MDS OR NMDS LCD CODES FROM TWISTED REED-SOLOMON CODES

DAITAO HUANG, QIN YUE, AND YONGFENG NIU

Abstract. Maximum distance separable codes with linear complementary duals (LCD MDS codes) are very important in coding theory and practice. Thus it is interesting to construct LCD MDS codes. In this paper, we give check matrices of twisted generalized Reed-Solomon codes and construct three classes of new LCD MDS codes from twisted generalized Reed-Solomon codes. Moreover, LCD NMDS codes are also presented.

1. Introduction

A linear complementary dual code (LCD) is a linear code $\mathcal{C}$ whose dual code $\mathcal{C}^{\perp}$ satisfies $\mathcal{C} \cap \mathcal{C}^{\perp} = \{\mathbf{0}\}$. Massey demonstrated that there exists asymptotically good LCD codes and provided an optimum linear coding solution for the two-user binary adder channel [8]. Afterwards, Yang and Massey [20] gave a necessary and sufficient condition for a cyclic code to have a complementary dual. In [19], Li et al. showed some families of LCD cyclic code over finite field and gave their parameters. Bringer et al. [17] and Carlet and Guilley [4] introduced and analyzed a masking scheme, called orthogonal direct sum masking (ODSM), to protect against side-channel attacks and fault injection attacks (FIAs). The complementary-dual property plays a decisive role in the working performance of ODSM, because it enables us to use orthogonal projection to recover information of an LCD code to against FIAs. It is well known that LCD codes have been widely used in communications systems, consumer electronics, cryptography and so on. Moreover, some other classes of LCD codes were explicitly considered in [11]-[18].

It was shown that LCD codes with relatively large minimum distance are desirable. Maximum distance separable (MDS) codes are optimal in the sence that no code of length n with M codewords has a larger minimum distance than an MDS code with length n and size M. The construction of LCD MDS codes is thus becoming a hot research issue in coding theory. Recently, Jin constructed several classes of LCD MDS codes by using two classes of generalized Reed-Solomon codes [5]. Then, Chen and Liu constructed some new LCD MDS codes by a different approach from generalized

---

2010 *Mathematics Subject Classification.* 94B05.

Key words and phrases. Linear complementary dual, generalized twisted Reed-Solomon codes, MDS codes .

This work was supported in part by National Natural Science Foundation of China (No. 61772015).

Reed-Solomon codes [7]. In [17], Carlet et al. showed LCD codes are equivalent to an arbitrary linear code for $q > 3$ in the Euclidean case. In [1], Beelen et al. presented twisted Reed-Solomon codes and gave a efficient and necessary condition for twisted Reed-Solomon codes to be MDS. In this paper, we constructed several classes of LCD MDS codes from twisted Reed-Solomon codes. Since twisted Reed-Solomon codes is different from Reed-Solomon codes, then LCD MDS codes we constructed in this paper is different from the known. Moreover, NMDS codes were introduced in 1995 in [21] by weakening the definition of MDS codes. If a code has one singleton defect from being an MDS code, then it is called almost MDS (AMDS). An AMDS code is an NMDS code if the dual code is also an AMDS code. NMDS codes also have application in secret sharing scheme [22, 23]. In this paper, we also present several classes of NMDS LCD codes from twisted generalized Reed-Solomon codes.

The paper is organized as follows. In section 2, some basic notations and results about twisted generalized Reed-Solomon codes are introduced. In Section 3, three new constructions of MDS or NMDS LCD codes are provided. In Section 4, We conclude the paper.

2. Preliminaries

In this section, we review some basic notations and some basic knowledge. In particular, we introduce MDS codes and NMDS codes from twisted generalized Reed-Solomon codes and show their check matrices.

2.1. **TGRS codes.**

Let $\mathbb{F}_q[x]$ be a polynomial ring over a field field $\mathbb{F}_q$ of order q. We denote the rank of a matric M over $\mathbb{F}_q$ by $R(M)$. We abbreviate generalized Reed-Solomon codes, twisted Reed-Solomon codes, and twisted generalized Reed-Solomon codes as RS codes, GRS codes, and TGRS codes, respectively.

Now, let us recall some definitions of TRS codes in [1].

Definition 1. *Let $\mathcal{V}$ be a k-dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q[x]$. Let $\alpha_1, \dots, \alpha_n$ be distinct elements in $\mathbb{F}_q$ and $\alpha = (\alpha_1, \dots, \alpha_n)$. Let $v_1, \dots, v_n$ be nonzero elements in $\mathbb{F}_q$ and $v = (v_1, \dots, v_n)$. We call $\alpha_1, \dots, \alpha_n$ the evaluation points. Define the evaluation map of α on $\mathcal{V}$ by*

$$ev_\alpha : \mathcal{V} \longrightarrow \mathbb{F}_q^n, f(x) \longmapsto ev_\alpha(f(x)) = (f(\alpha_1), \dots, f(\alpha_n));$$

define the evaluation map of α and v by

$$ev_{\alpha,v} : \mathcal{V} \longrightarrow \mathbb{F}_q^n, f(x) \longmapsto ev_\alpha(f(x)) = (v_1 f(\alpha_1), \dots, v_n f(\alpha_n)).$$

Definition 2. *Let k, t, and h be positive integers with $0 \le h < k \le q$ and $\eta \in \mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$. Define the set of (k, t, h, η)-twisted polynomials as*

$$\mathcal{V}_{k,t,h,\eta} = \{f(x) = \sum_{i=0}^{k-1} a_i x^i + \eta a_h x^{k-1+t} : a_i \in \mathbb{F}_q, 0 \le i \le k-1\},$$

which is a k-dimensional $\mathbb{F}_q$-linear subspace. We call h the hook and t the twist.

In this paper, we always assume that $h = 0$ and $t = 1$, so

$$\mathcal{V}_{k,1,0,\eta} = \{f(x) = \sum_{i=0}^{k-1} a_i x^i + \eta a_0 x^k : a_i \in \mathbb{F}_q, 0 \le i \le k-1\}.$$

For convenience, set $k \le n - k$.

