Communications in Combinatorics and Optimization
Vol. xx, No. x (xxxx), pp. 1-16
https://doi.org/10.22049/cco.2026.30942.2674

CCO
Commun. Comb. Optim.

Research Article

Construction of LCD codes from tridiagonal Toeplitz matrices

Wajid M. Shaikh[1,2,†], Rupali S. Jain[1,‡], B. Surendranath Reddy[1,*], Bhagyashri S. Patil[1,3]

[1] School of Mathematical Sciences, SRTMU Nanded, India
[†] `wajidshaikh144@gmail.com`
[‡] `rupalisjain@gmail.com`
[*] `surendra.phd@gmail.com`

[2] P.E.S. College of Engineering, Chhatrapati Sambhajinagar, India

[3] MGM's College of Engineering, Nanded, India
`patilbhagyashri0506@gmail.com`

Received: 25 August 2025; Accepted: 27 June 2026

Abstract: A Toeplitz matrix T is characterized by having constant entries along diagonals parallel to the main diagonal. Double Toeplitz (DT) codes are linear codes whose generator matrix takes the form (I, T), where T is a Toeplitz matrix. In 2021, Shi et al. established the necessary and sufficient condition for a DT code to be an LCD, assuming that T is symmetric. In 2024, Cheng obtained the necessary and sufficient condition for a DT code to be an LCD when T is skew-symmetric. In this paper, we consider Toeplitz tridiagonal matrices that are neither symmetric nor skew-symmetric. We derive the necessary and sufficient condition under which a DT code is an LCD code, using the factorization of Dickson polynomials over finite fields. Furthermore, by applying concatenation techniques, we construct a family of LCD codes with arbitrary minimum distance.

Keywords: LCD code, Toeplitz matrix, Dickson polynomial.

AMS Subject Classification: 94B05, 15B05, 12E10

1. Introduction

Let $q = p^l$, where p is a prime and l is a positive integer. We denote $\mathbb{F}_q$ as the finite field with q elements and characteristic p. A q-ary linear code $\mathscr{C}$ of length n and dimension k is a k-dimensional subspace of $\mathbb{F}_q^n$. A linear code that intersects trivially with its

---

[*] *Corresponding Author*

dual is called a linear complementary dual (LCD) code. These codes were introduced by Massey [15], who also provided a characterization of LCD codes over finite fields. Furthermore, Massey demonstrated that LCD codes offer an optimal solution for the two-user binary adder channel (2-BAC). Later, Sendrier [16] showed that LCD codes are asymptotically good and applied them in the context of equivalence testing of linear codes (see [17]). In 2016, Carlet and Guilley [4] highlighted the significance of LCD codes as effective countermeasures against passive and active side-channel attacks on embedded cryptosystems. This finding significantly increased research interest in LCD codes.

Following these foundational contributions, the study of LCD codes has been extended to more general algebraic structures. In 2019, Liu and Wang [13] explored LCD codes over finite rings, while Liu and Wu [14] further investigated LCD codes over Frobenius rings. Additionally, growing interest has emerged in studying LCD codes over various alphabets [1, 8, 12]. In addition to classical LCD codes, Carlet et al. [6, 7] investigated Hermitian LCD and σ-LCD codes as generalizations based on different inner products.

Alongside these theoretical developments, various constructions of LCD codes have been proposed. DT codes [22] represent a significant generalization of both double circulant and double negacirculant codes, which have previously been constructed over diverse alphabets [10, 18, 19, 21–23].

A code is called a DT code if its generator matrix has the form (I, T), where I is an identity matrix and T is a Toeplitz matrix of the same dimension. Recall that a matrix is Toeplitz if all its diagonals parallel to the main diagonal have constant entries. Notably, both circulant and negacirculant matrices are special cases of Toeplitz matrices.

Shi et al. [20] recently constructed a class of LCD DT codes by utilizing the class of symmetric tridiagonal Toeplitz matrices. Following this, Li et al. [11] gave an improved method for constructing formally self-dual codes with small hulls using symmetric tridiagonal Toeplitz matrices. Subsequently, Cheng [9] constructed a class of LCD DT codes by using the class of skew-symmetric tridiagonal Toeplitz matrices.

Motivated by the aforementioned work, in this paper, we construct a new class of LCD double Toeplitz codes using a family of tridiagonal Toeplitz matrices that are neither symmetric nor skew-symmetric. This construction represents a generalization of the results presented in [9]. While the LCD codes constructed in [9] have a minimum distance of at most 2, the codes proposed in this paper achieve a minimum distance of up to 3. Furthermore, this distance can be increased by applying the concatenation technique described in [5].

This paper is organized as follows: In Section 2, we consider a new class of tridiagonal Toeplitz matrices that are neither symmetric nor skew-symmetric. Additionally, we derive the relationship between Dickson polynomials and the characteristic polynomial of defined matrices. Sections 3 and 4 establish the necessary and sufficient conditions for DT codes to be LCD, and also present sufficient conditions under certain mild arithmetic conditions. In Section 5, we construct LCD codes with arbitrarily large minimum distance using concatenation techniques.

2. Class of Toeplitz matrices

Throughout this paper, let p be an odd prime and $q = p^l$, where l is a positive integer. Denote, finite field with q elements by $\mathbb{F}_q$ and let $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$. For $u \in \mathbb{F}_q$, define triadiagonal Toeplitz matrix as follows

$$\mathcal{M}_n(u) = \begin{pmatrix} u & 1 & 0 & \cdots & 0 & 0 \\ -1 & u & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & u & 1 \\ 0 & 0 & 0 & \cdots & -1 & u \end{pmatrix}_{n\times n} \tag{2.1}$$

For example

$$\mathcal{M}_1(u) = \begin{pmatrix} u \end{pmatrix}_{1\times 1}, \quad \mathcal{M}_2(u) = \begin{pmatrix} u & 1 \\ -1 & u \end{pmatrix}_{2\times 2}, \mathcal{M}_3(u) = \begin{pmatrix} u & 1 & 0 \\ -1 & u & 1 \\ 0 & -1 & u \end{pmatrix}_{3\times 3}$$

Note that for $n \geq 2$ and $u \neq 0$, $\mathcal{M}_n(u)$ is neither symmetric nor skew-symmetric. The characteristic polynomial of such matrices was established by Li et al. [11]. We state the particular case relevant to $\mathcal{M}_n(u)$ as follows:

Lemma 1. *Let $P_n(x,u) = det(\mathcal{M}_n(u) - xI_n)$ be a characteristic polynomial of $\mathcal{M}_n(u)$, where I_n is the $n \times n$ identity matrix and $n \in \mathbb{N}$. Then*

$$P_1(x,u) = u - x, \quad P_2(x,u) = (u-x)^2 + 1$$

$$P_n(x,u) = (u-x)P_{n-1}(x,u) + P_{n-2}(x,u)$$

for any $n \geq 3$.

For any non-negative integer n and $a \in \mathbb{F}_q$, the n^{th} order Dickson polynomial, denoted by $E_n(x,a)$, is defined recursively.

$$E_{n+1}(x,a) = xE_n(x,a) - aE_{n-1}(x,a)$$

with $E_0(x,a) = 1$ and $E_1(x,a) = x$ as the initial conditions.
The relationship of the characteristic polynomial of $\mathcal{M}_n(u)$ with the Dickson polynomial was proved in [11, Proposition 2.2.]. We recall the specific result here for our construction.

