LCD CODES FROM TRIDIAGONAL TOEPLITZ MATRICES

Minjia Shi, Patrick Solé, Li Xu, Ferruh Ozbudak

LCD CODES FROM TRIDIAGONAL TOEPLITZ MATRICES

MINJIA SHI & FERRUH ÖZBUDAK & PATRICK SOLÉ & LI XU

Abstract. Double Toeplitz (DT) codes are codes with a generator matrix of the form (I, T) with T a Toeplitz matrix, that is to say constant on the diagonals parallel to the main. When T is tridiagonal and symmetric we determine its spectrum explicitly by using Dickson polynomials, and deduce from there conditions for the code to be LCD. Using a special concatenation process, we construct optimal or quasi-optimal examples of binary and ternary LCD codes from DT codes over extension fields.

Keywords: LCD codes, Toeplitz matrices, Dickson polynomials
AMS(2020) Math Sc. Cl. 94B05, 15B05, 12E10

1. Introduction

Linear Complementary Dual (LCD) codes are linear codes which intersect their dual trivially. They were introduced by Massey in 1992 to solve a problem in Information Theory [11]. They were proved to be asymptotically good by Sendrier [12], who used them in relation with equivalence testing of linear codes [13]. They enjoyed a renewal of interest in 2016, with an application to side-channel attacks on embarked cryptosystems [5]. Recently LCD double circulant codes or double negacirculant codes were constructed over various alphabets [9, 14, 15, 16, 18]. A far reaching generalization of both double circulant and double negacirculant codes is that of double Toeplitz codes [17]. In the present paper, we introduce a class of double Toeplitz codes which can be effectively tested for being LCD.

A code is double Toeplitz (DT) if its generator matrix is of the form (I, T) with I an identity matrix, and T a Toeplitz matrix of the same order. Recall that a matrix is Toeplitz if it has constant entries on all diagonals parallel to the main diagonal. Thus circulant matrices and negacirculant matrices are Toeplitz.

Minjia Shi is with Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, China, e-mail: smjwcl.good@163.com.

Ferruh Özbudak is with Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey; e-mail: ozbudak@metu.edu.tr.

Patrick Solé is with I2M, Aix Marseille Univ., Centrale Marseille, CNRS, Marseille, France , e-mail: sole@enst.fr.

Li Xu is with School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, China, e-mail: xuli1451@163.com.

It is easy to check that such a code is LCD iff -1 is not an eigenvalue of TT^t. To make that condition easy to check we will make two hypotheses on T :

- $T = T^t$ implying $TT^t = T^2$;
- T is tridiagonal, in the sense that $T_{ij} = 0$ if $|i - j| > 1$.

In the next section, we show that the characteristic polynomial of a tridiagonal symmetric Toeplitz matrix satisfies a three-term recurrence that can be identified, up to an easy change of variable to that of the Dickson polynomials [10]. The roots of these polynomials can be determined explicitly [3]. Hence we obtain an exact and explicit characterization on whether a given DT code (I, T) is LCD or not, when T is tridiagonal and symmetric (see Theorems 2.9 and 2.10 below). It seems very difficult to obtain such a characterization for arbitrary Toeplitz T. Moreover this is the first paper in the literature using factorization of Dickson polynomials for the characterization of some LCD codes as far as we know.

Under some mild arithmetic conditions we can show that this spectrum does not intersect the base field, and in particular does not contain -1. Some sufficient conditions for the DT code to be LCD follow. Since the DT codes so constructed have minimum distance at most three, a rather sophisticated concatenation process, namely isometry (see Definition 3.1 below) can be used to construct an LCD code over a small field. Note that because of the fundamental result that any linear code over $\mathbb{F}_q$ with $q > 3$ is equivalent to an LCD code [6], the theory of LCD codes is focusing on the cases of $\mathbb{F}_2$ and $\mathbb{F}_3$. Using the said concatenation process optimal or quasi-optimal LCD codes over these two fields are explicitly constructed.

The material is organized as follows. The next section studies the spectrum of Toeplitz matrices. Section 3 describes a concatenation process that allow for LCD codes over small fields. Numerical examples are given there. The last section concludes the paper.

2. Toeplitz matrices

2.1. **A Spectral lemma.** Throughout this paper, let p be a prime, $q = p^s$ for a positive integer s. Let $\mathbb{F}_q$ denote the finite field of q elements. Let $\overline{\mathbb{F}}_q$ denote an agebraic closure of $\mathbb{F}_q$.

Lemma 2.1. *For $n \geq 1$ let A be an $n \times n$ matrix over $\mathbb{F}_q$. We have the following cases:*

- *char $\mathbb{F}_q$ is even: -1 is an eigenvalue of A^2 if and only if -1 is an eigenvalue of A.*
- *char $\mathbb{F}_q$ is odd: -1 is an eigenvalue of A^2 if and only if $-\mu$ or μ is an eigenvalue of A, where $\mu \in \mathbb{F}_{q^2}$ with $\mu^2 = -1$.*

Proof. If char $\mathbb{F}_q$ is even, then

$$(A + I_n)^2 = A^2 + I_n^2 = A^2 + I_n,$$

which completes the proof in this case.

If char $\mathbb{F}_q$ is odd, then

$$(A + \mu I_n)(A - \mu I_n) = A^2 - \mu^2 I_n = A^2 + I_n,$$

which completes the proof. □

2.2. **Characteristic polynomial.** For $a \in \mathbb{F}_q$ and $n \geq 3$, let $T_n(a)$ be the $n \times n$ *tridiagonal Toeplitz* matrix depending on a defined as

$$T_n(a) = \begin{bmatrix} a & 1 & 0 & \cdots & \\ 1 & a & 1 & \cdots & \\ \vdots & & & & \\ 0 & & & \cdots & 1 \quad a \end{bmatrix}.$$

Namely, for example, we have

$$T_3(a) = \begin{bmatrix} a & 1 & 0 \\ 1 & a & 1 \\ 0 & 1 & a \end{bmatrix} \text{ and } T_4(a) = \begin{bmatrix} a & 1 & 0 & 0 \\ 1 & a & 1 & 0 \\ 0 & 1 & a & 1 \\ 0 & 0 & 1 & a \end{bmatrix}.$$

We also define the cases for $n = 1, 2$ as

$$T_1(a) = \begin{bmatrix} a \end{bmatrix} \text{ and } T_2(a) = \begin{bmatrix} a & 1 \\ 1 & a \end{bmatrix}.$$

For $n \geq 1$ let

$$\phi_n(\lambda) = \det\left(T_n(a) - \lambda I_n\right).$$

Lemma 2.2. *Under notation as above, we have*

$$\phi_n(\lambda) = (a - \lambda)\phi_{n-1}(\lambda) - \phi_{n-2}(\lambda)$$

for $n \geq 2$ with $\phi_1(\lambda) = a - \lambda$ and $\phi_0(\lambda) = 1$.