Definition 3. *Let $\alpha_1, \ldots, \alpha_n$ be distinct elements in $\mathbb{F}_q$ and $\alpha = (\alpha_1, \ldots, \alpha_n)$. Let $v_1, \ldots, v_n$ be nonzero elements in $\mathbb{F}_q$ and $v = (v_1, \ldots, v_n)$. Let $\mathcal{V}_{k,1,0,\eta}$ be in Definition 2. The TRS code of length n and dimension k is defined as*

$$\mathcal{C}_k(\alpha, 1, \eta) = ev_\alpha(\mathcal{V}_{k,1,0,\eta}) \subseteq \mathbb{F}_q^n.$$

The TGRS code of length n and dimension k is defined as

$$\mathcal{C}_k(\alpha, v, \eta) = ev_{\alpha,v}(\mathcal{V}_{k,1,0,\eta}) \subseteq \mathbb{F}_q^n.$$

Remark 1. *Compared with GRS codes, TGRS codes is different. See more details in* [1].

In fact, if $v = (1, \ldots, 1) = 1$, then $\mathcal{C}_k(\alpha, v, \eta) = \mathcal{C}_k(\alpha, 1, \eta)$, i.e., the TGRS code is the TRS code.

Let G_k is a generator matrix of $\mathcal{C}_k(\alpha, v, \eta)$, then

$$G_k = \begin{pmatrix} v_1(1+\eta\alpha_1^k) & v_2(1+\eta\alpha_2^k) & \ldots & v_n(1+\eta\alpha_n^k) \\ v_1\alpha_1 & v_2\alpha_2 & \ldots & v_n\alpha_n \\ \vdots & \vdots & & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \ldots & v_n\alpha_n^{k-1} \end{pmatrix}. \tag{2.1}$$

Definition 4. *A $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is MDS if $d = n - k + 1$. A $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is almost MDS if $d = n - k$. A $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is NMDS if $\mathcal{C}$ and the dual of $\mathcal{C}$ are almost MDS codes, respectively.*

Now, we present the sufficient and necessary condition that TGRS code is an MDS or NMDS code (The part of MDS codes are covered in [1]).

Lemma 1. *Let $\alpha_1, \ldots, \alpha_n$ are distinct elements in $\mathbb{F}_q$, $\alpha = (\alpha_1, \ldots, \alpha_n)$, $v = (v_1, \ldots, v_n) \in (\mathbb{F}_q^*)^n$, and $\eta \in \mathbb{F}_q^*$. Let*

$$S_k = \{(-1)^k \prod_{i \in I} \alpha_i^{-1} : I \subset \{1, \ldots, n\}, |I| = k\},$$

then we have the following:
(1) the TGRS code $\mathcal{C}_k(\alpha, v, \eta)$ is MDS if and only if $\eta \in \mathbb{F}_q^* \setminus S_k$;
(2) the TGRS code $\mathcal{C}_k(\alpha, v, \eta)$ is NMDS if and only if $\eta \in S_k$.

Proof. (1) For the completeness, we provide another method to prove it.

$C_k(\alpha, v, \eta)$ is MDS $\Longleftrightarrow$ any k columns of G_k are linear independently.

$$\Longleftrightarrow \begin{vmatrix} v_{i_1}(1+\eta\alpha_{i_1}^k) & v_{i_2}(1+\eta\alpha_{i_2}^k) & \dots & v_{i_k}(1+\eta\alpha_{i_k}^k) \\ v_{i_1}\alpha_{i_1} & v_{i_2}\alpha_{i_2} & \dots & v_{i_k}\alpha_{i_k} \\ \vdots & \vdots & & \vdots \\ v_{i_1}\alpha_{i_1}^{k-1} & v_{i_2}\alpha_{i_2}^{k-1} & \dots & v_{i_k}\alpha_{i_k}^{k-1} \end{vmatrix} \neq 0,$$

where $\{i_1, i_2, \dots, i_k\}$ is an arbitrary k-subset of $\{1, 2, \dots, n\}$. Then the result follows immediately by linear algebra.

(2) " $\Longleftarrow$ " By linear algebra, we know that any $k-1$ columns of G_k are linear independently over $\mathbb{F}_q$. If $\eta \in S_k$, then there exists k columns of G_k are linear dependently over $\mathbb{F}_q$. Thus, the parameter of $C_k(\alpha, v, \eta)^{\perp}$ is $[n, n-k, k]$. Similarly, since any $n-k-1$ columns of H_k are linear independently over $\mathbb{F}_q$ and $C_k(\alpha, v, \eta)^{\perp}$ is not MDS, we obtain the parameter of $C_k(\alpha, v, \eta)$ is $[n, k, n-k]$. Thus, $C_k(\alpha, v, \eta)$ is NMDS.

" $\Longrightarrow$ " Conversely, if $C_k(\alpha, v, \eta)$ is NMDS, then the parameter of $C_k(\alpha, v, \eta)^{\perp}$ is $[n, n-k, k]$, which implies that there exists k columns of G_k is linear dependently over $\mathbb{F}_q$, i.e. $\eta \in S_k$. $\square$

Remark 2. *It should be noted that $\mathbb{F}_q^* \setminus S_k$ in Lemma 1 can always be a nonempty set. In particular, if $q-1 > \frac{n!}{k!(n-k)!}$, or $\{\alpha_1, \alpha_2, \dots, \alpha_n\} \subseteq H$, where H is a proper subgroup of $\mathbb{F}_q^*$, then $\mathbb{F}_q^* \setminus S_k$ is a nonempty set. Or rather, there are many choices of $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ such that S_k is a proper subset of $\mathbb{F}_q^*$.*

Let G_k be the generator matrix of $\mathcal{C}_k(\alpha, v, \eta)$ as (2.1). We shall find the check matrix of of $\mathcal{C}_k(\alpha, v, \eta)$.