Lemma 2. *Let $P_n(x,u)$ be the characteristic polynomial of $\mathcal{M}_n(u)$, and let $E_n(x,a)$ be the n^{th} order Dickson polynomial. If we set $P_0(x,u)=1$, then*

$$P_n(x,u) = E_n(u-x,-1)$$

where, n is a non-negative integer and $a,u \in \mathbb{F}_q$.

The reason we state the above lemma is that Bhargava and Zieve [2] provided an important result about the factoring of Dickson polynomials, which is stated below.

Lemma 3. *[2] Let $\mathbb{F}_q$ be a finite field of odd characteristic p, and let t be a positive integer such that $\gcd(t+1,q)=1$. Let $E_t(x,a)$ denote the Dickson polynomial of order t over $\mathbb{F}_q$. Then $E_t(x,a)$ can be factored into linear factors over the algebraic closure $\overline{\mathbb{F}}_q$ as follows*

$$E_t(x,a) = \prod_{j=1}^{t}\left(x - \sqrt{a}(\xi^j + \xi^{-j})\right),$$

where ξ is a primitive $2(t+1)$-th root of unity.

If we write $n+1$ in the form $p^m(t+1)$, where $\gcd(t+1,p)=1$. Using the functional equation for E_n, we find

$$E_n\left(z+\frac{a}{z},a\right) = \frac{\left(z^{t+1}-\left(\frac{a}{z}\right)^{t+1}\right)^{p^m}}{z-\frac{a}{z}} = E_t\left(z+\frac{a}{z},a\right)^{p^m}\left(z-\frac{a}{z}\right)^{p^m-1}$$

which gives

$$E_n(x,a) = (E_t(x,a))^{p^m}(x^2-4a)^{\frac{p^m-1}{2}}$$

Hence, combining Lemmas 2 and 3, we get the following result, which is a special case of [11, Theorem 2.3].

Corollary 1. *Let $\mathbb{F}_q$ be a finite field of odd characteristic p. Let n be a positive integer such that $n = p^m(t+1)-1$, where gcd$(t+1,p)=1$. Then for any $u \in \mathbb{F}_q$, the characteristic polynomial of $\mathcal{M}_n(u)$ can be factored completely over $\overline{\mathbb{F}}_q$ as follows:*

$$P_n(x,u) = \begin{cases} (u-x+2\eta)^{\frac{p^m-1}{2}}(u-x-2\eta)^{\frac{p^m-1}{2}}\prod_{j=1}^{t}(u-x-\eta(\xi^j+\xi^{-j}))^{p^m} & \text{if } t \geq 1 \\ (u-x+2\eta)^{\frac{p^m-1}{2}}(u-x-2\eta)^{\frac{p^m-1}{2}} & \text{if } t=0 \end{cases}$$

where, η is square root of -1 and ξ is a primitive $2(t+1)$-th root of unity in $\overline{\mathbb{F}}_q$.

From Corollary 1, we obtain the eigenvalues of $\mathcal{M}_n(u)$. For the construction of LCD double Toeplitz codes, we require the eigenvalues of $\mathcal{M}_n(u)\mathcal{M}_n^T(u)$, which are provided in the following theorem.

Theorem 1. *Let $n \geq 2$ and $u \in \mathbb{F}_q$. Then, $u - \lambda$ is an eigenvalue of $\mathcal{M}_n(u)$, where $\lambda \in \{\pm 2\eta\} \cup \{\eta(\xi^j + \xi^{-j}) \mid 1 \leq j \leq t\}$, if and only if $u^2 - \lambda^2$ is an eigenvalue of $\mathcal{M}_n(u)\mathcal{M}_n^T(u)$.*

Proof. Consider

$$
\begin{aligned}
&\det\Big(\mathcal{M}_n(u)\mathcal{M}_n^T(u) - (u^2 - \lambda^2)I_n\Big) = 0 \\
\Leftrightarrow \ &\det\left(\begin{pmatrix}
u^2+1 & 0 & -1 & \cdots & 0 & 0 & 0 \\
0 & u^2+2 & 0 & \cdots & 0 & 0 & 0 \\
-1 & 0 & u^2+2 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & u^2+2 & 0 & -1 \\
0 & 0 & 0 & \cdots & 0 & u^2+2 & 0 \\
0 & 0 & 0 & \cdots & -1 & 0 & u^2+1
\end{pmatrix}_{n\times n} - (u^2 - \lambda^2)I_n\right) = 0 \\
\Leftrightarrow \ &\begin{vmatrix}
\lambda^2+1 & 0 & -1 & \cdots & 0 & 0 & 0 \\
0 & \lambda^2+2 & 0 & \cdots & 0 & 0 & 0 \\
-1 & 0 & \lambda^2+2 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & \lambda^2+2 & 0 & -1 \\
0 & 0 & 0 & \cdots & 0 & \lambda^2+2 & 0 \\
0 & 0 & 0 & \cdots & -1 & 0 & \lambda^2+1
\end{vmatrix}_{n\times n} = 0 \\
\Leftrightarrow \ &\begin{vmatrix}
\lambda' & -1 & 0 & \cdots & 0 & 0 \\
1 & \lambda' & -1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & \lambda' & -1 \\
0 & 0 & 0 & \cdots & 1 & \lambda'
\end{vmatrix}_{n\times n}
\begin{vmatrix}
\lambda' & 1 & 0 & \cdots & 0 & 0 \\
-1 & \lambda' & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & \lambda' & 1 \\
0 & 0 & 0 & \cdots & -1 & \lambda'
\end{vmatrix}_{n\times n} = 0, \quad \text{where } \lambda' \in \{\pm\lambda\} \\
\Leftrightarrow \ &\det(\mathcal{M}_n^T(u) - (u - \lambda')I_{n\times n}) \cdot \det(\mathcal{M}_n(u) - (u - \lambda')I_{n\times n}) = 0.
\end{aligned}
$$

The above equation holds if and only if $(u - \lambda')$ is an eigenvalue of either $\mathcal{M}_n(u)$ or $\mathcal{M}_n^T(u)$. Hence, $u - \lambda$ is an eigenvalue of $\mathcal{M}_n(u)$ if and only if $u^2 - \lambda^2$ is an eigenvalue of $\mathcal{M}_n(u)\mathcal{M}_n^T(u)$. □

3. Construction of LCD double Toeplitz codes

In this section, we consider a family of DT codes and derive a necessary and sufficient condition for these codes to be LCD. We also provide sufficient conditions under some mild mathematical assumptions.

Definition 1. For a positive integer n, define $\mathscr{C}_n(u)$ as a linear code over the finite field $\mathbb{F}_q$ of length $2n$ and dimension n, with generator matrix $(I_n, \mathcal{M}_n(u))$, where $\mathcal{M}_n(u)$ is the matrix defined in (2.1).

Following theorem describes the necessary and sufficient condition for DT code $\mathscr{C}_n(u)$ to be an LCD.

