_{q^2}$.
2. If $q \equiv 3 \mod 4$, then we have negacyclic Hermitian LCD codes over $\mathbb{F}_{q^2}$ of parameters $\left[q^2 + 1, 4l - 4, d \geq \frac{q^2+5}{2} - 2l\right]_{q^2}$.
Table 6: Some negacyclic Hermitian LCD codes obtained from Theorem 24

| $q$ | $n$ | $l$  | Negacyclic Hermitian LCD Codes |
|-----|-----|------|-------------------------------|
| 3   | 10  | 2    | [10, 4, $d \geq 3$]          |
| 5   | 26  | $4 \leq l \leq 6$ | $[26, 4l - 3, d \geq 15 - 2l]$ |
| 7   | 50  | $6 \leq l \leq 12$ | $[50, 4l - 4, d \geq 27 - 2l]$ |
| 13  | 170 | $12 \leq l \leq 42$ | $[170, 4l - 3, d \geq 87 - 2l]$ |

5. Conclusion

In this paper, we studied some classes of MDS negacyclic LCD codes of length $n | \frac{q^2 - 1}{2}, n | \frac{q^2 + 1}{2}$ and a class of negacyclic LCD codes of length $n = q + 1$. We obtained some parameters of Hermitian negacyclic LCD codes over $\mathbb{F}_{q^2}$ of length $n = q^2 - 1$ and $n = q - 1$. For both Euclidean and Hermitian cases the dimension of these codes are determined and for some classes the minimum distance was settled. For the other classes, by studying $q$ and $q^2$-cyclotomic classes we give lower bounds on the minimum distance.

References

[1] N. Aydin, S. Irfan, and D. K. Ray-Chaudhuri, "The structure of 1-generator quasi-twisted codes and new linear codes," Des. Codes Cryptogr, vol. 24, no. 3, pp. 313-326, 2001.

[2] A. Krishna and D. V. Sarwate, "Pseudocyclic maximum-distance-separable codes," IEEE Trans. Inform. Theory, vol. 36, no. 4, pp. 880-884, 1990.

[3] J. L. Massey, "Linear codes with complementary duals," Discrete Math, vol. 106, pp. 337-342, 1992.

[4] J. L. Massey, "Reversible codes" Information and Control, vol. 7, no. 3, pp. 369-380, 1964.

[5] N. Sendrier, "Linear codes with complementary duals meet the Gilbert–Varshamov bound," Discrete Math, vol. 285, no. 1, pp. 345-347, 2004.

[6] X. Yang, and J. L. Massey, "The condition for a cyclic code to have a complementary dual," Discrete Math, vol. 126, no. 1-3, pp. 391-393, 1994.
[7] H. Q. Dinh, "On repeated-root constacyclic codes of length $4p^s$," Asian-Eur. J Math, vol. 6, no. 2, 1350020, 2013.

[8] B. Chen, H. Q. Dinh, and H. Liu, "Repeated-root constacyclic codes of length $2\ell^m p^n$." Finite Fields Th App, vol. 33, pp. 137-159, 2015.

[9] M. Esmaeili, and S. Yari, "On complementary-dual quasi-cyclic codes," Finite Fields Th App, vol. 15, no. 3, pp. 375-386, 2009.

[10] S. T. Dougherty, J. L. Kim, B. Ozkaya, L. Sok, and P. Solé, "The combinatorics of LCD codes: Linear Programming bound and orthogonal matrices," arXiv:1506.01955v1.

[11] C. Gumeri, B. Ozkaya and P. Solé, "Quasi-Cyclic Complementary Dual Code," Finite Fields Th App, vol. 42, pp. 67-80, 2016.

[12] S. Zhu, B. Pang and Z. Sun, "The reversible negacyclic codes over finite fields," arXiv:1610.08206.

[13] C. Carlet, and S. Guilley, "Complementary dual codes for countermeasures to side-channel attacks," In: E. R. Pinto et al. (eds), In Coding Theory and Applications, CIM Series in Mathematical Sciences, vol. 3, pp. 97-105, Springer International Publishing. 2014.

[14] H. Q. Dinh, "Constacyclic codes of length $p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$," Journal of Algebra, vol. 324, no. 5, pp. 940-950, 2010.

[15] Y. Yang and W. Cai, "On self-dual constacyclic codes over finite fields," Des. Codes Cryptogr, vol. 74, no. 2, pp. 355-364, 2015.

[16] C. Ding, C. Li, and S. Li, "LCD cyclic codes over finite fields," arXiv:1608.02170.

[17] X. Kai and S. Zhu, "New quantum MDS codes from negacyclic codes," IEEE Trans. Inform. Theory, vol. 59, no. 2, pp. 1193-1197, 2013.