Theorem 1. *For convenience, set $a = \prod_{i=1}^n \alpha_i \neq 0$. Then*

$$H_{n-k} = \begin{pmatrix} \frac{u_1}{v_1} & \frac{u_2}{v_2} & \dots & \frac{u_n}{v_n} \\ \frac{u_1}{v_1}\alpha_1 & \frac{u_2}{v_2}\alpha_2 & \dots & \frac{u_n}{v_n}\alpha_n \\ \vdots & \vdots & & \vdots \\ \frac{u_1}{v_1}\alpha_1^{n-k-2} & \frac{u_2}{v_2}\alpha_2^{n-k-2} & \dots & \frac{u_u}{v_n}\alpha_1^{n-k-2} \\ \frac{u_1}{v_1}(\alpha_1^{n-k-1} - \frac{\eta a}{\alpha_1}) & \frac{u_2}{v_2}(\alpha_2^{n-k-1} - \frac{\eta a}{\alpha_2}) & \dots & \frac{u_n}{v_n}(\alpha_n^{n-k-1} - \frac{\eta a}{\alpha_n}) \end{pmatrix} \quad (2.2)$$

is the check matrix of $C_k(\alpha, v, \eta)$, where $u_i = \prod_{j=1, j\neq i}^n (\alpha_i - \alpha_j)^{-1}$, $1 \leq i \leq n$.

Proof. To calculate the check matrix of $\mathcal{C}_k(\alpha, v, \eta)$, we investigate the check matrix of $\mathcal{C}_k(\alpha, 1, \eta)$.

There is a $n \times n$ matrix over $\mathbb{F}_q$:

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{pmatrix}.$$

(1) Consider the system of equations over $\mathbb{F}_q$: $G(u_1, u_2, \ldots, u_n)^T = (0, \ldots, 0, 1)^T$. Then there is an unique solution: $(u_1, \ldots, u_n)^T$, where $u_i = \prod_{j=1, j\neq i}^{n} (\alpha_i - \alpha_j)^{-1}$, $1 \leq i \leq n$.

(2) Consider the system of equations over $\mathbb{F}_q$: $G(w_1, w_2, \ldots, w_n)^T = (1, 0, \ldots, 0)^T$. Then there is an unique solution: $(w_1, \ldots, w_n)^T$, where $w_i = \prod_{j=1, j\neq i}^{n} (\alpha_i - \alpha_j)^{-1}\alpha_j = u_i \prod_{j=1, j\neq i}^{n} \alpha_j, 1 \leq i \leq n$.

(3) Let

$$H = \begin{pmatrix} w_1 & u_1\alpha_1^{n-2} & \cdots & u_1\alpha_1^{n-k-1} & \cdots & u_1 \\ w_2 & u_2\alpha_1^{n-2} & \cdots & u_2\alpha_1^{n-k-1} & \cdots & u_2 \\ \vdots & \vdots & & \vdots & & \vdots \\ w_n & u_n\alpha_n^{n-2} & \cdots & u_n\alpha_n^{n-k-1} & \cdots & u_n \end{pmatrix}.$$

Then

$$GH = L = \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & & \vdots & & \vdots \\ 0 & * & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * & \cdots & 1 \end{pmatrix}$$

is an lower triangular matrix over $\mathbb{F}_q$ and its all elements of main diagonal are equal to 1, where $*$ is not necessarily 0. This is a little similar to RS codes (for details see RS codes in [8]) but more difficult.

(4) Hence

$$P_1GHP_2 = L' = \begin{pmatrix} 1 & * & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & & \vdots & & \vdots \\ 0 & * & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * & \cdots & 1 \end{pmatrix},$$

where $P_1 = P(1, (k+1)(\eta))$ is an elementary matrix, that 1th row is replaced by sum of η times $k+1$th row and 1th row, and $P_2 = P(1, (k+1)(-\eta))$ is an elementary matrix, that $k+1$th column is replaced by sum of $-\eta$ times 1th column and $k+1$th column.

For convenience, let $a = \prod_{i=1}^{n} \alpha_i \neq 0$ and

$$H'_{n-k} = \begin{pmatrix} u_1 & u_2 & \cdots & u_n \\ u_1\alpha_1 & u_2\alpha_2 & \cdots & u_n\alpha_n \\ \vdots & \vdots & & \vdots \\ u_1\alpha_1^{n-k-2} & u_2\alpha_2^{n-k-2} & \cdots & u_1\alpha_1^{n-k-2} \\ u_1(\alpha_1^{n-k-1} - \eta\frac{a}{\alpha_1}) & u_2(\alpha_2^{n-k-1} - \eta\frac{a}{\alpha_2}) & \cdots & u_n(\alpha_n^{n-k-1} - \eta\frac{a}{\alpha_n}) \end{pmatrix}.$$

Then $G'_k {H'_{n-k}}^T = 0$, where $G'_k = G_k$ with $v_i = 1, 1 \leq i \leq n$.

Let H_{n-k} be the matrix as (2.2). Then $G_k H_{n-k}^T = 0$ and it is the check matrix of $C_k(\alpha, v, n)$.

By the discussion above, the result follows immediately. $\square$

2.2. **Hull of TGRS codes.** Given two vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$, the Euclidean inner product is defined by $\langle \mathbf{x}, \mathbf{y} \rangle_E = \sum_{i=1}^{n} x_i y_i$. For a linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$, the code

$$\mathcal{C}^{\perp} = \{\mathbf{x} \in \mathbb{F}_q^n \,|\langle \mathbf{x}, \mathbf{y} \rangle_E = 0, \text{ for all } \mathbf{y} \in \mathcal{C}\}$$

is referred to as its Euclidean dual code. Define the Hull of C as

$$Hull(\mathcal{C}) = \mathcal{C} \bigcap \mathcal{C}^{\perp}.$$

If $Hull(\mathcal{C}) = \{0\}$, $\mathcal{C}$ is called an *Euclidean* LCD code: if $Hull(\mathcal{C}) = \mathcal{C}$ and $dim(C) = dim(C^{\top})$, $\mathcal{C}$ is called a self-dual code; if $Hull(\mathcal{C}) = \mathcal{C}$, $\mathcal{C}$ is call a self-orthogonal code.

