Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 6(12): 14044–14053.
DOI:10.3934/math.2021812
Received: 14 September 2021
Accepted: 18 October 2021
Published: 19 October 2021

Research article

Further results on LCD generalized Gabidulin codes

Xubo Zhao*, **Xiaoping Li**, **Tongjiang Yan and Yuhua Sun**

College of Sciences, China University of Petroleum, Qingdao 266580, China

* **Correspondence:** Email: zhaoxubo@upc.edu.cn; Tel: +86 13305422493.

Abstract: Linear complementary dual (abbreviated LCD) generalized Gabidulin codes (including Gabidulin codes) have been recently investigated by Shi and Liu et al. (Shi et al. IEICE Trans. Fundamentals E101-A(9):1599-1602, 2018, Liu et al. Journal of Applied Mathematics and Computing 61(1): 281-295, 2019). They have constructed LCD generalized Gabidulin codes of length n over $\mathbb{F}_{q^n}$ by using self-dual bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ when q is even or both q and n are odd. Whereas for the case of odd q and even n, whether LCD generalized Gabidulin codes of length n over $\mathbb{F}_{q^n}$ exist or not is still open. In this paper, it is shown that one can always construct LCD generalized Gabidulin codes of length n over $\mathbb{F}_{q^n}$ for the case of odd q and even n.

Keywords: generalized Gabidulin codes; LCD codes; MRD codes; rank metric
Mathematics Subject Classification: 94B05

1. Introduction

Rank metric was defined as “arithmetic distance” by Loo-Keng Hua [10]. In 1978, this metric was firstly studied in coding theory [6], it measured the distance between two codewords, represented as matrices over a finite field [6] or vectors with entries in an extension field [8], as the rank of their differences. Rank metric codes have drawn much attention [2, 4, 5, 9, 16, 21, 23, 26] because of their important applications related to network coding [28], public-key cryptosystems [22], space-time coding [18], wireless communications [29], storage equipments [24].

Rank metric codes that achieve the Singleton-type bound are called maximum rank distance (MRD) codes, which are presented in analogy to MDS codes in the Hamming metric. Recently, several results on subclasses of MRD codes have been investigated [8, 9, 13, 20, 25], in which Gabidulin codes [8] and generalized Gabidulin codes [13] are of much interest for their efficient encoding and decoding algorithms. On the other hand, Euclidean linear complementary dual codes (that is, linear codes which intersect with their Euclidean dual codes trivially), abbreviated by LCD codes, have been extensively investigated due to their theoretical and practical applications [3, 15, 19, 30, 31]. Devi in [7] found that not all MRD codes over an extension field with an even character are LCD codes. Liu et al. pointed out the relationship between LCD Delsarte codes and LCD Gabidulin codes in [17]. Kandasamy et al. in [12] have shown that Gabidulin codes of length n over $\mathbb{F}_{2^n}$ generated by the trace-orthogonal generator matrix are LCD codes. Later, Shi and Liu et al. [17, 27] generalized the result of [12], by using a self-dual basis, they discussed the construction of LCD generalized Gabidulin codes over $\mathbb{F}_{q^n}$ when q is even or both q and n are odd. However, for the case of odd q and even n, it is unknown whether LCD generalized Gabidulin codes of length n exist over $\mathbb{F}_{q^n}$.

Therefore, in this paper we devote to dealing with this open problem, and show that one can always construct LCD generalized Gabidulin codes of length n over $\mathbb{F}_{q^n}$ for the case of odd q and even n. The main technique is based on constructing a special basis of the extension field $\mathbb{F}_{q^n}$, such that the associated matrix of the basis over the extension field $\mathbb{F}_{q^n}$ satisfies the desired condition. First of all, a special basis of the extension field $\mathbb{F}_{q^n}$ is constructed from a self-dual basis of field $\mathbb{F}_{q^m}$, which ensures that the product of the associated matrix of the special basis and its transpose matrix is a nonsingular diagonal matrix, where $n = 2m$ and m is any odd integer. Then, the construction is generalized to a more general case of $n = 2^t \cdot m$, where $t \geq 2$ is a positive integer, and m is any odd integer. As a consequence, in the case of odd q and even n, LCD generalized Gabidulin codes over $\mathbb{F}_{q^n}$ can be constructed by using an appropriated basis of $\mathbb{F}_{q^n}$.

The rest of this paper is organized as follows. In Section 2, basic definitions and properties about finite fields, Euclidean LCD codes, and rank metric codes are reviewed. In Section 3, some results about construction of LCD generalized Gabidulin codes are provided. The conclusion of this paper is given in Section 4.

2. Preliminaries

Denote $\mathbb{F}_q$ be a base field and $\mathbb{F}_{q^N}$ be an extension field of degree N of $\mathbb{F}_q$, where q is a prime power and N is a positive integer. Let $g_1, g_2, \ldots, g_n \in \mathbb{F}_{q^N}$, where n is a positive integer, and $n \leq N$. Denote $\mathbf{g} = \{g_1, g_2, \ldots, g_n\}$ be some fixed *linearly independent set* (abbreviated LIS) of the extension field $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$, i.e., coordinates $g_i \in \mathbb{F}_{q^N}$, $i = 1, 2, \ldots, n$, are linearly independent over the base field $\mathbb{F}_q$. If $g_1, g_2, \ldots, g_N \in \mathbb{F}_{q^N}$ are linearly independent over $\mathbb{F}_q$, then the LIS $\mathbf{g} = \{g_1, g_2, \ldots, g_N\}$ is called a *basis* of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$. Throughout this paper, we write $g^{[i]} = g^{q^i}$ for an element $g \in \mathbb{F}_{q^N}$, and $A^{[i]} = (a_{ij})^{[i]} = (a_{ij}^{[i]}) = (a_{ij}^{q^i})$ for a matrix $A = (a_{ij})$ over $\mathbb{F}_{q^N}$, where i is a nonnegative integer.