Theorem 2. *Let $\mathbb{F}_q$ be a finite field of odd characteristic p. Let n be a positive integer such that $n = p^m(t+1) - 1$, where $\gcd(t+1, p) = 1$. For $u \in \mathbb{F}_q$, let $\mathscr{C}_n(u)$ be the linear code defined in Definition 1. Let ξ be a primitive $2(t+1)$-th root of unity and $\eta = \sqrt{-1}$ in $\overline{\mathbb{F}}_q$. Then $\mathscr{C}_n(u)$ is an LCD code if and only if $u \notin \chi_t$, where*

$$\chi_t = \begin{cases} \{-\eta\sqrt{5}, \eta\sqrt{5}\} & \text{if } t = 0 \\ \{-\eta\sqrt{5}, \eta\sqrt{5}\} \cup \{\pm\eta(3 + \xi^{2j} + \xi^{-2j})^{\frac{1}{2}} \mid 1 \le j \le t\} & \text{if } t \ge 1 \end{cases} \tag{3.1}$$

Proof. We know that a linear code $\mathscr{C}$ is an LCD if and only if GG^T is invertible, where G is generator matrix of $\mathscr{C}$. In this case we want following matrix to be invertible

$$\begin{pmatrix} I_n & \mathcal{M}_n(u) \end{pmatrix} \begin{pmatrix} I_n \\ \mathcal{M}_n^T(u) \end{pmatrix} = I_n + \mathcal{M}_n(u)\mathcal{M}_n^T(u)$$

Clearly, above matrix is invertible if and only if -1 is not an eigenvalue of $\mathcal{M}_n(u)\mathcal{M}_n^T(u)$. From Theorem 1, we know that eigenvalues of $\mathcal{M}_n(u)\mathcal{M}_n^T(u)$ is of the form $u^2 - \lambda^2$, where $\lambda \in \{\pm 2\eta\} \cup \{\eta(\xi^j + \xi^{-j}) \mid 1 \le j \le t\}$.
Hence, we require $u^2 - \lambda^2 \neq -1$. i.e. $u^2 + 4 \neq -1$ and $u^2 + (\xi^j + \xi^{-j})^2 \neq -1$, which concludes the proof. □

When $u = 0$, our results coincide with those in [9], and hence generalize them. Now, for $u \in \mathbb{F}_q^*$, we will establish sufficient conditions for the existence of LCD code $\mathscr{C}_n(u)$.

Corollary 2. *Let n be a positive integer such that $n = p^m(t+1) - 1$, where $\gcd(t+1, p) = 1$. Let $\mathbb{F}_q$ be a finite field with odd characteristic p, and let $q > 2\left(\lceil \frac{t}{2} \rceil\right) + 3$, where $\lceil \cdot \rceil$ denotes the least integer function. Then, there exists an LCD code $\mathscr{C}_n(u)$, where $u \in \mathbb{F}_q^*$.*

Proof. Consider the set $\mathcal{S} = \{\pm\eta(3 + \xi^{2j} + \xi^{-2j})^{\frac{1}{2}} \mid 1 \le j \le t\}$ in χ_t. Note that if $i + j = t + 1$, then $3 + \xi^{2j} + \xi^{-2j} = 3 + \xi^{2i} + \xi^{-2i}$, which implies $\eta(3 + \xi^{2j} + \xi^{-2j})^{\frac{1}{2}} = \pm\eta(3 + \xi^{2i} + \xi^{-2i})^{\frac{1}{2}}$. From this we get

$$|\mathcal{S}| \le \begin{cases} t, & \text{if } t \text{ is even} \\ 2\lceil \frac{t}{2} \rceil, & \text{if } t \text{ is odd} \end{cases}$$

By the condition, we have $q > 2(\lceil \frac{t}{2} \rceil) + 3$, hence $|\mathbb{F}_q| = q \ge 2(\lceil \frac{t}{2} \rceil) + 4$. This implies $|\mathbb{F}_q| \ge |\chi_t| + 2$. Hence, from Theorem 2, there exists $u \in \mathbb{F}_q^*$ such that $\mathscr{C}_n(u)$ is an LCD code. □

Corollary 3. *Let $\mathbb{F}_q$ be a finite field with odd characteristic p, and $q = p^l$. Let $\mathcal{S}_1 = \{p^m - 1 \mid m \in \mathbb{N}\}$ and $\mathcal{S}_2 = \{p^m(t+1) - 1 \mid m, t \in \mathbb{N}$ with $gcd(t+1, p) = 1\}$. Let n be a positive integer such that $n = p^m(t+1) - 1$, where $gcd(t+1, p) = 1$. For $u \in \mathbb{F}_q^*$, let $\mathscr{C}_n(u)$ be the linear code defined in Definition 1. The following statements hold.*

- *(i) If $p \equiv 11, 13, 17, 19 \pmod{20}$ and $2 \nmid l$, then for any $u \in \mathbb{F}_q^*$ and $n \in \mathcal{S}_1$, $\mathscr{C}_n(u)$ is an LCD code.*

(ii) *If* $p \equiv 1, 3, 7, 9 \pmod{20}$ *or* $p \equiv 11, 13, 17, 19 \pmod{20}$ *and* $2 \mid l$*, then for any* $u \in \mathbb{F}_q^* \setminus \{\pm\eta\sqrt{5}\}$ *and* $n \in \mathcal{S}_1$*,* $\mathscr{C}_n(u)$ *is an LCD code.*

(iii) *If* $p \equiv 11, 13, 17, 19 \pmod{20}$ *and* $2 \nmid l$*, then for any* $u \in \mathbb{F}_q^*$ *and* $n \in \mathcal{S}_2$ *such that* $(t+1) \nmid j(q^2-1)$ *for all* $1 \leq j \leq t$*,* $\mathscr{C}_n(u)$ *is an LCD code.*

(iv) *If* $p \equiv 1, 3, 7, 9 \pmod{20}$ *or* $p \equiv 11, 13, 17, 19 \pmod{20}$ *and* $2 \mid l$*, then for any* $u \in \mathbb{F}_q^* \setminus \{\pm\eta\sqrt{5}\}$ *and* $n \in \mathcal{S}_2$ *such that* $(t+1) \nmid j(q^2-1)$ *for all* $1 \leq j \leq t$*,* $\mathscr{C}_n(u)$ *is an LCD code.*

Proof. Let n be a positive integer such that $n = p^m(t+1) - 1$, where $\gcd(t+1, p) = 1$, and let χ_t be as defined in (3.1). Before proving Corollary 3, we assert that

(a) $\eta\sqrt{5} \in \mathbb{F}_q$ if and only if $p \equiv 1, 3, 7, 9 \pmod{20}$ or $p \equiv 11, 13, 17, 19 \pmod{20}$ and $2 \mid l$.

(b) If $(t+1) \nmid j(q^2-1)$, then $\xi^{2j} + \xi^{-2j} \notin \mathbb{F}_q$ for positive integer j.