To investigate LCD TGRS codes, we first study the hull of TGRS codes with the same notations above.

Lemma 2. *$dim(Hull(C_k(\alpha, v, \eta)) = n - R \begin{pmatrix} G_k \\ H_{n-k} \end{pmatrix}$.*

Proof. Firstly, by the definition, we obtain

$$Hull(C_k(\alpha, v, \eta) = \{\mu G \mid \mu G_k = \kappa H_{n-k}, \mu \in \mathbb{F}_q^k, \kappa \in \mathbb{F}_q^{n-k}\}.$$

Then we have

$$dim(Hull(C_k(\alpha, v, \eta))) = dim\{\mu \mid \begin{pmatrix} \mu & -\kappa \end{pmatrix} \begin{pmatrix} G_k \\ H_{n-k} \end{pmatrix} = 0,\ \mu \in \mathbb{F}_q^k, \kappa \in \mathbb{F}_q^{n-k}\}$$

$$= dim\{\begin{pmatrix} \mu & -\kappa \end{pmatrix} \mid \begin{pmatrix} \mu & -\kappa \end{pmatrix} \begin{pmatrix} G_k \\ H_{n-k} \end{pmatrix} = 0,\ \mu \in \mathbb{F}_q^k, \kappa \in \mathbb{F}_q^{n-k}\}$$

$$= n - R \begin{pmatrix} G_k \\ H_{n-k} \end{pmatrix},$$

where the second equality holds because the rank of rows of H_{n-k} is full. $\square$

Next, we consider LCD codes $C_k(\alpha, v, \eta)$ which satisfies $dim(Hull(C_k(\alpha, v, \eta)) = 0$, i.e. $R \begin{pmatrix} G_k \\ H_{n-k} \end{pmatrix} = n$.

Considering $\begin{pmatrix} G_k^T & H_{n-k}^T \end{pmatrix}$, multiplying v_i to the ith row for $1 \le i \le n$, we then obtain a matrix D, where

$$D = \begin{pmatrix} v_1^2(1+\eta\alpha_1^k) & v_1^2\alpha_1 & \ldots & v_1^2\alpha_1^{k-1} & u_1 & u_1\alpha_1 & \ldots & u_1\alpha_1^{n-k-2} & u_1(\alpha_1^{n-k-1} - \eta\frac{a}{\alpha_1}) \\ v_2^2(1+\eta\alpha_1^k) & v_2^2\alpha_2 & \ldots & v_2^2\alpha_2^{k-1} & u_2 & u_2\alpha_2 & \ldots & u_2\alpha_2^{n-k-2} & u_2(\alpha_2^{n-k-1} - \eta\frac{a}{\alpha_2}) \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ v_n^2(1+\eta\alpha_n^k) & v_n^2\alpha_n & \ldots & v_n^2\alpha_n^{k-1} & u_n & u_n\alpha_n & \ldots & u_n\alpha_n^{n-k-2} & u_n(\alpha_n^{n-k-1} - \eta\frac{a}{\alpha_n}) \end{pmatrix}.$$

Next, we will give some construction of LCD MDS codes by choosing α, v such that $R(D) = n$.

3. LCD MDS codes

In this section, we always assume that $C_k(\alpha, v, \eta)$ is a TGRS code, and S_k is defined as in (2.2). Then it is a MDS or NMDS code. Now we shall construct three classes of LCD MDS codes or LCD NMDS codes from TGRS codes. We always assume q is an odd prime power.

3.1. **Construction I.** If $n|q-1$, let $\lambda \in \mathbb{F}_q^*$, then there is an element $\epsilon \in \mathbb{F}_q^*$ such that $\epsilon^n = \lambda$. Let $w \in \mathbb{F}_q$ with $\mathrm{ord}(w) = n$. Then there is an irreducible factorization over $\mathbb{F}_q$:

$$m(x) = x^n - \lambda = \prod_{i=1}^{n}(x - \epsilon w^i).$$

Set $\alpha_i = \epsilon w^{i-1}$, $1 \le i \le n$. Consequently, $u_i = \prod_{j=1, j\neq i}^{n}(\alpha_i - \alpha_j)^{-1} = m'(\alpha_i)^{-1} = \frac{1}{n\lambda}\alpha_i, 1 \le i \le n$. Let $a = \prod_{i=1}^{n} \alpha_i = (-1)^{n+1}\lambda$. To construct LCD codes, we need the following statement.

Lemma 3. *If $n = 2k$, then $1 + \eta^2 a = 1 - \eta^2\lambda \neq 0$.*

Proof. Suppose that $1 - \eta^2\lambda = 0$, then $x^{2k} - \lambda = x^{2k} - \eta^{-2} = (x^k + \eta^{-1})(x^k - \eta^{-1})$. Consequently, $(-1)^k \prod_{i\in I} \alpha_i = \eta^{-1}$ or $-\eta^{-1}$ for some $I \subseteq \{1, 2, \ldots, n\}$ with $|I| = k$, which is a contraction with the choice of η. $\square$