For $g \in \mathbb{F}_{q^N}$, the *trace* of g over $\mathbb{F}_q$ is defined as

$$Tr_{\mathbb{F}_{q^N}/\mathbb{F}_q}(g) = \sum_{i=0}^{N-1} g^{[i]}.$$

Two bases $\mathbf{g} = \{g_1, g_2, \ldots, g_N\}$ and $\mathbf{h} = \{h_1, h_2, \ldots, h_N\}$ of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$ are said to be *dual bases*, if $Tr_{\mathbb{F}_{q^N}/\mathbb{F}_q}(g_i h_j) = \delta_{i,j}$, for all $1 \leq i, j \leq N$, where $\delta_{i,j}$ is Kroneker delta function. If $Tr_{\mathbb{F}_{q^N}/\mathbb{F}_q}(g_i g_j) = \delta_{i,j}$, for all $1 \leq i, j \leq N$, the basis $\{g_1, g_2, \ldots, g_N\}$ is called a *self-dual basis*.

The criterion for the existence of self-dual bases of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$ is given by Lemma 2.1.

Lemma 2.1. *[11] $\mathbb{F}_{q^N}$ has a self-dual basis over $\mathbb{F}_q$ if and only if either q is even or both q and N are odd.*

In [8], the linear rank metric was considered as a metric for linear block codes over extension fields. In this sense, *a linear rank metric code* C of length n with dimension k over $\mathbb{F}_{q^N}$ is a k-dimensional subspace of $\mathbb{F}_{q^N}^n$. And the *Euclidean dual code* of C is denoted by

$$C^{\perp} = \{\mathbf{u} \in \mathbb{F}_{q^N}^n \mid \langle \mathbf{u}, \mathbf{v} \rangle = 0, \forall \mathbf{v} \in C\},$$

where vectors $\mathbf{u} = (u_1, u_2, \dots, u_n)$ and $\mathbf{v} = (v_1, v_2, \dots, v_n)$ belong to $\mathbb{F}_{q^N}^n$, $\langle \mathbf{u}, \mathbf{v} \rangle$ is defined as $\langle \mathbf{u}, \mathbf{v} \rangle = \sum\limits_{i=1}^{n} u_i v_i$. If $C^{\perp} \bigcap C = \{\mathbf{0}\}$, C is called *a Euclidean LCD* (or for short, LCD) *code*. The following proposition gives a complete characterization of LCD codes.

Proposition 2.2. *[3] If G is a generator matrix for the $[n, k]$ linear block code $C \subseteq \mathbb{F}_{q^N}^n$, then C is an LCD code of length n if and only if the $k \times k$ matrix $GG^{\top}$ is nonsingular, where $G^{\top}$ is the transpose of the matrix G.*

Definition 2.3. *The rank of a vector $\boldsymbol{u} = (u_1, u_2, \dots, u_n) \in \mathbb{F}_{q^N}^n$, denoted by $Rk(\boldsymbol{u})$, is defined as the maximal number of linearly independent coordinates u_i over $\mathbb{F}_q$, namely,*

$$Rk(\boldsymbol{u}) = dim_{\mathbb{F}_q} \langle u_1, u_2, \dots, u_n \rangle,$$

where $\langle u_1, u_2, \dots, u_n \rangle$ represents the vector space generated by $u_1, u_2, \dots, u_n$. The rank distance between vectors $\boldsymbol{u}, \boldsymbol{v}$ of $\mathbb{F}_{q^N}^n$, is defined as

$$d_R(\boldsymbol{u}, \boldsymbol{v}) = Rk(\boldsymbol{u} - \boldsymbol{v}).$$

The minimum rank distance of a linear rank metric code C, denoted by $d_R(C)$, is the minimum rank distance over all nonzero codewords, namely,

$$d_R(C) = min\{Rk(\boldsymbol{u}) \mid \boldsymbol{u} \in C, \text{ and } \boldsymbol{u} \neq \boldsymbol{0}\}.$$

The well-known Singleton bound for block codes in the Hamming metric also implies an upper bound for block codes in the rank metric.

Theorem 2.4. *[8] Let $C \subseteq \mathbb{F}_{q^N}^n$ be a linear rank metric code of dimension k, then $d_R(C) \leq n - k + 1$.*

Definition 2.5. *A linear rank metric code $C \subseteq \mathbb{F}_{q^N}^n$ of dimension k is called a maximum rank distance (MRD) code, if $d_R(C) = n - k + 1$.*

Let s be a positive integer. For some ordered set $\mathbf{g} = \{g_1, g_2, \dots, g_n\}$ of n elements $g_i \in \mathbb{F}_{q^N}$ $(n \leq N)$, $i = 1, 2, \dots, n$, let $M_{s,k,\mathbf{g}}$ be the $k \times n$ *associated matrix* of $\mathbf{g}$, defined by

$$M_{s,k,\mathbf{g}} = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[s]} & g_2^{[s]} & \cdots & g_n^{[s]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[(k-1)s]} & g_2^{[(k-1)s]} & \cdots & g_n^{[(k-1)s]} \end{pmatrix}. \tag{2.1}$$

Keeping the above notation, a generalized Gabidulin code is defined as follows.