Proof. For $n = 2$ we have

$$T_2(a) - \lambda I_2 = \begin{bmatrix} a - \lambda & 1 \\ 1 & a - \lambda \end{bmatrix}$$

and hence

$$\phi_2(\lambda) = \det\left(T_2(a) - \lambda I_2\right) = (a - \lambda)^2 - 1 = (a - \lambda)\phi_1(\lambda) - \phi_0(\lambda).$$

This completes the proof for $n = 2$.

For $n = 3$ we have

$$T_3(a) - \lambda I_3 = \begin{bmatrix} a-\lambda & 1 & 0 \\ 1 & a-\lambda & 1 \\ 0 & 1 & a-\lambda \end{bmatrix}.$$

Considering the expansion of $\det(T_3(a) - \lambda I_3)$ using the last row we obtain

$$\phi_3(\lambda) = (a-\lambda)\begin{vmatrix} a-\lambda & 1 \\ 1 & a-\lambda \end{vmatrix} - \begin{vmatrix} a-\lambda & 0 \\ 1 & 1 \end{vmatrix} = (a-\lambda)\phi_2(\lambda) - \phi_1(\lambda).$$

This completes the proof for $n = 3$.

For $n \geq 3$ we will show that the lemma holds for $n+1$. Note that this will complete the proof. Assume that $n \geq 3$. For the $(n+1) \times (n+1)$ tridiagonal Toeplitz matrix $T_{n+1}(a)$ depending on a we have

$$T_{n+1}(a) = \begin{bmatrix} T_{n-1}(a) & C_{n-1} & 0_{(n-1)\times 1} \\ R_{n-1} & a & 1 \\ 0_{1\times(n-1)} & 1 & a \end{bmatrix}.$$

Here $T_{n-1}(a)$ is the $(n-1) \times (n-1)$ triagonal Toeplitz matrix depending on a, $0_{1\times(n-1)}$ is the $1 \times (n-1)$ matrix whose all entries are 0 and $0_{(n-1)\times 1}$ is the $(n-1) \times 1$ matrix whose all entries are 0. Moreover, R_{n-1} is an $1 \times (n-1)$ row matrix and C_{n-1} is an $(n-1) \times 1$ column matrix.

Considering the expansion of $\det(T_{n+1}(a) - \lambda I_{n+1})$ using the last row we obtain

$$\begin{aligned} \phi_{n+1}(\lambda) &= \begin{vmatrix} T_{n-1}(a) - \lambda I_{n-1} & C_{n-1} & 0_{(n-1)\times 1} \\ R_{n-1} & a-\lambda & 1 \\ 0_{1\times(n-1)} & 1 & a-\lambda \end{vmatrix} \\ &= (a-\lambda)\begin{vmatrix} T_{n-1}(a) - \lambda I_{n-1} & C_{n-1} \\ R_{n-1} & a-\lambda \end{vmatrix} - \begin{vmatrix} T_{n-1}(a) - \lambda I_{n-1} & 0_{(n-1)\times 1} \\ R_{n-1} & 1 \end{vmatrix} \\ &= (a-\lambda)\begin{vmatrix} T_{n-1}(a) - \lambda I_{n-1} & C_{n-1} \\ R_{n-1} & a-\lambda \end{vmatrix} - \phi_{n-1}(a). \end{aligned}$$

In the last equality we use the expansion of $\begin{vmatrix} T_{n-1}(a) - \lambda I_{n-1} & 0_{(n-1)\times 1} \\ R_{n-1} & 1 \end{vmatrix}$ using the last column. Note that

$$\begin{bmatrix} T_{n-1}(a) - \lambda I_{n-1} & C_{n-1} \\ R_{n-1} & a-\lambda \end{bmatrix} = T_n(a) - \lambda I_n.$$

Hence we conclude that

$$\phi_{n+1}(\lambda) = (a-\lambda)\phi_n(\lambda) - \phi_{n-1}(\lambda)$$

for $n \geq 3$, which completes the proof. □

For $n \geq 0$, $a \in \mathbb{F}_q$ and $x \in \overline{\mathbb{F}}_q$, let ψ_n be the function on $\overline{\mathbb{F}}_q$ defined as

$$\begin{array}{rccc} \psi_n : \overline{\mathbb{F}}_q & \to & \overline{\mathbb{F}}_q \\ x & \mapsto & \phi_n(a-x). \end{array}$$

Lemma 2.3. *Under notation as above we have*

$$\psi_n(x) = x\psi_{n-1}(x) - \psi_{n-2}(x)$$

for $n \geq 2$ with $\psi_1(x) = x$ and $\psi_0(x) = 1$.

Proof. For $n = 1$ and $n = 0$ we have

$$\psi_1(x) = \phi_1(a-x) = a - (a-x) = x, \text{ and } \psi_0(x) = \phi_0(a-x) = 1.$$

For $n \geq 2$ we have

$$\begin{array}{rcl} \psi_n(x) & = & \phi_n(a-x) \\ & = & (a-(a-x))\,\phi_{n-1}(a-x) - \phi_{n-2}(a-x), \text{ using Lemma 2.2,} \\ & = & x\phi_{n-1}(a-x) - \phi_{n-2}(a-x) \\ & = & x\psi_{n-1}(x) - \psi_{n-2}(x), \text{ by definitions of } \psi_{n-1}(x) \text{ and } \psi_{n-2}(x). \end{array}$$

This completes the proof. □

Recall that (see, for example, [10]) for $\alpha \in \mathbb{F}_q$ and $n \geq 0$, the Dickson polynomial of the second kind

$$E_n(x, \alpha) \in \mathbb{F}_q[x]$$

is defined recursively

$$E_n(x, \alpha) = xE_{n-1}(x, \alpha) - \alpha E_{n-2}(x, \alpha)$$

with the initial conditions $E_1(x, \alpha) = x$ and $E_0(x) = 1$.

We put $\alpha = 1$ and denote $E_n(x) = E_n(x, 1)$ throughout the paper. We obtain that $E_n(x) \in \mathbb{F}_q[x]$ is the polynomial defined resursively

$$E_n(x) = xE_{n-1}(x) - E_{n-2}(x) \tag{1}$$

with the initial conditions $E_1(x) = x$ and $E_0(x) = 1$.

Combining Lemma 2.2, Lemma 2.3 and (1) we prove the following proposition immediately.

Proposition 2.1. *Under notation as above we have*

$$\det\left(T_n(a) - xI_n\right) = \phi_n(x) = E_n(a-x),$$

for all $n \geq 1$ and $x \in \overline{\mathbb{F}}_q$.