Let $\left(\frac{a}{p}\right)$ denote the Legendre symbol, whose value is 1 if a is a quadratic residue modulo p and -1 if a is a quadratic non-residue modulo p. First we prove above claims

(a) We know that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$, which also means $\left(\frac{-1}{p}\right) = -1$ if and only if $p \equiv 3 \pmod 4$. Since $5 \equiv 1 \pmod 4$, we have $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. We can easily prove that $\left(\frac{p}{5}\right) = 1$ if and only if $p \equiv 1, 4 \pmod 5$, which also implies $\left(\frac{p}{5}\right) = -1$ if and only if $p \equiv 2, 3 \pmod 5$. We know that Legendre's symbols are multiplicative, which gives

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right)$$

Hence, $\left(\frac{-5}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$ and $p \equiv 1, 4 \pmod 5$ or $p \equiv 3 \pmod 4$ and $p \equiv 2, 3 \pmod 5$. From this, we get $\left(\frac{-5}{p}\right) = 1$ if and only if $p \equiv 1, 3, 7, 9 \pmod{20}$, which implies $\eta\sqrt{5} \in \mathbb{F}_p \subseteq \mathbb{F}_q$. Now for second part, observe that if $p \equiv 11, 13, 17, 19 \pmod{20}$, then exactly either $\eta \in \mathbb{F}_p$ or $\sqrt{5} \in \mathbb{F}_p$, but not both η and $\sqrt{5}$ simultaneously belongs $\mathbb{F}_p$, which implies $\eta\sqrt{5} \notin \mathbb{F}_p$. Consider the polynomial $x^2 + 5$ over $\mathbb{F}_p$, which is a minimal polynomial of $\pm\eta\sqrt{5}$. Thus, we have $\eta\sqrt{5} \in \mathbb{F}_{p^2}$, and hence $\eta\sqrt{5} \in \mathbb{F}_{p^l}$ if and only if $2 \mid l$.

(b) If $(t+1) \nmid j(q^2-1)$, then $(t+1) \nmid j(q-1)$, and hence $\xi^{2j} \notin \mathbb{F}_q$.
Now, suppose that $\gamma = (\xi^{2j} + \xi^{-2j}) \in \mathbb{F}_q$. Consider the minimal polynomial $x^2 - \gamma x + 1$ of ξ^{2j}. From this, we conclude that $\mathbb{F}_q(\xi^{2j})$ is a quadratic field extension of $\mathbb{F}_q$. Hence, we have $\mathbb{F}_q(\xi^{2j}) = \mathbb{F}_{q^2}$, which implies $(\xi^{2j})^{q^2-1} = 1$. Since ξ^2 is an $(t+1)$-th primitive root of unity, it follows that $(t+1) \mid j(q^2-1)$. This is a contradiction to our assumption. Therefore, $\gamma = \xi^{2j} + \xi^{-2j} \notin \mathbb{F}_q$.

We now proceed to prove that parts (i)–(iv) of Corollary 3 are true.

(i) If $p \equiv 11, 13, 17, 19 \pmod{20}$ and $2 \nmid l$, then from claim (a), we have $\pm\eta\sqrt{5} \notin \mathbb{F}_q$. For $n \in \mathcal{S}_1$, by Theorem 2, we have $\chi_t = \{\pm\eta\sqrt{5}\}$, which implies $\mathbb{F}_q \cap \chi_t = \emptyset$. Hence, for any $u \in \mathbb{F}_q^*$, we have that $\mathscr{C}_n(u)$ is an LCD code over $\mathbb{F}_q$.

(ii) If $p \equiv 1,3,7,9 \pmod{20}$ or $p \equiv 11,13,17,19 \pmod{20}$ and $2 \nmid l$, then from claim (a), we have $\pm\eta\sqrt{5} \in \mathbb{F}_q$. From Theorem 2, and for $n \in \mathcal{S}_1$, we have $\chi_t = \{\pm\eta\sqrt{5}\}$. Hence, part (ii) of Corollary 3 is true.

(iii) For $n \in \mathcal{S}_2$, from Theorem 2, we have $\chi_t = \{\pm\eta\sqrt{5}\} \cup \{\pm\eta(3+\xi^{2j}+\xi^{-2j})^{\frac{1}{2}} \mid 1 \leq j \leq t\}$. If $p \equiv 11,13,17,19 \pmod{20}$ and $2 \nmid l$, then from claim (a), we have $\eta\sqrt{5} \notin \mathbb{F}_q$, which gives $\pm\eta\sqrt{5} \notin \mathbb{F}_q$. Suppose that $\eta(3+\xi^{2j}+\xi^{-2j})^{\frac{1}{2}} \in \mathbb{F}_q$, then $(3+\xi^{2j}+\xi^{-2j})^{\frac{1}{2}} \in \mathbb{F}_q$, which implies $\xi^{2j}+\xi^{-2j} \in \mathbb{F}_q$. Since $(t+1) \nmid j(q^2-1)$, from claim (b), we have $\xi^{2j}+\xi^{-2j} \notin \mathbb{F}_q$, which is a contradiction. Thus, we have $\eta(3+\xi^{2j}+\xi^{-2j})^{\frac{1}{2}} \notin \mathbb{F}_q$, which also implies $\mathbb{F}_q \cap \chi_t = \emptyset$. Hence, for any $u \in \mathbb{F}_q^*$ and $n \in \mathcal{S}_2$, we have that $\mathscr{C}_n(u)$ is an LCD code over $\mathbb{F}_q$.

(iv) Note that if $p \equiv 1,3,7,9 \pmod{20}$ or $p \equiv 11,13,17,19 \pmod{20}$ and $2 \mid l$, then $\eta\sqrt{5} \in \mathbb{F}_q$. The remaining proof follows from part (iii).

□

Remark 1. Note that in Corollary 3, we did not consider the case where $p \equiv 5,15 \pmod{20}$. If $p \equiv 5,15 \pmod{20}$, then $p \equiv 0 \pmod{5}$. Hence, $\{\pm\eta\sqrt{5}\} = \{0\}$. Therefore, if $p \equiv 5,15 \pmod{20}$ and $(t+1) \nmid j(q^2-1)$, then for $n \in \mathcal{S}_1 \cup \mathcal{S}_2$ and for any $u \in \mathbb{F}_q^*$, we have that $\mathscr{C}_n(u)$ is an LCD code over $\mathbb{F}_q$.

4. Generalized Results for $\mathcal{M}_n(u,v)$

In this section, we generalize the results from Section 3. First, we define a new tridiagonal Toeplitz matrix $\mathcal{M}_n(u,v)$, which extends the matrix $\mathcal{M}_n(u)$ defined in Section 2. Following this, we introduce the linear code $\mathscr{C}_n(u,v)$ over $\mathbb{F}_q$ and provide precise characterizations for $\mathscr{C}_n(u,v)$ to be an LCD code.