Definition 2.6. *[13] Let s be a positive integer such that $gcd(s, N) = 1$. A generalized Gabidulin code of dimension k relative to the set $\boldsymbol{g}$ is the code $\mathcal{G}_{s,k,\boldsymbol{g}}$ of length n over $\mathbb{F}_{q^N}$ generated by the associated matrix $M_{s,k,\boldsymbol{g}}$, where $1 \leq k \leq n$, $\boldsymbol{g} = \{g_1, g_2, \dots, g_n\}$ $(n \leq N)$ is an LIS of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$. In particular, if $s = 1$, $\mathcal{G}_{s,k,\boldsymbol{g}}$ is called a Gabidulin code.*

As discussed in [17, 27], below we study LCD generalized Gabidulin codes of length n over $\mathbb{F}_{q^N}$, with the assumption of $N = n$.

3. Construction of LCD generalized Gabidulin codes

In this section, in the case of odd q and even n, LCD generalized Gabidulin codes of length n over $\mathbb{F}_{q^n}$ are constructed. Firstly, we give the description of LCD generalized Gabidulin codes.

Definition 3.1. *Let $\mathcal{G}_{s,k,\mathbf{g}}$ be an k-dimensional generalized Gabidulin code over $\mathbb{F}_{q^n}$, generated by the matrix $M_{s,k,\mathbf{g}}$, where $1 \leq k \leq n$, $gcd(s,n) = 1$, and $\mathbf{g} = \{g_1, g_2, \ldots, g_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. If the intersection of $\mathcal{G}_{s,k,\mathbf{g}}$ and its dual $\mathcal{G}^{\perp}_{s,k,\mathbf{g}}$ is trivial, namely, $\mathcal{G}_{s,k,\mathbf{g}} \cap \mathcal{G}^{\perp}_{s,k,\mathbf{g}} = \{\mathbf{0}\}$, then $\mathcal{G}_{s,k,\mathbf{g}}$ is called an LCD generalized Gabidulin code of length n over $\mathbb{F}_{q^n}$.*

Let the notations be the same as before, the following Theorems 3.2-3.3 on generalized Gabidulin codes can be found in [13].

Theorem 3.2. *Let $\mathcal{G}_{s,k,\mathbf{g}}$ be an k-dimensional generalized Gabidulin code of length n over $\mathbb{F}_{q^n}$, generated by the matrix $M_{s,k,\mathbf{g}}$, where $gcd(s,n) = 1$, and $\mathbf{g} = \{g_1, g_2, \ldots, g_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, $d_R(\mathcal{G}_{s,k,\mathbf{g}}) = n - k + 1$. Thus, generalized Gabidulin codes are MRD codes.*

Theorem 3.3. *Let $\mathcal{G}_{s,k,\mathbf{g}}$ be an k-dimensional generalized Gabidulin code of length n over $\mathbb{F}_{q^n}$, generated by the matrix $M_{s,k,\mathbf{g}}$, where $gcd(s,n) = 1$, and $\mathbf{g} = \{g_1, g_2, \ldots, g_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, the dual $\mathcal{G}^{\perp}_{s,k,\mathbf{g}}$ of $\mathcal{G}_{s,k,\mathbf{g}}$ is also a generalized Gabidulin code of dimension $n - k$.*

It is known [17, 27] that in the case of q is even or both of q and n are odd, an LCD generalized Gabidulin code over $\mathbb{F}_{q^n}$ can be constructed by employing a self-dual basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ as follows.

Theorem 3.4. *Assume that q is even or both of q and n are odd. Let $\mathbf{g} = \{g_1, g_2, \ldots, g_n\}$ be a self-dual basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, $M_{s,n,\mathbf{g}}M^{\top}_{s,n,\mathbf{g}} = I_n$, where $M_{s,n,\mathbf{g}}$ is the associated matrix of basis $\mathbf{g}$, and s is a positive integer such that $gcd(s,n) = 1$. Furthermore, let $\mathcal{G}_{s,k,\mathbf{g}}$ be a generalized Gabidulin code of length n over $\mathbb{F}_{q^n}$ with $M_{s,k,\mathbf{g}}$ as its generator matrix, then $\mathcal{G}_{s,k,\mathbf{g}}$ is an LCD MRD code, with parameters $[n, k, n - k + 1]$.*

For the associated matrix $M_{1,n,\mathbf{g}}$ of some ordered set $\mathbf{g} = \{g_1, g_2, \ldots, g_n\}$ over $\mathbb{F}_{q^n}$, we have the following result (see Lemma 3.51 in [14]).

Lemma 3.5. *Let $g_1, g_2, \ldots, g_n$ be elements of $\mathbb{F}_{q^n}$. Then the $n \times n$ associated matrix $M_{1,n,\mathbf{g}}$ of $\mathbf{g} = \{g_1, g_2, \ldots, g_n\}$ is nonsingular if and only if $\mathbf{g} = \{g_1, g_2, \ldots, g_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where*

$$M_{1,n,\mathbf{g}} = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[(n-1)]} & g_2^{[(n-1)]} & \cdots & g_n^{[(n-1)]} \end{pmatrix}.$$

A generalization variation of the above lemma is as follows.