We recall the following result due to Bhargava and Zieve [3, Theorem 4].

Theorem 2.1. *Let $n \geq 1$ be an integer. Assume that* $\gcd(n+1, q) = 1$. *We have the following cases*

- char $\mathbb{F}_q$ *is odd:*

$$E_n(x) = \prod_{i=1}^{n} \left(x - \left(\theta^i + \theta^{-i}\right)\right),$$

  where θ is a primitive $2(n+1)$-th root of 1.
- char $\mathbb{F}_q$ *is even: then n is even and*

$$E_n(x) = \prod_{i=1}^{n/2} \left(x - \left(\theta^i + \theta^{-i}\right)\right)^2,$$

  where θ is a primitive $(n+1)$-th root of 1.

Definition 2.2. For $a \in \mathbb{F}_q$ and an integer $n \geq 1$, let $C_n(a)$ be the $\mathbb{F}_q$-linear code of length $2n$ and dimension n whose generator polynomial is the $n \times 2n$ matrix given by

$$[I_n \mid T_n(a)].$$

2.3. **LCD double Toeplitz codes.** Now we present our first characterization result on whether $C_n(a)$ is LCD or not.

Theorem 2.3. *For $a \in \mathbb{F}_q$ and an integer $n \geq 1$, consider the $[2n, n]_q$ code $C_n(a)$ given in Definition 2.2. Assume that* $\gcd(n+1, q) = 1$ *and* char $\mathbb{F}_q$ *is even. Then n is even and $C_n(a)$ is LCD if and only if*

$$a \notin \left\{-1 + \theta^i + \theta^{-i} : 1 \leq i \leq \frac{n}{2}\right\},$$

where θ is a primitive $(n+1)$-th root of 1.

Proof. It is well known that $C_n(a)$ is LCD (see, for example, [11]) if and only if GG^T is invertible, where $G = [I_n \mid T_n(a)]$. Note that

$$GG^T = [I_n \mid T_n(a)] \begin{bmatrix} I_n \\ T_n(a) \end{bmatrix} = I_n + T_n(a)^2,$$

where we use the fact that $T_n(a)$ is symmetric. Hence $C_n(a)$ is LCD iff -1 is not an eigenvalue of $T_n^2(a)$. Using Lemma 2.1 we conclude that $C_n(a)$ is LCD iff -1 is not an eigenvalue of $T_n(a)$. It follows from the definition of $\phi_n(x)$ that -1 is an eigenvalue of $T_n(a)$ iff $\phi_n(-1) = 0$. Using Proposition 2.1 we have that $\phi_n(-1) = E_n(a+1)$. Finally using Theorem 2.1 we complete the proof. □

In odd characteristic we have the following result.

Theorem 2.4. *For $a \in \mathbb{F}_q$ and an integer $n \geq 1$, consider the $[2n, n]_q$ code $C_n(a)$ given in Definition 2.2. Assume that* $\gcd(n+1, q) = 1$ *and* char $\mathbb{F}_q$ *is odd. Then $C_n(a)$ is LCD if and only if*

$$a \notin \left\{-\mu + \theta^i + \theta^{-i} : 1 \leq i \leq n\right\} \cup \left\{\mu + \theta^i + \theta^{-i} : 1 \leq i \leq n\right\},$$

where $\mu^2 = -1$ and θ is a primitive $2(n+1)$-th root of 1.

Proof. The proof is similar to that of Theorem 2.3. We only indicate the different steps in this proof. Note that -1 is an eigenvalue of $T_n^2(a)$ iff $-\mu$ or μ is an eigenvalue of $T_n(a)$ by Lemma 2.1. Hence $C_n(a)$ is not LCD iff $E_n(a+\mu) = 0$ or $E_n(a-\mu) = 0$. We complete the proof using the similar steps as in the proof of Theorem 2.3. □

The following corollaries are immediate.

Corollary 2.1. *Assume that* $\gcd(n+1, q) = 1$ *and* char $\mathbb{F}_q$ *is even. If $q > \frac{n}{2}$, then there exists $a \in \mathbb{F}_q$ such that $C_n(a)$ is LCD.*

Proof. Let $S = \{-1 + \theta^i + \theta^{-i} : 1 \leq i \leq n/2\}$, where θ is a primitive $(n+1)$-th roof of 1. Note that $|S| \leq n/2$ and hence $|S \cap \mathbb{F}_q| \leq n/2$. As $q > n/2$, there exists $a \in \mathbb{F}_q \setminus S$. Using such a and Theorem 2.3 we complete the proof. □

Corollary 2.2. *Assume that* $\gcd(n+1, q) = 1$ *and* char $\mathbb{F}_q$ *is odd. If $q > 2n$, then there exists $a \in \mathbb{F}_q$ such that $C_n(a)$ is LCD.*

Proof. Let $S = \{-\mu + \theta^i + \theta^{-i} : 1 \leq i \leq n\} \cup \{\mu + \theta^i + \theta^{-i} : 1 \leq i \leq n\}$, where $\mu^2 = -1$ and θ is a primitive $2(n+1)$-th root of 1. Note that $|S| \leq 2n$ and hence $|S \cap \mathbb{F}_q| \leq 2n$. As $q > 2n$, there exists $a \in \mathbb{F}_q \setminus S$. Using such a and Theorem 2.4 we complete the proof. □

Corollary 2.1 and Corollary 2.2 give that there exist $a \in \mathbb{F}_q$ so that $C_n(a)$ is LCD for infinitely many $C_n(a)$, namely if q is large compared to n. The corresponding conditions are not necessary for the existence. Under arithmetic conditions, the following two corollaries give simple existence results for even and odd characteristics.

Corollary 2.3. *Assume that q is even and* $\gcd(n+1, q(q^2-1)) = 1$. *We have that $C_n(a)$ is LCD for all $a \in \mathbb{F}_q$.*

Proof. Note that $\gcd(n+1, q) = 1$ and $\gcd(n+1, q^2-1) = 1$. Let θ be a primitive $(n+1)$-th root of 1. Let $1 \leq i \leq n/2$ be an arbitrary integer. Put $t = \theta^i$. We have $1 + t + 1/t \in \mathbb{F}_q$ iff $(1+t+1/t)^q = 1+t+1/t$ iff $u^q = u$ with $u = t + 1/t$. Thus u is in $\mathbb{F}_q$ and t is in $\mathbb{F}_{q^2}$. Since $t^{n+1} = 1$, with $t \neq 1$, this is impossible for $\gcd(n+1, q^2-1) = 1$. The result follows by Theorem 2.3. □

The analog of Corollary 2.3 for the odd characteristic is slightly more complicated.