For $u,v \in \mathbb{F}_q$ and $n \geq 2$, define the tridiagonal Toeplitz matrix $\mathcal{M}_n(u,v)$ as follows:

$$\mathcal{M}_n(u,v) = \begin{pmatrix} u & v & 0 & \cdots & 0 & 0 \\ -v & u & v & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & u & v \\ 0 & 0 & 0 & \cdots & -v & u \end{pmatrix}_{n\times n} \tag{4.1}$$

For example,

$$\mathcal{M}_2(u,v) = \begin{pmatrix} u & v \\ -v & u \end{pmatrix}_{2\times 2}, \mathcal{M}_3(u,v) = \begin{pmatrix} u & v & 0 \\ -v & u & v \\ 0 & -v & u \end{pmatrix}_{3\times 3}$$

Remark 2. The results in [9] become a special case of our result when $u = 0$. If $v = 0$ or $p = 2$, this case corresponds to the results in [20]. Therefore, we consider p to be an odd prime, and both u and v to be non-zero elements in $\mathbb{F}_q$.

Note that $\mathcal{M}_n(u,v) = v\mathcal{M}_n\left(\frac{u}{v}\right)$. Hence, the eigenvalues of $\mathcal{M}_n(u,v)$ are of the form $v\lambda'$, where λ' is an eigenvalue of $\mathcal{M}_n\left(\frac{u}{v}\right)$. From Corollary 1, we know that the eigenvalues of $\mathcal{M}_n\left(\frac{u}{v}\right)$ are of the form $\frac{u}{v}-\lambda$, where $\lambda \in \{-2\eta, 2\eta\} \cup \{\eta(\xi^j+\xi^{-j}) \mid 1 \leq j \leq t\}$. From these, one can observe that the eigenvalues of $\mathcal{M}_n(u,v)$ are of the form $u - v\lambda$.
This observation leads us to the following result.

Lemma 4. *Let $n \geq 2$, and $u, v \in \mathbb{F}_q^*$. Then $u - v\lambda$ is an eigenvalue of $\mathcal{M}_n(u,v)$ if and only if $u^2 - v^2\lambda^2$ is an eigenvalue of $\mathcal{M}_n(u,v)\mathcal{M}_n^T(u,v)$.*

Proof. Observe that $\mathcal{M}_n(u,v)\mathcal{M}_n^T(u,v) = v^2\mathcal{M}_n\left(\frac{u}{v}\right)\mathcal{M}_n^T\left(\frac{u}{v}\right)$. From Theorem 1, we have that $\frac{u}{v}-\lambda$ is an eigenvalue of $\mathcal{M}_n\left(\frac{u}{v}\right)$ if and only if $\left(\frac{u}{v}\right)^2-\lambda^2$ is an eigenvalue of $\mathcal{M}_n\left(\frac{u}{v}\right)\mathcal{M}_n^T\left(\frac{u}{v}\right)$. Hence, we conclude the proof. □

Definition 2. For a positive integer n, define $\mathscr{C}_n(u,v)$ as a linear code over the finite field $\mathbb{F}_q$ of length $2n$ and dimension n, with generator matrix $(I_n, \mathcal{M}_n(u,v))$, where $\mathcal{M}_n(u,v)$ is the matrix defined in (4.1).

The following result gives the necessary and sufficient condition for the linear code $\mathscr{C}_n(u,v)$ to be an LCD.

Theorem 3. *Let $\mathbb{F}_q$ be a finite field with odd characteristics p. Let n be a positive integer such that $n = p^m(t+1)-1$, where $\gcd(t+1,p)=1$. For $u,v \in \mathbb{F}_q^*$, let $\mathscr{C}_n(u,v)$ be the linear code defined in Definition 2. Let ξ be a $2(t+1)$-th primitive root of unity and $\eta = \sqrt{-1}$ in $\overline{\mathbb{F}}_q$. Then $\mathscr{C}_n(u,v)$ is an LCD if and only if $\frac{u}{v} \notin \chi_t$, where*

$$\chi_t = \begin{cases} \{\pm\eta\sqrt{\frac{1}{v^2}+4}\} & \text{if } t=0 \\ \{\pm\eta\sqrt{\frac{1}{v^2}+4}\} \cup \{\pm\eta(\frac{1}{v^2}+2+\xi^{2j}+\xi^{-2j})^{\frac{1}{2}} \mid 1 \leq j \leq t\} & \text{if } t \geq 1 \end{cases} \tag{4.2}$$

Proof. We know that $\mathscr{C}_n(u,v)$ is an LCD code if and only if -1 is not an eigenvalue of $\mathcal{M}_n(u,v)\mathcal{M}_n^T(u,v)$. Hence, form Lemma 4, we have $\mathscr{C}_n(u,v)$ is an LCD code if and only if $u^2 - v^2\lambda^2 \neq -1$, where

$$\lambda = \begin{cases} \{\pm 2\eta\} & \text{if } t=0 \\ \{\pm 2\eta\} \cup \{\pm\eta(\xi^j+\xi^{-j}) \mid 1 \leq j \leq t\} & \text{if } t \geq 1 \end{cases}$$

Hence, we conclude the proof. □

The following results provide sufficient conditions for the existence of an LCD code $\mathscr{C}_n(u,v)$ over $\mathbb{F}_q$.

Corollary 4. *Let n be a positive integer such that $n = p^m(t+1)-1$, where $\gcd(t+1,p)=1$. Let $\mathbb{F}_q$ be a finite field with odd characteristic, and let $q > 2\left(\lceil\frac{t}{2}\rceil\right)+5$, where $\lceil\cdot\rceil$ denotes the least integer function. Then, there exists an LCD code $\mathscr{C}_n(u,v)$, where $u,v \in \mathbb{F}_q^*$.*

Proof. The proof follows in a similar manner to Corollary 2. ☐

Lemma 5. *Let* $\mathbb{F}_q$ *be a finite field with* q *elements and* $\mathcal{H} = \langle g^2 \rangle$ *be a cyclic subgroup of* $\mathbb{F}_q^*$*, where* g *is a generator of* $\mathbb{F}_q^*$*. Then* $\sqrt{\frac{1}{v^2}+4} \in \mathbb{F}_q$ *if and only if* $1+4v^2 \in \{0\} \cup \mathcal{H}$*, where* $v \in \mathbb{F}_q^*$*.*

Proof. We observe that $1+4v^2=0$ if and only if $\sqrt{\frac{1}{v^2}+4}=0$.
Now, $\sqrt{\frac{1}{v^2}+4} \in \mathbb{F}_q^*$ if and only if $\sqrt{1+4v^2} \in \mathbb{F}_q^*$.
Since g is a generator of $\mathbb{F}_q^*$, we have

$$\begin{aligned} &\sqrt{1+4v^2} = g^i, \quad \text{for some } i \in \mathbb{Z} \\ &\Rightarrow 1+4v^2 = g^{2i} \\ &\Rightarrow 1+4v^2 \in \mathcal{H} \end{aligned}$$

Reversing the argument shows that the converse also holds. This completes the proof. ☐

Now, we divide the cases into $1+4v^2 \in \mathcal{H}$ and $1+4v^2 \notin \mathcal{H}$. Considering these cases, we obtain the following result, which provides sufficient conditions for the existence of an LCD code $\mathscr{C}_n(u,v)$ over $\mathbb{F}_q$.