Lemma 3.6. *Let $g_1, g_2, \ldots, g_n$ be elements of $\mathbb{F}_{q^n}$, and s be a positive integer such that $gcd(s,n) = 1$. Then the $n \times n$ associated matrix $M_{s,n,\mathbf{g}}$ of $\mathbf{g} = \{g_1, g_2, \ldots, g_n\}$ is nonsingular if and only if $\mathbf{g} = \{g_1, g_2, \ldots, g_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

Proof. In terms of (2.1), we have

$$M_{s,n,\mathbf{g}} = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[s]} & g_2^{[s]} & \cdots & g_n^{[s]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[(n-1)s]} & g_2^{[(n-1)s]} & \cdots & g_n^{[(n-1)s]} \end{pmatrix}.$$

Note that the matrix $M_{s,n,\mathbf{g}}$ is a row permutation of the matrix $M_{1,n,\mathbf{g}}$, since $\gcd(s, n) = 1$, and for index $[js]$, $js \bmod n$, $j = 0, 1, \ldots, n-1$, overrun all values from 0 to $n-1$. Therefore, the desired result follows by Lemma 3.5. □

The following two theorems are important for the construction of LCD generalized Gabidulin codes in the case of odd q and even n.

Theorem 3.7. *Let q, m be odd integers, $n = 2m$, and s be a positive integer such that $\gcd(s, n) = 1$. Denote $\boldsymbol{g} = \{g_1, g_2, \ldots, g_m\}$ be a self-dual basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and $M_{s,n,\boldsymbol{h}}$ be the $n \times n$ associated matrix of $\boldsymbol{h} = \{g_1, g_2, \ldots, g_m, \theta g_1, \theta g_2, \ldots, \theta g_m\}$, where $\theta = \xi^{\frac{q^m-1}{2}}$, and ξ is a primitive element of $\mathbb{F}_{q^n}$. Then $\boldsymbol{h}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and $M_{s,n,\boldsymbol{h}} M_{s,n,\boldsymbol{h}}^{\top}$ is a nonsingular diagonal matrix.*

Proof. Notice that for the set $\mathbf{h}$, its associated matrix $M_{s,n,\mathbf{h}}$ is with the form of

$$\begin{aligned} M_{s,n,\mathbf{h}} &= \begin{pmatrix} M_{s,m,\mathbf{g}} & XM_{s,m,\mathbf{g}} \\ M_{s,m,\mathbf{g}}^{[ms]} & X^{[ms]} M_{s,m,\mathbf{g}}^{[ms]} \end{pmatrix} \\ &= \begin{pmatrix} M_{s,m,\mathbf{g}} & XM_{s,m,\mathbf{g}} \\ M_{s,m,\mathbf{g}} & X^{[ms]} M_{s,m,\mathbf{g}} \end{pmatrix}, \end{aligned}$$

where $M_{s,m,\mathbf{g}}$ is the associated matrix of $\mathbf{g}$, and X is the following $m \times m$ diagonal matrix

$$X = \begin{pmatrix} \theta & 0 & \cdots & 0 \\ 0 & \theta^{[s]} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \theta^{[(m-1)s]} \end{pmatrix}.$$

Hence,

$$\begin{aligned} M_{s,n,\mathbf{h}} M_{s,n,\mathbf{h}}^{\top} &= \begin{pmatrix} M_{s,m,\mathbf{g}} & XM_{s,m,\mathbf{g}} \\ M_{s,m,\mathbf{g}} & X^{[ms]} M_{s,m,\mathbf{g}} \end{pmatrix} \cdot \begin{pmatrix} M_{s,m,\mathbf{g}}^{\top} & M_{s,m,\mathbf{g}}^{\top} \\ M_{s,m,\mathbf{g}}^{\top} X^{\top} & M_{s,m,\mathbf{g}}^{\top} X^{[ms]\top} \end{pmatrix} \\ &= \begin{pmatrix} I_m + X^2 & I_m + X^{1+[ms]} \\ I_m + X^{1+[ms]} & I_n + X^{2[ms]} \end{pmatrix} \\ &= \begin{pmatrix} I_m + X^2 & \mathbf{0} \\ \mathbf{0} & I_m + X^{2[ms]} \end{pmatrix}, \end{aligned} \tag{3.1}$$

where I_m is the $m \times m$ identity matrix. Notice that both q and s are odd. Thus, the last equality of (3.1) follows from the fact that $\theta^{1+[ms]} = \xi^{\frac{q^m-1}{2} \cdot (q^{ms}+1)} = \xi^{\frac{q^n-1}{2} \cdot \frac{q^{ms}+1}{q^m+1}} = -1$, and $(\theta^{[js]})^{1+[ms]} = (\theta^{1+[ms]})^{[js]} = (-1)^{q^{js}} = -1$ for $j \in \{1, 2, \ldots, m-1\}$.

Furthermore, we notice that all the eigenvalues of matrix X^2 (resp. $X^{2[ms]}$) are $\theta^{2[js]}$ (resp. $\theta^{2[(m+j)s]}$), for $j \in \{1, 2, \ldots, m-1\}$. It is easy to check that for any $j \in \{0, 1, \ldots, m-1\}$, the order of $\theta^{2[js]}$