Let $v_i \in \{1, -1\}$ for $k \le i \le n$, $v_i \in \mathbb{F}_q \setminus \{0, -1, 1\}$ for $1 \le i \le k-1$. Then we have

$$D = \begin{pmatrix} v_1^2(1+\eta\alpha_1^k) & v_1^2\alpha_1 & \ldots & v_1^2\alpha_1^{k-1} & \frac{1}{n\lambda}\alpha_1 & \ldots & \frac{1}{n\lambda}\alpha_1^{n-k-1} & \frac{1}{n\lambda}(\alpha_1^{n-k} - \eta a) \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ v_{k-1}^2(1+\eta\alpha_{k-1}^k) & v_{k-1}^2\alpha_{k-1} & \ldots & v_{k-1}^2\alpha_{k-1}^{k-1} & \frac{1}{n\lambda}\alpha_{k-1} & \ldots & \frac{1}{n\lambda}\alpha_{k-1}^{n-k-1} & \frac{1}{n\lambda}(\alpha_{k-1}^{n-k} - \eta a) \\ 1+\eta\alpha_k^k & \alpha_k & \ldots & \alpha_k^{k-1} & \frac{1}{n\lambda}\alpha_k & \ldots & \frac{1}{n\lambda}\alpha_k^{n-k-1} & \frac{1}{n\lambda}(\alpha_k^{n-k} - \eta a) \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 1+\eta\alpha_n^k & \alpha_n & \ldots & \alpha_n^{k-1} & \frac{1}{n\lambda}\alpha_n & \ldots & \frac{1}{n\lambda}\alpha_n^{n-k-1} & \frac{1}{n\lambda}(\alpha_n^{n-k} - \eta a) \end{pmatrix}.$$

If $k \le n-k-1$, by elementary transformation of matrix D, we obtain the following,

$$D' = \begin{pmatrix} (v_1^2-1)\alpha_1 & \ldots & (v_1^2-1)\alpha_1^{k-1} & s_1+1 & \alpha_1 & \ldots & \alpha_1^{n-k-1} & \alpha_1^{n-k} - \eta a \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ (v_{k-1}^2-1)\alpha_{k-1} & \ldots & (v_{k-1}^2-1)\alpha_{k-1}^{k-1} & s_{k-1}+1 & \alpha_{k-1} & \ldots & \alpha_{k-1}^{n-k-1} & \alpha_{k-1}^{n-k} - \eta a \\ 0 & \ldots & 0 & 1 & \alpha_k & \ldots & \alpha_k^{n-k-1} & \alpha_k^{n-k} - \eta a \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & \ldots & 0 & 1 & \alpha_n & \ldots & \alpha_n^{n-k-1} & \alpha_n^{n-k} - \eta a \end{pmatrix},$$

where $s_i = (v_i^2 - 1)(1 + \eta\alpha_i^k)$ for $1 \le i \le k-1$.

If $k = n-k$, then

$$D'' = \begin{pmatrix} (v_1^2-1)\alpha_1 & \dots & (v_1^2-1)\alpha_1^{k-1} & s_1+1+\eta^2 a & \alpha_1 & \dots & \alpha_1^{k-1} & \alpha_1^k-\eta a \\ \vdots & & & \vdots & \vdots & & \vdots & \vdots \\ (v_{k-1}^2-1)\alpha_{k-1} & \dots & (v_{k-1}^2-1)\alpha_{k-1}^{k-1} & s_{k-1}+1+\eta^2 a & \alpha_{k-1} & \dots & \alpha_{k-1}^{k-1} & \alpha_{k-1}^k-\eta a \\ 0 & \dots & 0 & 1+\eta^2 a & \alpha_k & \dots & \alpha_k^{k-1} & \alpha_k^k-\eta a \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 1+\eta^2 a & \alpha_n & \dots & \alpha_n^{k-1} & \alpha_n^k-\eta a \end{pmatrix}.$$

Using lemma 3, and by noting that the matrices D' and D'' are upper triangular block matrix, respectively. Then by some properties of Vandermonde determinant, it is not difficult to find D' and D'' are nonsingular. Then we have the following results.

Theorem 2. *Let $n|q-1$ with q a prime power and assume $m(x) = x^n - \lambda = \prod_{i=1}^n (x-\alpha_i) \in \mathbb{F}_q[x]$ with $\alpha_1, \dots, \alpha_n, \lambda \in \mathbb{F}_q$. Let $v_i \in \{1,-1\}$ for $k \le i \le n$ and $v_i \in \mathbb{F}_q \setminus \{-1,0,1\}$ for $1 \le i \le k-1$. Then*

$$C_k(\alpha, v, \eta) = \{(v_1 f(\alpha_1), \dots, v_n f(\alpha_n)) \mid f(x) = \sum_{i=1}^{k-1} f_i x^i + \eta f_0 x^k \in \mathbb{F}_q[x]\}$$

is an LCD MDS code, where $\eta \in \mathbb{F}_q^* \backslash S_k$.

Proof. Since $gcd(m(x), m'(x)) = 1$ and by the discussion above, we obtain $R(D) = n$. Consequently, LCD MDS is obvious. □

Remark 3. *In particular, if $\eta \in S_k$ in Theorem 2, then $C_k(\alpha, v, \eta)$ is an LCD NMDS code by Lemma 1.*

3.2. **Construction II.** Let $m(x) = x^n + bx + \lambda \in \mathbb{F}_{q_1}[x]$ with $\mathbb{F}_{q_1}$ a subfield of $\mathbb{F}_q$, and assume that $\mathbb{F}_q$ is the splitting field of $m(x)$ over $\mathbb{F}_{q_1}$. Assume that $\alpha_1, \alpha_2, \dots, \alpha_n$ are all roots of $m(x)$ in $\mathbb{F}_q$, i.e.,

$$m(x) = x^n + bx + \lambda = \prod_{i=1}^n (x-\alpha_i) \in \mathbb{F}_q[x].$$

Consequently, $u_i = \prod_{j=1, j\neq i}^n (\alpha_i - \alpha_j)^{-1} = m'(\alpha_i)^{-1} = \frac{\alpha_i}{b(1-n)\alpha_i - n\lambda}$. Let $a = \prod_{i=1}^n \alpha_i = (-1)^n \lambda$.