Corollary 2.4. *Assume that q is odd. Moreover, we assume the following:*

- *If* $q \equiv 1 \mod 4$, *then* $\gcd(n+1, q(q^2-1)/2) = 1$.
- *If* $q \equiv 3 \mod 4$, *then* $\gcd(n+1, q) = 1$ *and* $\gcd(n+1, (q^4-1)/2)$ *divides* $(q-1)/2$.

Let $\mu \in \mathbb{F}_{q^2}$ *such that* $\mu^2 = -1$. *We have the following:*

- *If* $q \equiv 1 \mod 4$, *then* $C_n(a)$ *is LCD for all* $a \in \mathbb{F}_q \setminus \{\mu+2, -\mu+2, \mu-2, -\mu-2\}$.
- *If* $q \equiv 3 \mod 4$, *then* $C_n(a)$ *is LCD for all* $a \in \mathbb{F}_q$.

Proof. Note that $\gcd(n+1, q) = 1$. Let θ be a primitive $2(n+1)$-th root of 1. Let $1 \le i \le n$ be an arbitrary integer. Put $t = \theta^i$. Also put $w = \pm\mu + t + 1/t$. Assume that $w \in \mathbb{F}_q$. Next we consider the cases separately:

- $q \equiv 1 \mod 4$: Here $\mu \in \mathbb{F}_q$ and hence $t + 1/t \in \mathbb{F}_q$. This implies that $t \in \mathbb{F}_{q^2}$ and $t^{q^2-1} = 1$. As $\gcd(q^2-1, 2(n+1)) = 2$ by assumption, we obtain that $t \in \{-1, 1\}$. Hence we have $\{\mu+t+1/t, -\mu+t+1/t\} = \{\mu+2, \mu-2, -\mu+2, -\mu-2\}$. We complete the proof using Theorem 2.4.
- $q \equiv 3 \mod 4$: Here $\mu \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and hence $t + 1/t \in \mathbb{F}_{q^2}$. This implies that $t \in \mathbb{F}_{q^4}$ and $t^{q^4-1} = 1$. As $\gcd(q^4-1, 2(n+1))$ divides $q-1$ by assumption, we obtain that $t \in \mathbb{F}_q$. Hence we have $\pm\mu + t + 1/t \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. We complete the proof using Theorem 2.4.

This completes the proof. □

We also give simple examples that are not covered by these corollaries.

Example 2.1. *Let* $q = 3$ *and* $n = 3$ *so that the condition* $q > 2n$ *of Corollary 2.2 does not hold. Also the conditions of Corollary 2.4 do not hold. Let* θ *be a primitive* $2(n+1) = 8$*-th root of* 1. *Let* $\mu = \theta^2$ *so that* $\mu^2 = -1$. *Let* $S = \{-\mu + \theta^i + \theta^{-i} : 1 \le i \le n\} \cup \{\mu + \theta^i + \theta^{-i} : 1 \le i \le n\}$. *Using Magma* [4] *we obtain that* $S = \{0, \theta^2, \theta^6\}$. *By Theorem 2.4 we conclude that* $C_n(a)$ *is LCD for* $a \in \mathbb{F}_q$ *iff* $a \in \{1, 2\}$.

Example 2.2. *Let* $q = 3$ *and* $n = 4$ *so that the condition* $q > 2n$ *of Corollary 2.2 does not hold. Also the conditions of Corollary 2.4 do not hold. Let* θ *be a primitive* $2(n+1) = 10$*-th root of* 1. *Let* $\mu = \theta^5$ *so that* $\mu^2 = -1$. *Let* $S = \{-\mu + \theta^i + \theta^{-i} : 1 \le i \le n\} \cup \{\mu + \theta^i + \theta^{-i} : 1 \le i \le n\}$. *Let* w *be a primitive element of* $\mathbb{F}_{3^4}$ *such that* $w^4 + 2w^3 + 2 = 0$. *Using Magma* [4] *we obtain that* $S = \{w^{10}, w^{20}, w^{30}, w^{50}, w^{60}, w^{70}\}$. *Note that* $\mathbb{F}_q = \{0, w^{40}, w^{80}\}$. *By Theorem 2.4 we conclude that* $C_n(a)$ *is LCD for any* $a \in \mathbb{F}_q$.

2.4. **Extension of the results for $T(a,b)$.** For $a,b \in \mathbb{F}_q$ and $n \geq 3$, let $\hat{T}_n(a,b)$ be the $n \times n$ *triagonal Topelitz* matrix depending on a and b defined as

$$\hat{T}_n(a,b) = \begin{bmatrix} a & b & 0 & \cdots & \\ b & a & b & \cdots & \\ \vdots & & & & \\ 0 & & \cdots & b & a \end{bmatrix}.$$

Namely, for example, we have

$$\hat{T}_3(a,b) = \begin{bmatrix} a & b & 0 \\ b & a & b \\ 0 & b & a \end{bmatrix} \text{ and } \hat{T}_4(a,b) = \begin{bmatrix} a & b & 0 & 0 \\ b & a & b & 0 \\ 0 & b & a & b \\ 0 & 0 & b & a \end{bmatrix}.$$

We also define the cases for $n = 2$ as

$$\hat{T}_2(a,b) = \begin{bmatrix} a & b \\ b & a \end{bmatrix}.$$

It is easy to observe that if $b \neq 0$, then

$$\frac{1}{b}\hat{T}_n(a,b) = T_n(a/b), \tag{2}$$

for $n \geq 2$ and $a \in \mathbb{F}_q$. This observation leads to the following.

Lemma 2.4. *For $n \geq 2$, $a,b \in \mathbb{F}_q$ and $b \neq 0$ we have that λ is an eigenvalue of $\hat{T}_n(a,b)$ if and only if λ/b is an eigenvalue of $T_n(a/b)$.*

Proof. For $\lambda \in \overline{\mathbb{F}}_q$ we have that

$$\begin{aligned} \det\left(\hat{T}_n(a,b) - \lambda I_n\right) = 0 &\iff \det\left(\tfrac{1}{b}\left(\hat{T}_n(a,b) - \lambda I_n\right)\right) = 0 \\ &\iff \det\left(T_n(a/b) - \lambda/b I_n\right) = 0, \end{aligned}$$

where we use (2). This completes the proof. □

Combining Theorem 2.3 and Lemma 2.4 we immediately obtain the following generalization.