(resp. $\theta^{2[(m+j)s]}$), denoted by $\mathrm{ord}(\theta^{2[js]})$ (resp. $\mathrm{ord}(\theta^{2[(m+j)s]})$ is not equal to 2, which is the order of -1. In fact, for $j \in \{0, 1, \ldots, m-1\}$, one can derive that $\mathrm{ord}(\theta^{2[js]})$=$\mathrm{ord}(\xi^{(q^m-1)\cdot q^{js}})$=$\frac{q^n-1}{\gcd(q^n-1,(q^m-1)\cdot q^{js})}$ =$\frac{q^n-1}{\gcd(q^n-1,q^m-1)}$=$q^m+1$. Analogously, one can obtain that $\mathrm{ord}(\theta^{2[(m+j)s]})$=$q^m+1$, for $j \in \{0, 1, \ldots, m-1\}$. So -1 is not an eigenvalue of matrices X^2 and $X^{2[ms]}$. Therefore, we conclude that

$$M_{s,n,\mathbf{h}}M_{s,n,\mathbf{h}}^{\top} = \begin{pmatrix} I_m + X^2 & \mathbf{0} \\ \mathbf{0} & I_m + X^{2[ms]} \end{pmatrix},$$

which is a nonsingular diagonal matrix. And using Lemma 3.6, $\mathbf{h} = \{g_1, g_2, \ldots, g_m, \theta g_1, \theta g_2, \ldots, \theta g_m\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. □

The result of Theorem 3.7 can be generalized as follows.

Theorem 3.8. *Let s be a positive integer, q, m are odd integers, and $n = 2^t \cdot m$. Assume that gcd(s, n) =gcd$(s, 2^t \cdot m) = 1$, where $t \geq 1$ is a positive integer. Then, there exists a basis of $\mathbb{F}_{q^n} = \mathbb{F}_{q^{2^t \cdot m}}$ over $\mathbb{F}_q$, denoted by $\boldsymbol{h}$, such that $M_{s,n,\boldsymbol{h}}M_{s,n,\boldsymbol{h}}^{\top}$ is a nonsingular diagonal matrix, where $M_{s,n,\boldsymbol{h}}$ is the $n \times n$ associated matrix of basis $\boldsymbol{h}$.*

Proof. We prove this result by mathematical induction.

For $t = 1$, in terms of Theorem 3.7, the result follows.

Assume that the conclusion holds for the case of $t-1$, we will prove that it also holds for the case of t, where $t \geq 2$ is a positive integer. Let s be a positive integer such that $\gcd(s, n)$ =$\gcd(s, 2^t \cdot m) = 1$, which implies $\gcd(s, \frac{n}{2})$ =$\gcd(s, 2^{t-1} \cdot m) = 1$. By induction assumption, there exists a basis of $\mathbb{F}_{q^{\frac{n}{2}}} = \mathbb{F}_{q^{2^{t-1} \cdot m}}$ over $\mathbb{F}_q$, denoted by $\mathbf{g} = \{g_1, g_2, \ldots, g_{\frac{n}{2}}\}$, such that $M_{s,\frac{n}{2},\mathbf{g}}M_{s,\frac{n}{2},\mathbf{g}}^{\top} = D$ is a nonsingular diagonal matrix, where $M_{s,\frac{n}{2},\mathbf{g}}$ is the $\frac{n}{2} \times \frac{n}{2}$ associated matrix of basis $\mathbf{g}$. Let $\theta = \xi^{\frac{q^{\frac{n}{2}}-1}{2}}$, where ξ is a primitive element of $\mathbb{F}_{q^n}$. Denote $\mathbf{h} = \{\mathbf{g}, \theta\mathbf{g}\} = \{g_1, g_2, \ldots, g_{\frac{n}{2}}, \theta g_1, \theta g_2, \ldots, \theta g_{\frac{n}{2}}\}$. Then, the associated matrix $M_{s,n,\mathbf{h}}$ of $\mathbf{h}$ is with the form of

$$\begin{aligned} M_{s,n,\mathbf{h}} &= \begin{pmatrix} M_{s,\frac{n}{2},\mathbf{g}} & XM_{s,\frac{n}{2},\mathbf{g}} \\ M_{s,\frac{n}{2},\mathbf{g}}^{[\frac{ns}{2}]} & X^{[\frac{ns}{2}]}M_{s,\frac{n}{2},\mathbf{g}}^{[\frac{ns}{2}]} \end{pmatrix} \\ &= \begin{pmatrix} M_{s,\frac{n}{2},\mathbf{g}} & XM_{s,\frac{n}{2},\mathbf{g}} \\ M_{s,\frac{n}{2},\mathbf{g}} & X^{[\frac{ns}{2}]}M_{s,\frac{n}{2},\mathbf{g}} \end{pmatrix}, \end{aligned}$$

where $M_{s,\frac{n}{2},\mathbf{g}}$ is the $\frac{n}{2} \times \frac{n}{2}$ associated matrix of basis $\mathbf{g}$, and

$$X = \begin{pmatrix} \theta & 0 & \cdots & 0 \\ 0 & \theta^{[s]} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \theta^{[(\frac{n}{2}-1)s]} \end{pmatrix}.$$

Hence,

$$\begin{aligned} M_{s,n,\mathbf{h}}M_{s,n,\mathbf{h}}^{\top} &= \begin{pmatrix} M_{s,\frac{n}{2},\mathbf{g}} & XM_{s,\frac{n}{2},\mathbf{g}} \\ M_{s,\frac{n}{2},\mathbf{g}} & X^{[\frac{ns}{2}]}M_{s,\frac{n}{2},\mathbf{g}} \end{pmatrix} \cdot \begin{pmatrix} M_{s,\frac{n}{2},\mathbf{g}}^{\top} & M_{s,\frac{n}{2},\mathbf{g}}^{\top} \\ M_{s,\frac{n}{2},\mathbf{g}}^{\top}X^{\top} & M_{s,\frac{n}{2},\mathbf{g}}^{\top}X^{[\frac{ns}{2}]^{\top}} \end{pmatrix} \\ &= \begin{pmatrix} D(I_{\frac{n}{2}} + X^2) & D(I_{\frac{n}{2}} + X^{1+[\frac{ns}{2}]}) \\ D(I_{\frac{n}{2}} + X^{1+[\frac{ns}{2}]}) & D(I_{\frac{n}{2}} + X^{2[\frac{ns}{2}]}) \end{pmatrix} \\ &= \begin{pmatrix} D(I_{\frac{n}{2}} + X^2) & \mathbf{0} \\ \mathbf{0} & D(I_{\frac{n}{2}} + X^{2[\frac{ns}{2}]}) \end{pmatrix}. \end{aligned} \tag{3.2}$$