Corollary 5. *Let* $\mathbb{F}_q$ *be a finite field with odd characteristic* p*, and* $q=p^l$*. Let* g *be a generator of the cyclic group* $\mathbb{F}_q^*$*, and for* $v \in \mathbb{F}_q^*$ *assume that* $1+4v^2 \in \mathcal{H} = \langle g^2 \rangle$*. Let* $\mathcal{S}_1 = \{p^m - 1 \mid m \in \mathbb{N}\}$ *and* $\mathcal{S}_2 = \{p^m(t+1)-1 \mid t,m \in \mathbb{N} \text{ with } gcd(t+1,p)=1\}$*. Let* n *be a positive integer such that* $n = p^m(t+1)-1$*, where* $gcd(t+1,p)=1$*. The following statements hold.*

- *(i) If* $p \equiv 3 \pmod 4$ *and* $2 \nmid l$*, then for any* $u \in \mathbb{F}_q^*$ *and* $n \in \mathcal{S}_1$*,* $\mathscr{C}_n(u,v)$ *is an LCD code.*
- *(ii) If* $p \equiv 1 \pmod 4$ *or* $p \equiv 3 \pmod 4$ *and* $2 \mid l$*, then for any* $u \in \mathbb{F}_q^* \setminus \{\pm\eta\sqrt{1+4v^2}\}$ *and* $n \in \mathcal{S}_1$*,* $\mathscr{C}_n(u,v)$ *is an LCD code.*
- *(iii) If* $p \equiv 1 \pmod 4$ *or* $p \equiv 3 \pmod 4$ *and* $2 \mid l$*, then for any* $u \in \mathbb{F}_q^* \setminus \{\pm\eta\sqrt{1+4v^2}\}$ *and* $n \in \mathcal{S}_2$ *such that* $(t+1) \nmid j(q^2-1)$ *for any* $1 \le j \le t$*,* $\mathscr{C}_n(u,v)$ *is an LCD code.*
- *(iv) If* $p \equiv 3 \pmod 4$ *and* $2 \nmid l$*, then for any* $u \in \mathbb{F}_q^*$ *and* $n \in \mathcal{S}_2$ *such that* $(t+1) \nmid j(q^2-1)$ *for any* $1 \le j \le t$*,* $\mathscr{C}_n(u,v)$ *is an LCD code.*

Proof. From Theorem 3, we know that $\mathscr{C}_n(u,v)$ is an LCD code if and only if $\frac{u}{v} \in \chi_t$ defined in (4.2). Here, $1+4v^2 \in \mathcal{H}$. From Lemma 5, we have $\sqrt{\frac{1}{v^2}+4} \in \mathbb{F}_q$. As we know that $\eta \in \mathbb{F}_q$ if and only if $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$ and $2 \mid l$. From this, we conclude that (i) and (ii) are true.
From claim (b) in Corollary 3, we have $\xi^{2j}+\xi^{-2j} \notin \mathbb{F}_q$, which implies $(\frac{1}{v^2}+2+\xi^{2j}+\xi^{-2j})^{\frac{1}{2}} \notin \mathbb{F}_q$. Hence (iii) and (iv) are true. ☐

Corollary 6. *Let* $\mathbb{F}_q$ *be a finite field with odd characteristic* p*, and* $q=p^l$*. Let* g *be a generator of the cyclic group* $\mathbb{F}_q^*$*, and for* $v \in \mathbb{F}_q^*$ *assume that* $1+4v^2 \notin \mathcal{H} = \langle g^2 \rangle$*. Let* $\mathcal{S}_1 = \{p^m - 1 \mid m \in \mathbb{N}\}$ *and* $\mathcal{S}_2 = \{p^m(t+1)-1 \mid m,t \in \mathbb{N} \text{ with } gcd(t+1,p)=1\}$*. Let*

n be a positive integer such that $n = p^m(t+1) - 1$, where $gcd(t+1, p) = 1$. The following statements hold.

(i) If $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$ and $2 \mid l$, then for any $u \in \mathbb{F}_q^*$ and $n \in \mathcal{S}_1$, $\mathscr{C}_n(u, v)$ is an LCD code.

(ii) If $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$ and $2 \mid l$, then for any $u \in \mathbb{F}_q^*$ and $n \in \mathcal{S}_2$ such that $(t+1) \nmid j(q^2-1)$ for any $1 \le j \le t$, $\mathscr{C}_n(u, v)$ is an LCD code.

Proof. The proof follows in a similar manner as in Corollary 5. □

Remark 3. Note that, $\frac{1}{v^2} + 4 = 0$ in $\mathbb{F}_q$ if and only if $v = \pm\frac{\eta}{2}$. If $v = \pm\frac{\eta}{2}$, then for $u \in \mathbb{F}_q^*$, $n \in \mathcal{S}_1 \cup \mathcal{S}_2$ and $(t+1) \nmid j(q^2-1)$, $\mathscr{C}_n(u, v)$ is an LCD code over $\mathbb{F}_q$.

From Corollaries 5 and 6 one can construct several examples of LCD codes. We can give an example which is not covered by above corollary.

Example 1. Let $q = 5$, $n = 19$, and $t = 3$. Let ω be a primitive element of $\mathbb{F}_{5^4}$. Define $\xi = \omega^{78}$ as a primitive eighth root of unity, and let η be a square root of -1. Through direct computation, we find that $\eta \in \mathbb{F}_5$. Additionally, using Magma [3], we obtain $\xi^2 + \xi^{-2} = 0$ and $\xi^4 + \xi^{-4} = 3$. Now, consider the following cases:

- For $v \in \{1, 4\}$, we have $\mathbb{F}_5 \cap \chi_t = \{0, 2, 3\}$. Consequently, for any $u \in \{1, 4\}$, the code $\mathscr{C}_{19}(u, v)$ is an LCD code.
- For $v \in \{2, 3\}$, we find that $\mathbb{F}_5 \cap \chi_t = \{1, 2, 3, 4\}$. Therefore, there does not exist any $u \in \mathbb{F}_5^*$ such that $\mathscr{C}_{19}(u, v)$ forms an LCD code.

5. Construction of LCD codes using concatenation

In classical coding theory, the method of concatenation serves as an effective technique for constructing long codes over small finite fields. This method combines codes over a large finite field (outer codes) with minimum distance d_o, along with suitable inner codes with minimum distance d_i. The outcome is linear codes over a small field, ensuring $d_o d_i$ serves as a lower bound for their minimum distance. Recently, Carlet et al. [5] improved the method of concatenation by introducing new class of codes called as isometry codes.

In this section, our aim is to construct LCD codes over the field $\mathbb{F}_q$ with a specified large minimum distance. This will be accomplished by using LCD codes over $\mathbb{F}_{q^s}$ that were constructed in previous sections, and combining them with an isometry map through concatenation.