Let $v_i \in \{1,-1\}$ for $k \le i \le n$, $v_i \in \mathbb{F}_q \backslash \{0,-1,1\}$ for $1 \le i \le k-1$. Then we have

$$D = \begin{pmatrix} v_1^2(1+\eta\alpha_1^k) & v_1^2\alpha_1 & \dots & v_1^2\alpha_1^{k-1} & \frac{\alpha_1}{s_1} & \dots & \frac{\alpha_1^{n-k-1}}{s_1} & \frac{\alpha_1^{n-k}-\eta a}{s_1} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ v_{k-1}^2(1+\eta\alpha_{k-1}^k) & v_{k-1}^2\alpha_{k-1} & \dots & v_{k-1}^2\alpha_{k-1}^{k-1} & \frac{\alpha_{k-1}}{s_{k-1}} & \dots & \frac{\alpha_{k-1}^{n-k-1}}{s_{k-1}} & \frac{\alpha_{k-1}^{n-k}-\eta a}{s_{k-1}} \\ 1+\eta\alpha_k^k & \alpha_k & \dots & \alpha_k^{k-1} & \frac{\alpha_k}{s_k} & \dots & \frac{\alpha_k^{n-k-1}}{s_k} & \frac{\alpha_k^{n-k}-\eta a}{s_k} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 1+\eta\alpha_n^k & \alpha_n & \dots & \alpha_n^{k-1} & \frac{\alpha_n}{s_n} & \dots & \frac{\alpha_n^{n-k-1}}{s_n} & \frac{\alpha_n^{n-k}-\eta a}{s_n} \end{pmatrix},$$

where $s_i = b(1-n)\alpha_i - n\lambda$ for $1 \le i \le k-1$.

By elementary transformation of matrix, when $k \leq n-k-2$, we obtain that $D' =$

$$\begin{pmatrix} (v_1^2-1)\alpha_1 s_1 & \dots & (v_1^2-1)\alpha_1^{k-1}s_1 & (v_1^2-1)(1+\eta\alpha_1^k)s_1 - n\lambda & \alpha_1 & \dots & \alpha_1^{n-k}-\eta a \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ (v_{k-1}^2-1)\alpha_{k-1}s_{k-1} & \dots & (v_{k-1}^2-1)\alpha_{k-1}^{k-1}s_{k-1} & (v_1^2-1)(1+\eta\alpha_1^k)s_{k-1} - n\lambda & \alpha_{k-1} & \dots & \alpha_{k-1}^{n-k}-\eta a \\ 0 & \dots & 0 & -n\lambda & \alpha_k & \dots & \alpha_k^{n-k}-\eta a \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & -n\lambda & \alpha_n & \dots & \alpha_n^{n-k}-\eta a \end{pmatrix}.$$

Thus, $R(D) = n$.

When $k = n-k-1$ with n an odd integer, we obtain that $D'' =$

$$\begin{pmatrix} (v_1^2-1)\alpha_1 s_1 & \dots & (v_1^2-1)\alpha_1^{k-1}s_1 & (v_1^2-1)(1+\eta\alpha_1^k)s_1 + s & \alpha_1 & \dots & \alpha_1^{n-k}-\eta a \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ (v_{k-1}^2-1)\alpha_{k-1}s_{k-1} & \dots & (v_{k-1}^2-1)\alpha_{k-1}^{k-1}s_{k-1} & (v_{k-1}^2-1)(1+\eta\alpha_{k-1}^k)s_{k-1} + s & \alpha_{k-1} & \dots & \alpha_{k-1}^{n-k}-\eta a \\ 0 & \dots & 0 & s & \alpha_k & \dots & \alpha_k^{n-k}-\eta a \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & s & \alpha_n & \dots & \alpha_n^{n-k}-\eta a \end{pmatrix},$$

where $s = \eta^2 ba(1-n) - n\lambda$. Choose $\eta^2 \neq a^{-1}b^{-1}(1-n)^{-1}n\lambda$. thus, $R(D) = n$.

Theorem 3. *Let $\eta \in \mathbb{F}_q^* \setminus S_k$ and $\eta^2 \neq a^{-1}b^{-1}(1-n)^{-1}n\lambda$. Assume that $\{\alpha_1, \dots, \alpha_n\}$ is the set of roots of a trinomial $m(x)$, which is given by $m(x) = x^n + bx + \lambda$ for some $b, \lambda \in \mathbb{F}_q^*$ such that $\alpha_i \neq n\lambda b^{-1}(1-n)^{-1}$ for $1 \leq i \leq n$. Let $v_i \in \{1, -1\}$ for $k \leq i \leq n$, $v_i \in \mathbb{F}_q \setminus \{0, -1, 1\}$ for $1 \leq i \leq k-1$. Then*

$$C_k(\alpha, v, \eta) = \{(v_1 f(\alpha_1), \dots, v_n f(\alpha_n)) \mid f(x) = \sum_{i=1}^{k-1} f_i x^i + \eta f_0 x^k \in \mathbb{F}_q[x]\}$$

is an k dimensional LCD MDS code for any $k \leq \lfloor \frac{n}{2} \rfloor$ with n an odd integer, while for any $k \leq \lfloor \frac{n}{2} \rfloor - 1$ with n an even integer.