Notice that both q and s are odd. Thus, the last equality of (3.2) follows from the fact that $\theta^{1+[\frac{ns}{2}]} = \xi^{\frac{q^{\frac{n}{2}}-1}{2}\cdot(q^{\frac{ns}{2}}+1)}\ \xi^{\frac{q^n-1}{2}\cdot\frac{q^{\frac{ns}{2}}+1}{q^{\frac{n}{2}}+1}} = -1$, and $(\theta^{[js]})^{1+[\frac{ns}{2}]} = (\theta^{1+[\frac{ns}{2}]})^{[js]} = (-1)^{q^{js}} = -1$ for $j \in \{1, 2, \ldots, \frac{n}{2} - 1\}$.

Furthermore, we notice that all the eigenvalues of matrix X^2 (resp. $X^{2[\frac{ns}{2}]}$) are $\theta^{2[js]}$ (resp. $\theta^{2[(\frac{n}{2}+j)s]}$) for $j \in \{0, 1, \ldots, \frac{n}{2} - 1\}$. It is easy to check that for any $j \in \{0, 1, \ldots, \frac{n}{2} - 1\}$, the order of $\theta^{2[js]}$ (resp. $\theta^{2[(\frac{n}{2}+j)s]}$), denoted by $\mathrm{ord}(\theta^{2[js]})$ (resp. $\mathrm{ord}(\theta^{2[(\frac{n}{2}+j)s]})$ is not equal to 2, which is the order of -1. In fact, for $j \in \{0, 1, \ldots, \frac{n}{2} - 1\}$, one can derive that $\mathrm{ord}(\theta^{2[js]})=\mathrm{ord}(\xi^{(q^{\frac{n}{2}}-1)\cdot q^{js}})=\frac{q^n-1}{\gcd(q^n-1,(q^{\frac{n}{2}}-1)\cdot q^{js})}$ $=\frac{q^n-1}{\gcd(q^n-1,q^{\frac{n}{2}}-1)}=q^{\frac{n}{2}}+1$. Analogously, one can obtain that $\mathrm{ord}(\theta^{2[(\frac{n}{2}+j)s]})=q^{\frac{n}{2}}+1$, where $j \in \{0, 1, \ldots, \frac{n}{2}-1\}$. So -1 is not an eigenvalue of matrices X^2 and $X^{2[\frac{ns}{2}]}$. Therefore, we conclude that

$$M_{s,n,\mathbf{h}}M_{s,n,\mathbf{h}}^{\top} = \begin{pmatrix} D(I_{\frac{n}{2}} + X^2) & \mathbf{0} \\ \mathbf{0} & D(I_{\frac{n}{2}} + X^{2[\frac{ns}{2}]}) \end{pmatrix},$$

which is a nonsingular diagonal matrix. And using Lemma 3.6, $\mathbf{h} = \{g_1, g_2, \ldots, g_m, \theta g_1, \theta g_2, \ldots, \theta g_m\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. □

Now we are going to illustrate Theorem 3.8 by two explicit examples. For the sake of simplicity, we assume that $s = 1$ in the following examples.

Example 3.9. *Let $q = 3$, and $n = 4$. Assume that ω_1 is a primitive element of field $\mathbb{F}_{3^2}$, and ω is a primitive element of field $\mathbb{F}_{3^4}$. Denote $\theta_1 = \omega_1^{\frac{q-1}{2}} = \omega_1$, and $\theta = \omega^{\frac{q^2-1}{2}} = \omega^4$. Utilizing the computer algebra system Magma [1], we verify that $\{1, \theta_1\}$ is a basis of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$, $\boldsymbol{h} = \{1, \theta_1, \theta, \theta\theta_1\}$= $\{1, \omega^{10}, \omega^4, \omega^{14}\}$ is a basis of $\mathbb{F}_{3^4}$ over $\mathbb{F}_3$. Moreover, the associated matrix of basis $\boldsymbol{h}$ is*

$$M_{1,4,\boldsymbol{h}} = \begin{pmatrix} 1 & \omega^{10} & \omega^4 & \omega^{14} \\ 1 & \omega^{30} & \omega^{12} & \omega^{42} \\ 1 & \omega^{10} & \omega^{36} & \omega^{46} \\ 1 & \omega^{30} & \omega^{28} & \omega^{58} \end{pmatrix},$$

and

$$M_{1,4,\boldsymbol{h}}M_{1,4,\boldsymbol{h}}^{\top} = \begin{pmatrix} \omega^{19} & 0 & 0 & 0 \\ 0 & \omega^{57} & 0 & 0 \\ 0 & 0 & \omega^{11} & 0 \\ 0 & 0 & 0 & \omega^{33} \end{pmatrix}.$$