Definition 2.5. For $a,b \in \mathbb{F}_q$ and an integer $n \geq 2$, let $\hat{C}_n(a,b)$ be the $\mathbb{F}_q$-linear code of length $2n$ and dimension n whose generator polynomial is the $n \times 2n$ matrix given by

$$\left[I_n \mid \hat{T}_n(a,b)\right].$$

Theorem 2.6. *For $a, b \in \mathbb{F}_q$ with $b \neq 0$ and an integer $n \geq 2$, consider the $[2n, n]_q$ code $\hat{C}_n(a, b)$ given in Definition 2.5. Assume that* $\gcd(n+1, q) = 1$ *and* $\mathrm{char}\ \mathbb{F}_q$ *is even. Then n is even and $\hat{C}_n(a, b)$ is LCD if and only if*

$$a/b \notin \left\{-1/b + \theta^i + \theta^{-i} : 1 \leq i \leq \frac{n}{2}\right\},$$

where θ is a primitive $(n+1)$-th root of 1.

Proof. Note that -1 is an eigenvalue of $\hat{T}_n(a, b)$ iff $-1/b$ is an eigenvalue of $T_n(a/b)$ by Lemma 2.4. This holds iff $E_n((a+1)/b) = 0$ by Proposition 2.1. We complete the proof using Theorem 2.1 as in the proof of Theorem 2.3. □

Theorem 2.7. *For $a, b \in \mathbb{F}_q$ with $b \neq 0$ and an integer $n \geq 2$, consider the $[2n, n]_q$ code $\hat{C}_n(a, b)$ given in Definition 2.5. Assume that* $\gcd(n+1, q) = 1$ *and* $\mathrm{char}\ \mathbb{F}_q$ *is odd. Then $\hat{C}_n(a, b)$ is LCD if and only if*

$$a/b \notin \left\{-\mu/b + \theta^i + \theta^{-i} : 1 \leq i \leq n\right\} \cup \left\{\mu/b + \theta^i + \theta^{-i} : 1 \leq i \leq n\right\},$$

where $\mu^2 = -1$ and θ is a primitive $2(n+1)$-th root of 1.

Proof. The proof is similar to those of Theorem 2.6 and Theorem 2.4. Note that $-\mu$ or μ is an eigenvalue of $\hat{T}_n(a, b)$ iff $-\mu/b$ or μ/b is an eigenvalue of $T_n(a/b)$ by Lemma 2.4. This holds iff $E_n((a+\mu)/b) = 0$ or $E_n((a-\mu)/b) = 0$ by Proposition 2.1. We complete the proof using Theorem 2.1 as in the proof of Theorem 2.4. □

2.5. **Extension of the results for** $\gcd(n+1, q) \neq 1$**.** First we introduce further notation: For positive integers a, b and a nonnegative integer u, $b^u \mid\mid a$ denotes that $b^u \mid a$ and $b^{u+1} \nmid a$. In the following theorem we recall the result in [3, Theorem 4] for the arbitrary case including $\gcd(n+1, q) \neq 1$.

Theorem 2.8. *Let $n \geq 1$ be an integer. For the characteristic p of $\mathbb{F}_q$, let r be the nonnegative integer such that $p^r \mid\mid (n+1)$. Let m be the nonnegative integer such that $n + 1 = p^r(m+1)$. We have the following:*

- *p is odd:*

$$E_n(x) = E_m(x)^{p^r}(x-2)^{(p^r-1)/2}(x+2)^{(p^r+1)/2} \text{ and } E_m(x) = \prod_{i=1}^{m}\left(x - \left(\theta^i + \theta^{-i}\right)\right),$$

  where θ is a primitive $2(m+1)$-th root of 1.

- *$p = 2$: then m is even and*

$$E_n(x) = E_m(x)^{2^r} x^{2^r-1} \text{ and } E_m(x) = \prod_{i=1}^{m/2}\left(x - \left(\theta^i + \theta^{-i}\right)\right)^2,$$

  where θ is a primitive $(m+1)$-th root of 1.

We extend Theorem 2.6 (and hence Theorem 2.3) for $\gcd(n+1, q) \neq 1$.

Theorem 2.9. *For $a, b \in \mathbb{F}_q$ with $b \neq 0$ and an integer $n \geq 2$, consider the $[2n, n]_q$ code $\hat{C}_n(a, b)$ given in Definition 2.5. Assume that* char $\mathbb{F}_q$ *is even. Let r be the nonnegative integer such that $2^r \mid\mid (n+1)$. Let m be the nonnegative integer such that $n + 1 = 2^r(m + 1)$. Assume that $r \geq 1$ (see Theorem 2.6 for the remaining case that $r = 0$). We have that m is even. If $m > 0$, then $\hat{C}_n(a, b)$ is LCD if and only if*

$$a/b \notin \{-1/b\} \cup \left\{-1/b + \theta^i + \theta^{-i} : 1 \leq i \leq \frac{m}{2}\right\},$$

where θ is a primitive $(m+1)$-th root of 1. If $m = 0$, then $\hat{C}_n(a, b)$ is LCD if and only if $a \neq 1$.

Proof. The proof is similar to that of Theorem 2.6. The main difference is that we use Theorem 2.8 instead of Theorem 2.1. □

Now we extend Theorem 2.7 (and hence Theorem 2.4) for $\gcd(n + 1, q) \neq 1$.

Theorem 2.10. *For $a, b \in \mathbb{F}_q$ with $b \neq 0$ and an integer $n \geq 2$, consider the $[2n, n]_q$ code $\hat{C}_n(a, b)$ given in Definition 2.5. Assume that* char $\mathbb{F}_q$ *is odd, which is p. Let r be the nonnegative integer such that $p^r \mid\mid (n + 1)$. Let m be the nonnegative integer such that $n + 1 = p^r(m + 1)$. Assume that $r \geq 1$ (see Theorem 2.7 for the remaining case that $r = 0$). If $m > 0$, then $\hat{C}_n(a, b)$ is LCD if and only if*

$$a/b \notin \begin{array}{l} \{-\mu/b + 2, -\mu/b - 2, \mu/b + 2, \mu/b - 2\} \cup \{-\mu/b + \theta^i + \theta^{-i} : 1 \leq i \leq m\} \\ \cup \{\mu/b + \theta^i + \theta^{-i} : 1 \leq i \leq m\}, \end{array}$$

where $\mu^2 = -1$ and θ is a primitive $2(m + 1)$-th root of 1. If $m = 0$, then $\hat{C}_n(a, b)$ is LCD if and only if $a/b \notin \{-\mu/b + 2, -\mu/b - 2, \mu/b + 2, \mu/b - 2\}$.

Proof. The proof is similar to that of Theorem 2.7. The main difference is that we use Theorem 2.8 instead of Theorem 2.1. □

Next we extend Corollaries 2.1, 2.2, 2.3 and 2.4.