Let's start with some definitions and results from [5]. Let p be an odd prime, $q = p^l$, and $2 \le s \le n$. The trace of $\gamma \in \mathbb{F}_{q^s}$ is defined as

$$\mathrm{Tr}(\gamma) = \sum_{i=0}^{s-1} \gamma^{q^i}.$$

Definition 3. [5, 9, 20] Let $(\theta_1, \theta_2, \ldots, \theta_s)$ be an ordered basis of $\mathbb{F}_{q^s}$ over $\mathbb{F}_q$. Then $(\theta'_1, \theta'_2, \ldots, \theta'_s)$ is called dual basis of $(\theta_1, \theta_2, \ldots, \theta_s)$, if $\mathrm{Tr}(\theta_i \theta'_j) = \delta_{ij}$ for $1 \leq i, j \leq s$, where δ_{ij} is the Kronecker symbol define as

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j \end{cases}$$

Definition 4. [5, 9, 20] For positive integers s and n with $2 \leq s \leq n$. A map $\pi : \mathbb{F}_{q^s} \to \mathbb{F}_q^n$ is called an isometry if π is an $\mathbb{F}_q$-linear map and there exists an ordered basis $(\theta_1, \theta_2, \ldots, \theta_s)$ of $\mathbb{F}_{q^s}$ over $\mathbb{F}_q$ such that $\pi(\theta_i) \cdot \pi(\theta'_j) = \delta_{ij}$, where $1 \leq i, j \leq s$. Here, $\cdot$ denotes the Euclidean inner product, and $(\theta'_1, \theta'_2, \ldots, \theta'_s)$ is the dual basis of $(\theta_1, \theta_2, \ldots, \theta_s)$.
The isometry code is defined as the image of $\mathbb{F}_{q^s}$ under π (i.e., $\pi(\mathbb{F}_{q^s})$) with respect to the basis $(\theta_1, \theta_2, \ldots, \theta_s)$.

An isometry code $\pi(\mathbb{F}_{q^s})$, defined with respect to the basis $(\theta_1, \theta_2, \ldots, \theta_s)$, can be easily verified as a subspace of $\mathbb{F}_q^n$. Consequently, it forms a linear code over $\mathbb{F}_q$ with length n and dimension s. It is well known that any $\mathbb{F}_q$-linear map $\phi : \mathbb{F}_{q^s} \to \mathbb{F}_q^n$ can be expressed as $\phi(x) = (\mathrm{Tr}(a_1 x), \mathrm{Tr}(a_2 x), \ldots, \mathrm{Tr}(a_n x))$, where $a_i \in \mathbb{F}_{q^s}$.

Definition 5. [5, 9, 20] For positive integers n and s with $2 \leq s \leq n$, let $d_{\max}(q; [n, s])$ denote the largest non-negative integer d such that there exists an isometry $\pi : \mathbb{F}_{q^s} \to \mathbb{F}_q^n$ with $\pi(\mathbb{F}_{q^s})$ has minimum distance d. If no such isometry exists, we define $d_{\max}(q; [n, s]) = 0$ by convention.

Let n and s be positive integers such that $2 \leq s \leq n$, and let $\mathbb{F}_q$ be a finite field with $d_{\max}(q; [n, s]) \geq 1$. Consider an isometry π from $\mathbb{F}_{q^s}$ to $\mathbb{F}_q^n$ with respect to a basis of $\mathbb{F}_{q^s}$ over $\mathbb{F}_q$. The image $\pi(\mathbb{F}_{q^s})$ is an $[n, s, d_{\max}(q; [n, s])]$ linear code over $\mathbb{F}_q$. Let M be a positive integer such that $2 \leq M$, and let $u, v \in \mathbb{F}_{q^s}^*$. Denote $\mathscr{C}_M(u, v)$ as the $[2M, M]$ code over $\mathbb{F}_{q^s}$ as defined in Definition 2. For any $(a_1, a_2, \ldots, a_{2M}) \in \mathbb{F}_{q^s}^{2M}$, define

$$\pi^{\otimes 2M}(a_1, a_2, \ldots, a_{2M}) = (\pi(a_1), \pi(a_2), \ldots, \pi(a_{2M})).$$

Now, with the help of above notation, we construct LCD codes with large minimum distance.

Theorem 4. *Let n and s be two positive integers such that $2 \leq s \leq n$, and let $\mathbb{F}_q$ be a finite field of odd characteristic p with $d_{max}(q; [n, s]) \geq 1$. Let M be a positive integer that $M = p^m(t + 1) - 1$, where $\gcd(t + 1, p) = 1$. For $u, v \in \mathbb{F}_q^*$, let $\mathscr{C}_M(u, v)$ be the linear code defined in Definition 2. Let χ_t be the set defined in (4.2). If $\frac{u}{v} \notin \chi_t$, then $\pi^{\otimes 2M}(\mathscr{C}_n(u, v))$ is an LCD code with parameters $[2nM, sM, D]$, where $D \geq dd_{max}(q; [n, s])$.*

Proof. Since $\frac{u}{v} \notin \chi_t$, it follows that $\mathscr{C}_M(u, v)$ is an LCD code. By [5, Theorem 3.1], we conclude that $\pi^{\otimes 2M}(\mathscr{C}_M(u, v))$ is also an LCD code with parameters $[2nM, sM, D]$, where $D \geq dd_{\max}(q; [n, s])$. ☐

Example 2. Let $q = 3$, $s = 3$, and $M = 2$. Let ω be a generator of $\mathbb{F}_{27}^*$. For $u = \omega$ and $v = 1$, we have $\frac{u}{v} = \omega \notin \{\pm\eta\sqrt{2}\}$. From Theorem 3, the code $\mathscr{C}_M(\omega, 1)$ is an LCD code with parameters $[4, 2, 3]$. For $n = 5$, it follows from [9] that $d_{\max}(3; [5, 3]) = 2$. The $\mathbb{F}_3$-linear map

$$\pi : \mathbb{F}_{27} \to \mathbb{F}_3^5$$
$$\pi(x) = (\mathrm{Tr}(\omega^2 x), \mathrm{Tr}(\omega^3 x), \mathrm{Tr}(\omega x), \mathrm{Tr}(\omega^2 x), \mathrm{Tr}(2x))$$

is an isometry such that the image code $\pi(\mathbb{F}_{27})$ attains the minimum distance $d_{\max}(3; [5, 3])$. From Theorem 4, we conclude that $\pi^{\otimes 2M}(\mathscr{C}_N(\omega, 1))$ is an LCD code with parameters $[20, 6, D]$, where $D \geq 6$.

The example with the same values of q, s, M, and n is discussed in [9]. However, in that example, the obtained minimum distance is 5, whereas in our case, we have $D \geq 6$ due to an increase in the minimum distance of $\mathscr{C}_M(\omega, 1)$.
As observed, for $n \geq 3$ and $u, v \in \mathbb{F}_q^*$, the minimum distance of the code $\mathscr{C}_n(u, v)$ defined in Definition 2 is 3. For $n = 2$, the minimum distance is 2 if and only if $u = \eta v$; otherwise, it is 3. This value is always greater than or equal to the minimum distance of $\mathcal{C}_n(u)$, which is 2, where $\mathcal{C}_n(u)$ is defined in [9]. Although the increase in distance is small, by constructing an LCD codes using the aforementioned concatenation method and $\mathscr{C}_n(u, v)$, we obtain $D \geq 3d_{\max}(q; [s, n])$. In contrast, when constructing LCD codes using the concatenation method and $\mathcal{C}_n(u)$, we obtain $D \geq 2d_{\max}(q; [s, n])$. Therefore, this approach yields a new class of LCD codes with a larger minimum distance.