Example 3.10. *Let $q = 3$, and $n = 6$. Assume that ω_1 is a primitive element of field $\mathbb{F}_{3^3}$, and ω is a primitive element of field $\mathbb{F}_{3^6}$. Utilizing the computer algebra system Magma [1], we find a self-dual basis of $\mathbb{F}_{3^3}$ over $\mathbb{F}_3$, denoted by $\{\omega_1^4, \omega_1^{10}, \omega_1^{12}\}$. Let $\theta = \omega^{\frac{q^3-1}{2}}$, $\boldsymbol{h} = \{\omega_1^4, \omega_1^{10}, \omega_1^{12}, \theta\omega_1^4, \theta\omega_1^{10}, \theta\omega_1^{12}\}$ $= \{\omega^{112}, \omega^{280}, \omega^{336}, \omega^{125}, \omega^{293}, \omega^{349}\}$. Then, it is easy to verify that $\boldsymbol{h}$ is a basis of $\mathbb{F}_{3^6}$ over $\mathbb{F}_3$. Moreover, the associated matrix of basis $\boldsymbol{h}$ is*

$$M_{1,6,\boldsymbol{h}} = \begin{pmatrix} \omega^{112} & \omega^{280} & \omega^{336} & \omega^{125} & \omega^{293} & \omega^{349} \\ \omega^{336} & \omega^{112} & \omega^{280} & \omega^{375} & \omega^{151} & \omega^{319} \\ \omega^{280} & \omega^{336} & \omega^{112} & \omega^{397} & \omega^{453} & \omega^{229} \\ \omega^{112} & \omega^{280} & \omega^{336} & \omega^{463} & \omega^{631} & \omega^{687} \\ \omega^{336} & \omega^{112} & \omega^{280} & \omega^{661} & \omega^{437} & \omega^{605} \\ \omega^{280} & \omega^{336} & \omega^{112} & \omega^{527} & \omega^{583} & \omega^{359} \end{pmatrix},$$

and

$$M_{1,6,\boldsymbol{h}}M_{1,6,\boldsymbol{h}}^{\top}=\begin{pmatrix}\omega^{83}&0&0&0&0&0\\0&\omega^{249}&0&0&0&0\\0&0&\omega^{19}&0&0&0\\0&0&0&\omega^{57}&0&0\\0&0&0&0&\omega^{171}&0\\0&0&0&0&0&\omega^{513}\end{pmatrix}.$$

Based on the above results, one can construct LCD generalized Gabidulin codes over $\mathbb{F}_{q^n}$ in the case of q is odd and n is even.

Theorem 3.11. *Assume that q is odd and n is even. Let $\mathbf{g}=\{g_1,g_2,\ldots,g_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ satisfying $M_{s,n,\mathbf{g}}M_{s,n,\mathbf{g}}^{\top}$ is a nonsingular diagonal matrix, where $M_{s,n,\mathbf{g}}$ is the associated matrix of basis $\mathbf{g}$, and s is a positive integer such that $gcd(s,n)=1$. Let $\mathcal{G}_{s,k,\mathbf{g}}$ be a generalized Gabidulin code of length n over $\mathbb{F}_{q^n}$ with $M_{s,k,\mathbf{g}}$ as its generator matrix, then $\mathcal{G}_{s,k,\mathbf{g}}$ is an LCD MRD code, with parameters* $[n,k,n-k+1]$.

Proof. By Theorem 3.8, we know that there exists a basis $\mathbf{g}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that the associated matrix $M_{s,n,\mathbf{g}}$ of basis $\mathbf{g}$ satisfying $M_{s,n,\mathbf{g}}M_{s,n,\mathbf{g}}^{\top}$ is a nonsingular diagonal matrix. Denote the $n\times n$ nonsingular diagonal matrix by $M_{s,n,\mathbf{g}}M_{s,n,\mathbf{g}}^{\top}$=diag$(\lambda_1,\lambda_2,\ldots,\lambda_n)$, where $\lambda_i\in\mathbb{F}_{q^n}$, and $\lambda_i\neq 0$, $i=1,2,\ldots,n$, are diagonal entries.

Note that the $k\times n$ matrix $M_{s,k,\mathbf{g}}$ consists of the first k rows of the $n\times n$ matrix $M_{s,n,\mathbf{g}}$. Thus, $M_{s,k,\mathbf{g}}M_{s,k,\mathbf{g}}^{\top}$ consists of the first k rows and first k columns of matrix $M_{s,n,\mathbf{g}}M_{s,n,\mathbf{g}}^{\top}$ =diag$(\lambda_1,\lambda_2,\ldots,\lambda_n)$, which is equal to diag$(\lambda_1,\lambda_2,\ldots,\lambda_k)$. Therefore, $M_{s,k,\mathbf{g}}M_{s,k,\mathbf{g}}^{\top}$ is an $k\times k$ nonsingular diagonal matrix. Then the desired result readily follows by Proposition 2.2 and Theorem 3.2. □

Remark 3.12. *In terms of Theorems 3.2 and 3.3, the dual of the code $\mathcal{G}_{s,k,\mathbf{g}}$ in Theorem 3.11 is also an LCD generalized Gabidulin code with parameters* $[n,n-k,k+1]$.

4. Conclusions

In this paper, for the case of odd q and even n, LCD generalized Gabidulin codes of length n over $\mathbb{F}_{q^n}$ are constructed by using an appropriated basis of $\mathbb{F}_{q^n}$. This work complements results previously obtained for constructing LCD generalized Gabidulin codes of length n over $\mathbb{F}_{q^n}$ when q is even or both q and n are odd. Therefore, one can always construct LCD generalized Gabidulin codes of length n over $\mathbb{F}_{q^n}$ for any positive n and prime power q.