Corollary 2.5. *Let $b \in \mathbb{F}_q$ with $b \neq 0$ and $n \geq 2$ an integer. Assume that* char $\mathbb{F}_q$ *is even. Let r be the nonnegative integer such that $2^r \mid\mid (n+1)$. Let m be the nonnegative integer such that $n + 1 = 2^r(m + 1)$. Assume that $r \geq 1$ (see Corollary 2.1 for the remaining case that $r = 0$). If $q > m/2 + 1$, then there exists $a \in \mathbb{F}_q$ such that $\hat{C}_n(a, b)$ is LCD.*

Proof. The proof is similar to that of Corollary 2.1. We have $q > m/2 + 1$ instead of $q > m/2$ in the hypothesis as $x = 0$ is a root of $E_n(x)$ for $r \geq 1$. □

Corollary 2.6. *Let $b \in \mathbb{F}_q$ with $b \neq 0$ and $n \geq 2$ an integer. Assume that* char $\mathbb{F}_q$ *is odd. Let r be the nonnegative integer such that $2^r \mid\mid (n + 1)$. Let m be the nonnegative integer such that $n + 1 = 2^r(m + 1)$. Assume that $r \geq 1$ (see Corollary 2.2 for the*

remaining case that $r = 0$). If $q > 2m + 4$, then there exists $a \in \mathbb{F}_q$ such that $\hat{C}_n(a, b)$ is LCD.

Proof. The proof is similar to that of Corollary 2.2. We have $q > 2m + 4$ instead of $q > 2m$ in the hypothesis as $x = 2$ and $x = -2$ are roots of $E_n(x)$ for $r \geq 1$. □

Corollary 2.7. *Let $b \in \mathbb{F}_q$ with $b \neq 0$ and $n \geq 2$ an integer. Assume that* char $\mathbb{F}_q$ *is even. Let r be the nonnegative integer such that $2^r \mid\mid (n+1)$. Let m be the nonnegative integer such that $n + 1 = 2^r(m + 1)$. Assume that $r \geq 1$ (see Corollary 2.3 for the remaining case that $r = 0$). Furthermore, assume that $\gcd(m + 1, q^2 - 1) = 1$. We have that $\hat{C}_n(a, b)$ is LCD for all $a \in \mathbb{F}_q \setminus \{1\}$.*

Proof. The proof is similar to that of Corollary 2.3. We have $\hat{C}_n(a, b)$ is LCD for all $a \in \mathbb{F}_q \setminus \{1\}$ instead of for all $a \in \mathbb{F}_q$ in the conclusion as $\hat{C}_n(1, b)$ is not LCD by Theorem 2.9 when $r \geq 1$. □

In the following corollary there are no differences in the conclusion for the cases $q \equiv 1 \mod 4$ and $q \equiv 3 \mod 4$, which is not the situation in Corollary 2.4.

Corollary 2.8. *Let $b \in \mathbb{F}_q$ with $b \neq 0$ and $n \geq 2$ an integer. Assume that* char $\mathbb{F}_q$ *is odd, which is p. Let r be the nonnegative integer such that $p^r \mid\mid (n + 1)$. Let m be the nonnegative integer such that $n+1 = p^r(m+1)$. Assume that $r \geq 1$ (see Corollary 2.4 for the remaining case that $r = 0$). Furthermore, assume that*

- *If $q \equiv 1 \mod 4$, then $\gcd(m + 1, (q^2 - 1)/2) = 1$.*
- *If $q \equiv 3 \mod 4$, then $\gcd(m + 1, (q^4 - 1)/2)$ divides $(q - 1)/2$.*

Let $\mu \in \mathbb{F}_{q^2}$ such that $\mu^2 = -1$. We have that $\hat{C}_n(a, b)$ is LCD for all $a \in \mathbb{F}_q \setminus \{\mu + 2b, \mu - 2b, -\mu + 2b, \mu - 2b\}$.

Proof. The proof is similar to the proof of Corollary 2.4. We have $\hat{C}_n(a, b)$ is not LCD for $a \in \{\mu + 2b, \mu - 2b, -\mu + 2b, \mu - 2b\}$ as $\hat{C}_n(a, b)$ is not LCD if $a/b \in \{\mu/b + 2, \mu/b - 2, -\mu/b + 2, -\mu/b - 2\}$ by Theorem 2.10 when $r \geq 1$. □

3. Concatenation

In this section we construct LCD codes over $\mathbb{F}_q$ with prescribed large minimum distance using DT that we characterize in Theorems 2.9 and 2.10 over an extension field $\mathbb{F}_{q^s}$ and a kind of concatenation. It is not difficult to observe that most of the concatenation maps do not work as they would not respect LCD property over the base and the extension fields. Hence we use an isometry map, which is introduced in [7] as a special concatenation respecting LCD property. The minimum distance of the DT codes in Theorems 2.9 and 2.10 have minimum distance at most 3. However, the

minimum distance of the isometry code can be arbitrarily large, provided the length of the isometry code is increased if necessary.

First we recall some results and notations from [7].

Definition 3.1. Let $n \geq s \geq 2$ be integers. An $\mathbb{F}_q$-linear map $\pi : \mathbb{F}_{q^s} \to \mathbb{F}_q^n$ is called an *isometry* if there exists a basis $(e_1, \ldots, e_s)$ of $\mathbb{F}_{q^s}$ over $\mathbb{F}_q$ such that

$$\pi(e_i) \cdot \pi(e'_j) = \delta_{i,j}$$

for all $1 \leq i, j \leq s$. Here $\cdot$ is the Euclidean inner product on $\mathbb{F}_q^n$, $(e'_1, \ldots, e'_s)$ is the dual basis of $(e_1, \ldots, e_s)$, and $\delta_{i,j}$ is the Kronecker delta.

The image $\pi(\mathbb{F}_{q^s})$ is an $[n, s]_q$ code, which we call an isometry code. Let $d_{\max-\text{isometry}}(q; [n, s])$ be the largest nonnegative integer d such that there exists an isometry $\pi : \mathbb{F}_{q^s} \to \mathbb{F}_q^n$ and $\pi(\mathbb{F}_{q^s})$ has minimum distance d.

Note that $d_{\max-\text{isometry}}(q; [n, s])$ coincides with the largest maximum distance of $[n, s]_q$ codes for many parameters. For example $d_{\max-\text{isometry}}(2; [4, 2]) = 2$, $d_{\max-\text{isometry}}(2; [5, 3]) = 2$ and $d_{\max-\text{isometry}}(3; [5, 2]) = 3$ (see [7]).

Let $s \geq 2$ be an integer. Let $n \geq s$ be an integer such that $d_{\max-\text{isometry}}(q, [n, s]) \geq 1$. Let $\pi : \mathbb{F}_{q^s} \to \mathbb{F}_q^n$ be an isometry such that $\pi(\mathbb{F}_{q^s})$ is an $[n, s, d]_q$ code, where $d = d_{\max-\text{isometry}}(q, [n, s])$.