Proof. Since $m'(x) = nx^{n-1} + b$, $m(\alpha_i) = 0$ and $\alpha_i \neq n\lambda b^{-1}(1-n)^{-1}$, we then obtain $m'(\alpha_i) \neq 0$ for $i = 1, 2, \dots, n$. Consequently, $(m(x), m'(x)) = 1$. That implies $\alpha_1, \alpha_2, \dots, \alpha_n$ are distinct elements in $\mathbb{F}_q$. By the choice of $v_i, i = 1, 2, \dots, n$ and η, we obtain that $C_k(\alpha, v, \eta)$ is MDS code over $\mathbb{F}_q$ by Lemma 1. By the discussion above, since $\eta^2 \neq a^{-1}b^{-1}(1-n)^{-1}n\lambda$, then $R(D) = n$. Consequently, $C_k(\alpha, v, \eta)$ is LCD. Thus, the result follows immediately. □

Remark 4. *In particular, if $\eta \in S_k$ in Theorem 3, then $C_k(\alpha, v, \eta)$ is an LCD NMDS code by Lemma 1.*

3.3. **Construction III.** Let $q = p^m$, $n+1 = p^e$ with $e \leq m$ and $U = \{\alpha_1, \dots, \alpha_n\} \bigcup \{0\}$ be an additive subgroup of $\mathbb{F}_q$. Actually, U is a vector space of dimension e over $\mathbb{F}_p$. Let $m(x) = \frac{\prod_{u \in U}(x-u)}{x}$, and write $\prod_{u \in U}(x-u) = x^{p^e} + \sum_{j=0}^{e-1} a_i x^{p^j - 1} \in \mathbb{F}_q[x]$. Then

$$m(x) = \prod_{j=1}^{n}(x - \alpha_j) = x^{p^e - 1} + \sum_{j=1}^{e-1} a_i x^{p^j - 1} + (-1)^n a$$

with

$$a = \prod_{i=1}^{n} \alpha_i = \prod_{j\neq i, j=1}^{n} (\alpha_i - \alpha_j)(\alpha_i - 0).$$

Thus, $u_i = \prod_{j=1,j\neq i}^{n}(\alpha_i - \alpha_j)^{-1} = a^{-1}\alpha_i$.

Let $v_i \in \{1, -1\}$ for $k \leq i \leq n$, $v_i \in \mathbb{F}_q \setminus \{0, -1, 1\}$ for $1 \leq i \leq k-1$. Then we have

$$D = \begin{pmatrix} v_1^2(1+\eta\alpha_1^k) & v_1^2\alpha_1 & \dots & v_1^2\alpha_1^{k-1} & a^{-1}\alpha_1 & \dots & a^{-1}\alpha_1^{n-k-1} & a^{-1}(\alpha_1^{n-k} - \eta a) \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ v_{k-1}^2(1+\eta\alpha_{k-1}^k) & v_{k-1}^2\alpha_{k-1} & \dots & v_{k-1}^2\alpha_{k-1}^{k-1} & a^{-1}\alpha_{k-1} & \dots & a^{-1}\alpha_{k-1}^{n-k-1} & a^{-1}(\alpha_{k-1}^{n-k} - \eta a) \\ 1+\eta\alpha_k^k & \alpha_k & \dots & \alpha_k^{k-1} & a^{-1}\alpha_k & \dots & a^{-1}\alpha_k^{n-k-1} & a^{-1}(\alpha_k^{n-k} - \eta a) \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 1+\eta\alpha_n^k & \alpha_n & \dots & \alpha_n^{k-1} & a^{-1}\alpha_n & \dots & a^{-1}\alpha_n^{n-k-1} & a^{-1}(\alpha_n^{n-k} - \eta a) \end{pmatrix}.$$

If $k \leq n-k-1$, by elementary transformation of matrix D, we obtain the following,

$$D' = \begin{pmatrix} (v_1^2-1)\alpha_1 & \dots & (v_1^2-1)\alpha_1^{k-1} & s_1+1 & \alpha_1 & \dots & \alpha_1^{n-k-1} & \alpha_1^{n-k} - \eta a \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ (v_{k-1}^2-1)\alpha_{k-1} & \dots & (v_{k-1}^2-1)\alpha_{k-1}^{k-1} & s_{k-1}+1 & \alpha_{k-1} & \dots & \alpha_{k-1}^{n-k-1} & \alpha_{k-1}^{n-k} - \eta a \\ 0 & \dots & 0 & 1 & \alpha_k & \dots & \alpha_k^{n-k-1} & \alpha_k^{n-k} - \eta a \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 1 & \alpha_n & \dots & \alpha_n^{n-k-1} & \alpha_n^{n-k} - \eta a \end{pmatrix},$$

where $s_i = (v_i^2 - 1)(1 + \eta\alpha_i^k)$ for $1 \leq i \leq k-1$.

If $k = n-k$, then

$$D'' = \begin{pmatrix} (v_1^2-1)\alpha_1 & \dots & (v_1^2-1)\alpha_1^{k-1} & s_1+1+\eta^2 a & \alpha_1 & \dots & \alpha_1^{k-1} & \alpha_1^{k} - \eta a \\ \vdots & & & \vdots & \vdots & & \vdots & \vdots \\ (v_{k-1}^2-1)\alpha_{k-1} & \dots & (v_{k-1}^2-1)\alpha_{k-1}^{k-1} & s_{k-1}+1+\eta^2 a & \alpha_{k-1} & \dots & \alpha_{k-1}^{k-1} & \alpha_{k-1}^{k} - \eta a \\ 0 & \dots & 0 & 1+\eta^2 a & \alpha_k & \dots & \alpha_k^{k-1} & \alpha_k^{k} - \eta a \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 1+\eta^2 a & \alpha_n & \dots & \alpha_n^{k-1} & \alpha_n^{k} - \eta a \end{pmatrix}.$$

Make an assumption that $\eta^2 \neq \frac{-1}{a}$, and by noting that the matrices D' and D'' are upper triangular block matrix, respectively. Then by some properties of Vandermonde determinant, it is not difficult to find D' and D'' are nonsingular. Then we have the following results.

Theorem 4. *Let $q = p^m, n+1 = p^e$ with q a prime power and e, m are integers satisfying $e \leq m$. Assume $x^{p^e-1} + \sum_{i=0}^{e-1} a_i x^{p^i} = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{F}_q[x]$ with $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$. Let $v_i \in \{1, -1\}$ for $k \leq i \leq n$ and $v_i \in \mathbb{F}_q \setminus \{-1, 0, 1\}$ for $1 \leq i \leq k-1$. Then*

$$C_k(\alpha, v, \eta) = \{(v_1 f(\alpha_1, \dots, v_n f(\alpha_n)) \mid f(x) = \sum_{i=1}^{k-1} f_i x^i + \eta f_0 x^k \in \mathbb{F}_q[x]\}$$

is an LCD MDS code, where $\eta \in \mathbb{F}_q^* \backslash S_k$ and $\eta^2 \neq \frac{-1}{a}$.