Acknowledgments

This work was supported in part by the Shandong Provincial Natural Science Foundation of China under Grant ZR2019MF070, in part by the National Natural Science Foundation of China under Grant 61902429 and Grant 11775306, in part by the Fundamental Research Funds for the Central Universities under Grant 20CX05012A and Grant 19CX02058A, and in part by the Major Scientific and Technological Projects of CNPC under Grant ZD2019-183-008.

Conflict of interest

The authors declare that they have no conflicts of interest.

References

1. W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: the user language, *J. Symb. Comput.*, **24** (1997), 235–265.
2. E. Byrne, A. Ravagnani, An Assmus-Mattson theorem for rank metric codes, *SIAM J. Discret. Math.*, **33** (2019), 1242–1260.
3. C. Carlet, S. Mesnager, C. Tang, Y. Qi, Euclidean and Hermitian LCD MDS codes, *Des. Codes Cryptogr.*, **86** (2018), 2605–2618.
4. J. De La Cruz, J. R. Evilla, F. Özbudak, Hermitian rank metric codes and duality, *IEEE Access*, **9** (2021), 38479–38487.
5. J. De La Cruz, E. Gorla, H. H. López, A. Ravagnani, Weight distribution of rank-metric codes, *Des. Codes Cryptogr.*, **86** (2018), 1–16.
6. P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, *J. Comb. Theory*, **25** (1978), 226–241.
7. M. Devi, *On the class of T-direct codes:constructions, properties and applications*, Ph.D. Dessertation, Department of Mathematics, Jaypee University of Information Technology, India, 2013.
8. E. M. Gabidulin, Theory of codes with maximum rank distance, *Probl. Inf. Trans.*, **21** (1985), 1–12.
9. M. Gadouleau, Z. Y. Yan, Properties of codes with the rank metric, *IEEE Global Telecommunications Conference*, San Francisco, 2006.
10. L. K. Hua, A theorem on matrices over a field and its application, *Acta Math. Sinica*, **1** (1951), 109–163.
11. D. Jungnickel, A. J. Menezes, S. A. Vanstone, On the number of self-dual bases of $GF(q^m)$ over $GF(q)$, *Proc. Am. Math. Soc.*, **109** (1990), 23–29.
12. W. V. Kandasamy, F. Smarandache, R. Sujatha, R. R. Duray, *Erasure Techniques in MRD Codes*, Infinite Study, Ohio: Zip Publishing, 2012.
13. A. Kshevelskiy, E. Gabidulin, The new construction of rank code, *Probl. Inf. Trans.*, **1** (2005), 2105–2108.
14. R. Lidl, H. Niederreiter, P. M. Cohn, *Finite Fields*, Cambridge: Cambridge University Press, 2003.
15. X. Liu, Y. Fan, H. Liu, Galois LCD codes over finite fields, *Finite Fields Appl.*, **49** (2018), 227–242.
16. X. Liu, H. Liu, Rank-metric complementary dual codes, *J. Appl. Math. Comput.*, **61** (2019), 281–295.
17. Z. Liu, J. Wang, Further results on Euclidean and Hermitian linear complementary dual code, *Finite Fields Appl.*, **59** (2019), 104–133.

18. P. Lusina, E. M. Gabidulin, M. Bossert, Maximum rank distance codes as space-time codes, *IEEE T. Inform. Theory*, **49** (2003), 2757–2760.

19. J. L. Massey, Linear codes with complementary duals, *Discret. Math.*, **106-107** (1992), 337–342.

20. K. Otal, F. Özbudak, Explicit constructions of some non-Gabidulin linear maximum rank distance codes, *Adv. Math. Commun.*, **3** (2016), 589–600.

21. K. Otal, F. Özbudak, Constructions of cyclic subspace codes and maximum rank distance codes, *Network Coding and Subspace Designs. Signals and Communication Technology,* 2018. Available from: `https://doi.org/10.1007/978-3-319-70293-3_3`.

22. A. V. Ourivski, E. M. Gabidulin, Column scramber for the GPT cryptosystems, *Discret. Appl. Math.*, **128** (2003), 207–221.

23. A. Ravagnani, Rank-metric codes and their duality theory, *Des. Codes Cryptogr.*, **80** (2016), 1–20.

24. R. M. Roth, Maximum-rank array codes and their application to crisscross error correction, *IEEE T. Inform. Theory*, **37** (1991), 328–336.

25. J. Sheekey, A new family of linear maximum rank distance codes, *Adv. Math. Commun.*, **10** (2016), 475–488.

26. J. Sheekey, MRD codes: constructions and connections, 2019. Available from: arXiv:1904.05813.

27. M. Shi, D. Huang, On LCD MRD codes, *IEICE Trans. Fundamentals*, **E101-A** (2018), 1599–1602.

28. D. Silva, F. R. Kschischang, R. Köetter, A rank-metric approach to error control in random network coding, *IEEE T. Inform. Theory*, **54** (2008), 3951–3967.

29. V. Tarokn, N. Seshadri, A. R. Calderbank, Space-time codes for high data rate wireless communication: Performance criterion and code construction, *IEEE T. Inform. Theory*, **50** (1998), 19–32.

30. Y. Wu, Y. Lee, Binary LCD codes and self-orthogonal codes via simplicial complexes, *IEEE Commun. Lett.*, **24** (2020), 1159–1162.

31. Y. Wu, J. Y. Hyun, Y. Lee, New LCD MDS codes of non-Reed-Solomon type, *IEEE T. Inform. Theory*, **67** (2021), 5069–5078.

AIMS Press