For $a, b \in \mathbb{F}_{q^s}$ with $b \neq 0$ and an integer $N \geq 2$, let $\hat{C}_N(a, b)$ be the $[2N, N]_{q^s}$ code given in Definition 2.5.

Let $\pi^{\otimes 2N} : \mathbb{F}_{q^s}^{2N} \to \mathbb{F}_q^{2Nn}$ be the $\mathbb{F}_q$-linear map given by

$$\pi^{\otimes 2N}(c_1, \ldots, c_{2N}) = (\pi(c_1), \ldots, \pi(c_{2N})) .$$

We use these notations in the following two theorems.

Now we are ready to construct LCD codes of arbitrary minimum distance using tridiagonal Toeplitz matrices over extension fields and isometry. First we present the even characteristic case.

Theorem 3.2. *Under notations as above assume that* $\operatorname{char} \mathbb{F}_q$ *is even. Let* r *be the nonnegative integer such that* $2^r \mid\mid (N+1)$. *Let* m *be the nonnegative integer such that* $N + 1 = 2^r(m+1)$. *Let* θ *be a primitive* $(m+1)$*-th root of* 1. *Moreover we assume the following in the corresponding cases:*

- *If* $r = 0$, *then* $a/b \notin \{1/b + \theta^i + \theta^{-i} : 1 \leq i \leq m/2\}$.
- *If* $r \geq 1$ *and* $m = 0$, *then* $a \neq 1$.
- *If* $r \geq 1$ *and* $m \geq 1$, *then* $a/b \notin \{1/b\} \cup \{1/b + \theta^i + \theta^{-i} : 1 \leq i \leq m/2\}$.

Then $\pi^{\otimes 2N}\left(\hat{C}_N(a, b)\right)$ *is an LCD code with parameters* $[2nN, sN, D^*]_q$ *such that* $D^* \geq dD$, *where* D *is the minimum distance of* $\hat{C}_N(a, b)$.

Proof. Using Theorem 2.9 we obtain that $\hat{C}_N(a,b)$ is an LCD code over the extension field $\mathbb{F}_{q^s}$ with minimum distance D. As $\pi(\mathbb{F}_{q^s})$ is an $[n,s,d]_q$ isometry code, we complete the proof by [7, Theorem 3.1]. □

Next we consider the odd characteristic case.

Theorem 3.3. *Under notation as above assume that* char $\mathbb{F}_q$ *is odd, which is* p. *Let* r *be the nonnegative integer such that* $p^r \mid\mid (N+1)$. *Let* m *be the nonnegative integer such that* $N+1 = p^r(m+1)$. *Let* θ *be a primitive* $2(m+1)$*-th root of* 1. *Let* $\mu^2 = -1$. *Moreover, we assume the following in the corresponding cases:*

- *If* $r = 0$, *then*
  $a/b \notin \{-\mu/b + \theta^i + \theta^{-i} : 1 \le i \le m\} \cup \{\mu/b + \theta^i + \theta^{-i} : 1 \le i \le m\}$.
- *If* $r \ge 1$ *and* $m = 0$, *then*
  $a/b \notin \{-\mu/b + 2, -\mu/b - 2, \mu/b + 2, \mu/b - 2\}$.
- *If* $r \ge 1$ *and* $m \ge 1$, *then*
  $a/b \notin \{-\mu/b + 2, -\mu/b - 2, \mu/b + 2, \mu/b - 2\} \cup \{-\mu/b + \theta^i + \theta^{-i} : 1 \le i \le m\} \cup \{\mu/b + \theta^i + \theta^{-i} : 1 \le i \le m\}$.

Then $\pi^{\otimes 2N}\left(\hat{C}_N(a,b)\right)$ *is an LCD code with parameters* $[2nN, sN, D^*]_q$ *such that* $D^* \ge dD$, *where* D *is the minimum distance of* $\hat{C}_N(a,b)$.

Proof. The proof is similar to that of Theorem 3.2. The difference is that we use Theorem 2.10 instead of Theorem 2.9. □

In the following examples, we illustrate how to construct LCD codes with a prescribed lower bound on the minimum distance over small fields, in particular $\mathbb{F}_2$ and $\mathbb{F}_3$, using the methods of this paper. In fact, we obtain good codes having optimal and almost optimal parameters and the actual minimum distances of our constructed codes are even better than the prescribed lower bounds in these examples.

Example 3.1. *Let* $s = 2$, $q = 2$ *and* $N = 4$. *Let* w *be a primitive element of* $\mathbb{F}_{q^s}$ *satisfying* $w^2 + w + 1 = 0$. *For* $a = w$ *and* $b = 1$, *the* $[2N, N]_{q^s}$ *code* $\hat{C}_N(a,b)$ *given in Definition 2.5 is an LCD code having parameters* $[4,2,3]_4$ *(see Theorem 2.9). Put* $n = 4$. *For* $a_1 = w$, $a_2 = w^2$, $a_3 = 1$ *and* $a_4 = 1$, *the* $\mathbb{F}_q$*-linear map*

$$\begin{array}{rcl} \pi : \mathbb{F}_{q^s} & \to & \mathbb{F}_q^n \\ x & \mapsto & (\mathrm{Tr}(a_1 x), \mathrm{Tr}(a_2 x), \mathrm{Tr}(a_3 x), \mathrm{Tr}(a_4 x)) \end{array}$$

is an isometry map such that the corresponding isometry code $\pi(\mathbb{F}_{q^s})$ *is an* $[4,2,2]_2$ *code. Here* Tr *is the trace map from* $\mathbb{F}_{q^s}$ *onto* $\mathbb{F}_q$. *Using Theorem 3.2 we obtain that* $\pi^{\otimes 2N}\left(\hat{C}_N(a,b)\right)$ *is an LCD code with parameters* $[16,4,D^*]_2$ *with the prescribed lower*

bound on the minimum distance D^* given by $D^* \geq 6$. In fact using Magma [4] it is easy to verify that $D^* = 7$. This is an optimal LCD code, namely the largest minimum distance D of LCD code with parameters $[16, 4, D]_2$ is 7 (see [1]).