6. Conclusion

In this paper, we considered class of tridiagonal Toeplitz matrices that are neither symmetric nor skew-symmetric, extending the class studied in [9]. Using the factorization of Dickson polynomials over finite fields, we derived necessary and sufficient condition under which a double Toeplitz (DT) code is an LCD code. Additionally, we established some sufficient conditions for DT codes to be LCD under certain mild arithmetic assumptions.
Furthermore, we constructed LCD codes with arbitrarily large minimum distance using concatenation techniques. Specifically, by applying the concatenation technique to the LCD codes constructed in [9], the minimum distance satisfies $D \geq 2d_{\max}(q; [s, n])$. In contrast, applying the concatenation technique to the LCD codes proposed in this paper yields a minimum distance of $D \geq 3d_{\max}(q; [s, n])$.
Up to this point, using the tridiagonal Toeplitz matrix

$$\mathcal{M}_n(u, v, w) = \begin{pmatrix} u & v & 0 & \cdots & 0 & 0 \\ w & u & v & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & u & v \\ 0 & 0 & 0 & \cdots & w & u \end{pmatrix}_{n \times n}$$

where w is either v or $-v$, several LCD codes have been constructed. Finding the relationship between the characteristic polynomial of $\mathcal{M}_n(u,v,w)$ and Dickson polynomials is not a difficult task. However, determining the eigenvalues of $\mathcal{M}_n(u,v,w)\mathcal{M}_n^T(u,v,w)$ for $w \neq v, -v$ remains a challenging problem. Therefore, an interesting direction for future research is the construction of LCD codes using values of w distinct from v and $-v$. Additionally, one can explore the construction of Hermitian and Galois LCD codes using the Toeplitz matrix $\mathcal{M}_n(u,v,w)$.

Acknowledgment

One of the authors gratefully acknowledges financial support from the Ministry of Minority Affairs, Government of India, under the Maulana Azad National Fellowship scheme.

Conflict of Interest: The authors declare no conflict of interest.

Data Availability: Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

References

[1] A. Agrawal, G.K. Verma, and R.K. Sharma, *Galois LCD codes over* $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, Bull. Aust. Math. Soc. **107** (2023), no. 2, 330–341. https://doi.org/10.1017/S0004972722001344.

[2] M. Bhargava and M.E. Zieve, *Factoring Dickson polynomials over finite fields*, Finite Fields Appl. **5** (1999), no. 2, 103–111. https://doi.org/10.1006/ffta.1998.0221.

[3] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. https://doi.org/10.1006/jsco.1996.0125.

[4] C. Carlet and S. Guilley, *Complementary dual codes for counter-measures to side-channel attacks*, Coding Theory and Applications (R. Pinto, P. Rocha Malonek, and P. Vettori, eds.), CIM Series in Mathematical Sciences, vol. 3, Springer, Cham, 2014, pp. 97–105. https://doi.org/10.1007/978-3-319-17296-5_9.

[5] C. Carlet, C. Güneri, F. Özbudak, and P. Solé, *A new concatenated type construction for LCD codes and isometry codes*, Discrete Math. **341** (2018), no. 3, 830–835. https://doi.org/10.1016/j.disc.2017.12.004.

[6] C. Carlet, S. Mesnager, C. Tang, and Y. Qi, *Euclidean and Hermitian LCD MDS codes*, Des. Codes Cryptogr. **86** (2018), 2605–2618. https://doi.org/10.1007/s10623-018-0463-8.

[7] ———, *On σ-LCD codes*, IEEE Transactions on Information Theory **65** (2019), no. 3, 1694–1704.
https://doi.org/10.1109/TIT.2018.2873130.

[8] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan, *Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$*, IEEE Transactions on Information Theory **64** (2018), no. 4, 3010–3017.
https://doi.org/10.1109/TIT.2018.2789347.

[9] K. Cheng, *On LCD codes from skew symmetric Toeplitz matrices*, Finite Fields Appl. **95** (2024), 102380.
https://doi.org/10.1016/j.ffa.2024.102380.

[10] D.T. Huang, M.J. Shi, and P. Solé, *Double circulant self-dual and LCD codes over $\mathbb{Z}_{p^2}$*, Internat. J. Found. Comput. Sci. **30** (2019), no. 3, 407–416.
https://doi.org/10.1142/S0129054119500114.

[11] S. Li, M. Shi, and J. Wang, *An improved method for constructing formally self-dual codes with small hulls*, Des. Codes Cryptogr. **91** (2023), no. 7, 2563–2583.
https://doi.org/10.1007/s10623-023-01210-y.

[12] X. Liu and H. Liu, *LCD codes over finite chain rings*, Finite Fields Appl. **34** (2015), 1–19.
https://doi.org/10.1016/j.ffa.2015.01.004.

[13] Z. Liu and J. Wang, *Linear complementary dual codes over rings*, Des. Codes Cryptogr. **87** (2019), 3077–3086.
https://doi.org/10.1007/s10623-019-00664-3.

[14] Z. Liu and X.W. Wu, *Notes on LCD codes over frobenius rings*, IEEE Communications Letters **25** (2021), no. 2, 361–364.
https://doi.org/10.1109/LCOMM.2020.3029073.

[15] J.L. Massey, *Linear codes with complementary duals*, Discrete Math. **106** (1992), 337–342.
https://doi.org/10.1016/0012-365X(92)90563-U.

[16] N. Sendrier, *On the dimension of the hull*, SIAM J. Discrete Math. **10** (1997), no. 2, 282–293.
https://doi.org/10.1137/S0895480195294027.

[17] ———, *Finding the permutation between equivalent linear codes: The support splitting algorithm*, IEEE Transactions on Information Theory **46** (2000), no. 4, 1193–1203.
https://doi.org/10.1109/18.850662.

[18] M. Shi, D. Huang, L. Sok, and P. Solé, *Double circulant LCD codes over Z_4*, Finite Fields Appl. **58** (2019), 133–144.
https://doi.org/10.1016/j.ffa.2019.04.001.

[19] ———, *Double circulant self-dual and LCD codes over Galois rings*, Adv. Math. Commun. **13** (2019), no. 1, 171–183.
https://doi.org/10.3934/amc.2019011.

[20] M. Shi, F. Özbudak, L. Xu, and P. Solé, *LCD codes from tridiagonal Toeplitz matrices*, Finite Fields Appl. **75** (2021), 101892.
https://doi.org/10.1016/j.ffa.2021.101892.

[21] M. Shi, L. Qian, and P. Solé, *On the self-dual negacirculant codes of index two and four*, Des. Codes Cryptogr. **86** (2018), no. 11, 2485–2494. https://doi.org/10.1007/s10623-017-0455-0.

[22] M. Shi, L. Xu, and P. Solé, *On isodual double Toeplitz codes*, J. Sys. Sci. Complex. **37** (2024), no. 5, 2196–2206. https://doi.org/10.1007/s11424-024-2397-8.

[23] M. Shi, H. Zhu, L. Qian, L. Sok, and P. Solé, *On self-dual and LCD double circulant and double negacirculant codes over* $\mathbb{F}_q + u\mathbb{F}_q$, Cryptogr. Commun. **12** (2020), no. 1, 53–70. https://doi.org/10.1007/s12095-019-00363-9.