Proof. From the discussion above, we obtain $R(D) = n$. Consequently, LCD MDS is obvious. ∎

Remark 5. *In particular, if $\eta \in S_k$ and $\eta^2 \neq \frac{-1}{a}$ in Theorem 4, then $C_k(\alpha, v, \eta)$ is an LCD NMDS code by Lemma 1.*

4. Conclusion and Future work

In this paper, we investigate MDS or NMDS LCD codes by TGRS codes. We give the check matrix of TGRS codes, which plays an important role in investigating dual codes of TGRS codes. By factorization of binomial, trinomial and linearized polynomial over $\mathbb{F}_q$, we choose α and v such that the matrix D is full rank. Consequently, we obtain three classes of MDS or NMDS LCD codes. It is possible to construct more classes MDS or NMDS LCD codes by different polynomials from TGRS codes.

A part from the problem mentioned above, there could be many other interesting problems associated with MDS codes. A possible direction for future work is to investigate self-dual MDS codes from TGRS codes (e.g., see [6]).

References

[1] P. Beelen, S. Puchinger, and J. Ronsenkilde ne Nielsen, "Twisted Reed-Solomon Codes," in IEEE ISIT, 2017, PP. 336-340.

[2] P.Beelen, M. Bossert, S.Puchinger, and J.Ronsenkilde, "Structural Properties of Twisted Reed-Solomon Codes with Applications to Cryptography," arXiv:1801.07003v2 [cs.IT] 11 May 2018.

[3] J. Bringer, C. Carlet, H. Chabanne, S. Guilley, and H. Maghrebi, "Orthogonal direct sum masking: A smartcard friendly computation paradigm in a code, with Builtin protection against side-channel and fault attacks," in Information Security Theory and Practice. Securing the Internet of Things (Lecture Notes in Computer Science), vol. 8501. New York, NY, USA: Springer, 2014, pp. 40-56.

[4] C. Carlet and S. Guilley, "Complementary dual codes for countermeasures to side-channel attacks," Adv. Math. Commun., vol. 10, no. 1, pp. 131-150, 2016.

[5] L. Jin, "Construction of MDS codes with complementary duals," IEEE Trans. Inf. Theory, vol. 63, no. 5, pp. 2843-2847, May 2017.

[6] L. Jin, and C. Xing, "New MDS self-dual codes from generalized Reed-Solomon codes," IEEE Trans. Inf. Theory, vol. 63, no. 3, pp. 1434-1438, Mar. 2017.

[7] B. Chen, and H. Liu, "New Constructions of MDS Codes With Complementary Duals," IEEE Trans. Inf. Theory, vol. 64, no. 8, pp. 5776-5782, Aug. 2018.

[8] J. Massey, "Linear codes with complementary duals," Discrete Math. vol. 106-107, pp. 337-342, Sep. 1992.

[9] X. Shi, Q. Yue, "New LCD MDS codes constructed from generalized Reed-Solomon codes," Journal of Algebra and Its Applications, doi: 10.1142/S0219498819501500, Aug. 2018.

[10] W. Huffman, V. Pless, "Fundamentals of Error Correcting Codes," Cambridge University Press, 2003.

[11] S. Liu, Y. Fan, H. Liu, "Galois LCD codes over finite fields," Finite Fields and Their Appl. 49: 227-242(2018).

[12] M. Shi, H. Zhu, L. Qian, L. Sok, P. Sole, "On slf-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q$", 10.1007/s12095-019-00363-92019

[13] H. Dinh, "Structure of repeated-root constacyclic codes of length 6ps and their duals," Contemp. Math., vol. 609, pp. 69-87, May 2014.

[14] S. Dougherty, J. Kim, B. Ozkaya, L. Sok, and P. Sol, "The combinatorics of LCD codes: Linear programming bound and orthogonal matrices," Int. J. Inf. Coding Theory, vol. 4, nos. 2-3, pp. 116-128, 2017.

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

[16] C. Gneri, B. Özkaya, and P. Sol, "Quasi-cyclic complementary dual codes," Finite Fields Appl., vol. 42, pp. 67-80, Nov. 2016.

[17] C. Carlet, S. Mesnager, C. Tang, and Y. Qi: Euclidean and Hermitian LCD MDS Codes, arXiv preprint arXiv:1702.08033, 2017.

[18] X. Hou and F. Oggier, "On LCD codes and lattices," in Proc. IEEE Int. Symp. Inf. Theory, Jul. 2016, pp. 1501-1505.

[19] C. Li, C. Ding, and S. Li, "LCD cyclic codes over finite fields," IEEE Trans. Inf. Theory, vol. 63, no. 7, pp. 4344-4356, Jul. 2017, doi: 10.1109/TIT.2017.2672961.

[20] X. Yang and J. Massey: The necessary and sufficient condition for a cyclic code to have a complementary dual, Discrete Math., vol. 126, pp. 391-393, 1994.

[21] S. Dodunkov, I. Landjev, "On near-MDS codes," J. Geometry, vol. 54, nos. 1-2, pp. 30-43, 1994.

[22] D. E. Simos and Z. Varbanov. MDS codes, NMDS Codes and Their Secret-Sharing Schems. Accessed: Apr. 2018. [Online].

[23] Y. Zhou, F. Wang, Y. Xin, S. Luo, S. Qing and Y. Yang, "A Secret sharing scheme based on near-MDS codes," in Proc. IC-NIDC, 2009, pp. 833-836.

College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, 211100, P. R. China

E-mail address: dthuang666@163.com

Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, 211100, P. R. China

E-mail address: yueqin@nuaa.edu.cn

College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, 211100, P. R. China

E-mail address: niuajm@163.com