Example 3.2. *Let $s = 3$, $q = 2$ and $N = 4$. Let w be a primitive element of $\mathbb{F}_{q^s}$ satisfying $w^3 + w + 1 = 0$. For $a = w$ and $b = w^6$, the $[2N, N]_{q^s}$ code $\hat{C}_N(a, b)$ given in Definition 2.5 is an LCD code having parameters $[4, 2, 3]_4$ (see Theorem 2.9). Put $n = 5$. For $a_1 = w^3$, $a_2 = w^5$, $a_3 = w^6$, $a_4 = 1$ and $a_5 = 1$, the $\mathbb{F}_q$-linear map*

$$\begin{array}{rcl} \pi : \mathbb{F}_{q^s} & \to & \mathbb{F}_q^n \\ x & \mapsto & (\mathrm{Tr}(a_1 x), \mathrm{Tr}(a_2 x), \mathrm{Tr}(a_3 x), \mathrm{Tr}(a_4 x), \mathrm{Tr}(a_5 x)) \end{array}$$

is an isometry map such that the corresponding isometry code $\pi(\mathbb{F}_{q^s})$ is an $[5, 3, 2]_2$ code. Here Tr *is the trace map from $\mathbb{F}_{q^s}$ onto $\mathbb{F}_q$. Using Theorem 3.2 we obtain that $\pi^{\otimes 2N}\left(\hat{C}_N(a, b)\right)$ is an LCD code with parameters $[20, 6, D^*]_2$ with the prescribed lower bound on the minimum distance D^* given by $D^* \geq 6$. In fact using Magma [4] it is easy to verify that in fact $D^* = 7$. This is an almost optimal LCD code, namely the largest minimum distance D of and LCD code with parameters $[20, 6, D]_2$ is 8 (see [1]).*

Example 3.3. *Let $s = 2$, $q = 3$ and $N = 4$. Let w be a primitive element of $\mathbb{F}_{q^s}$ satisfying $w^2 + 2w + 2 = 0$. For $a = 2$ and $b = w$, the $[2N, N]_{q^s}$ code $\hat{C}_N(a, b)$ given in Definition 2.5 is an LCD code having parameters $[4, 2, 3]_9$ (see Theorem 2.10). Put $n = 5$. For $a_1 = w$, $a_2 = w$, $a_3 = w^3$, $a_4 = w^3$ and $a_5 = 2$, the $\mathbb{F}_q$-linear map*

$$\begin{array}{rcl} \pi : \mathbb{F}_{q^s} & \to & \mathbb{F}_q^n \\ x & \mapsto & (\mathrm{Tr}(a_1 x), \mathrm{Tr}(a_2 x), \mathrm{Tr}(a_3 x), \mathrm{Tr}(a_4 x), \mathrm{Tr}(a_5 x)) \end{array}$$

is an isometry map such that the corresponding isometry code $\pi(\mathbb{F}_{q^s})$ is an $[5, 2, 3]_3$ code. Here Tr *is the trace map from $\mathbb{F}_{q^s}$ onto $\mathbb{F}_q$. Using Theorem 3.2 we obtain that $\pi^{\otimes 2N}\left(\hat{C}_N(a, b)\right)$ is an LCD code with parameters $[20, 4, D^*]_3$ with the prescribed lower bound on the minimum distance D^* given by $D^* \geq 9$. Using Magma [4] it is easy to verify that in fact $D^* = 10$. The largest minimum distance D of an LCD code with parameters $[20, 4, D]_3$ is 12 by* [2, Table 7].

4. Conclusion

In this paper we have constructed LCD double Toeplitz codes from tridiagonal symmetric Toeplitz matrices. It would be worthwhile to extend these results to symmetric Toeplitz matrices with more than three nontrivial diagonals. We conjecture that this might require multivariate Dickson polynomials [10]. This might help to construct DT codes over small fields without recourse to the concatenation process of the previous section.

Acknowledgement

This research is supported by the National Natural Science Foundation of China (Grants no. 12071001 and 61672036), the Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), the Academic Fund for Outstanding Talents in Universities (gxbjZD03).

References

[1] M. Araya, M. Harada: On the minimum weights of binary linear complementary dual codes, Cryptography and Communications, Discrete Structures, Boolean Functions and Sequences, **12** (2020), 285–300.

[2] M. Araya, M. Harada, K. Saito: On the minimum weights of binary LCD codes and ternary LCD codes, `https://arxiv.org/pdf/1908.08661.pdf`.

[3] M. Bhargava, M. E. Zieve: Factoring Dickson Polynomials over Finite Fields, Finite Fields Appl. **5** (1999), no. 2, 103–111.

[4] W. Bosma, J. Cannon, and C. Playoust: The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997), 235–265.

[5] Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. Adv. Math. Commun. **10**(1) (2016), 131–150.

[6] C. Carlet, S. Mesnager, C. Tang, Y. Qi, R. Pellikaan: Linear codes over F_q are equivalent to LCD codes for $q > 3$, IEEE Transactions on Information Theory-IT, **10** (2018), 3010–3017.

[7] Claude Carlet, Cem Güneri, Ferruh Özbudak, Patrick Solé, A new concatenated type construction for LCD codes and isometry codes, Discrete Math, **341** (2018), 830–835.

[8] M. Grassl, Code tables: Bounds on the parameters of various types of codes, Available online at http:// www.codetables.de/, Accessed on 2021-02-28

[9] Daitao Huang, Minjia Shi, Patrick Solé, Double Circulant Self-Dual and LCD Codes Over Z_{p^2}. Int. J. Found. Comput. Sci., **30**(3) (2019), 407–416.

[10] R. Lidl, G. L. Mullen, and G. Turnwald: *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Math., Longman, London/Harlow/Essex (1993).

[11] J. Massey: Linear codes with complementary duals, Discrete Math. **106/107** (1992), 337–342.

[12] N. Sendrier On the dimension of the hull. SIAM Journal on Discrete Mathematics, **10**(2) (1997), 282–293.

[13] N. Sendrier , Finding the permutation between equivalent codes: the support splitting algorithm, IEEE Trans. Inf. Theory, **46**(4) (2000), 1193–1203.

[14] Minjia Shi, Daitao Huang, Lin Sok, Patrick Solé, Double circulant LCD codes over $\mathbb{Z}_4$. Finite Fields Their Appl. **58** (2019), 133–144.

[15] Minjia Shi, Daitao Huang, Lin Sok, Patrick Solé, Double circulant self-dual and LCD codes over Galois rings. Adv. Math. Commun. **13**, (2019), 171–183.

[16] Minjia Shi, Liqin Qian, Patrick Solé, On the self-dual negacirculant codes of index two and four, Des. Codes Cryptography **86** (11), (2018), 2485–2494.

[17] Minjia Shi, Li Xu, Patrick Solé, On isodual double Toeplitz codes, `https://arxiv.org/abs/2102.09233.`

[18] Minjia Shi, Hongwei Zhu, Liqin Qian, Lin Sok, Patrick Solé, On self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q$, Cryptography and Communications, Discrete Structures, Boolean Functions and Sequences, **12**,(2020), 53–70.