GENERALIZED TWISTED GABIDULIN CODES

GUGLIELMO LUNARDON, ROCCO TROMBETTI, AND YUE ZHOU

Abstract. Based on the twisted Gabidulin codes obtained recently by Sheekey, we construct a new family of maximal rank distance codes as a set of \( q \)-polynomials over \( \mathbb{F}_{q^n} \), which includes the generalized Gabidulin codes and the twisted Gabidulin codes. Their Delsarte duals and adjoint codes are investigated. We also obtain necessary and sufficient conditions for the equivalence between two members of our new family of MRD codes except for several special parameters.

1. Introduction

Let \( K \) be a field. Clearly, the set \( K^{m \times n} \) of \( m \times n \) matrices over \( K \) is a \( K \)-vector space. The rank metric distance on the \( K^{m \times n} \) is defined by \( d(A, B) = \text{rank}(A - B) \) for \( A, B \in K^{m \times n} \).

A subset \( C \subseteq K^{m \times n} \) is called a rank metric code. The minimum distance of \( C \) is

\[
d(C) = \min_{A,B \in C} \{ d(A, B) \}.
\]

When \( C \) is a \( K \)-linear subspace of \( K^{m \times n} \), we say that \( C \) is \( K \)-linear code and the dimension \( \text{dim}_K(C) \) is defined to be the dimension of \( C \) as a subspace over \( K \). In this paper, we restrict ourselves to the \( K = \mathbb{F}_q \) cases, where \( \mathbb{F}_q \) denotes a finite field of order \( q \).

Let \( C \subseteq \mathbb{F}_q^{m \times n} \). When \( d(C) = d \), it is well-known that

\[
\#C \leq q^{\max\{m,n\}(\min\{m,n\) - d + 1)}.
\]

which is the Singleton bound for the rank metric distance; see [6]. When the equality holds, we called \( C \) a maximal rank distance (MRD for short) code. MRD codes have various applications in communications and cryptography; for instance, see [8, 11]. More properties of MRD codes can be found in [6, 7, 9, 14, 15].

A trivial example \( C \) of MRD codes in \( \mathbb{F}_q^{m \times n} \) with \( d(C) = m \) (here \( m \leq n \)) can be obtained as follows: Take all elements in \( a \in \mathbb{F}_q^n \), write the linear maps \( x \mapsto ax \) as \( n \times n \) matrices \( M_a \) over \( \mathbb{F}_q \). Then we get an MRD code \( C = \{ LM_a : a \in \mathbb{F}_q^n \} \), where \( L \) is an \( m \times n \) matrix of rank \( m \). If we replace \( ax \) by \( a \circ x \) where \( \circ \) is the multiplication of a prequasifield of order \( q^n \), then still we can get an MRD code. This code is \( \mathbb{F}_q \)-linear if and only if the prequasifield is a presemifield which is isotopic to a semifield with kernel containing \( \mathbb{F}_q \); see [3].

In [6] and [7], Delsarte and Gabidulin independently construct the first family of \( \mathbb{F}_q \)-linear MRD codes of size \( q^{nk} \) over finite fields \( \mathbb{F}_q \) for every \( k \) and \( n \). This family is generalized by Kshevetskiy and Gabidulin in [12].

\[\text{Date: July 29, 2015.}\]
Definition 1.1. Let $n, k, s \in \mathbb{Z}^+$ such that $\gcd(n, s) = 1$ and $q$ a power of prime. Then the set

$$\mathcal{G}_{k,s} = \{a_0 x + a_1 x^q + \ldots a_{k-1} x^{q^{(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

is a $\mathbb{F}_q$-linear MRD code of size $q^{nk}$, which we call a generalized Gabidulin code.

Actually, generalized Gabidulin codes are defined in a different way. Under a given basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, it is well-known that each element $a$ of $\mathbb{F}_{q^n}$ can be written as a (column) vector $\mathbf{v}(a)$ in $\mathbb{F}^n_q$. Let $\alpha_1, \ldots, \alpha_m$ be a set of linear independent elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where $m \leq n$. Then

$$\{(\mathbf{v}(f(\alpha_1)), \ldots, \mathbf{v}(f(\alpha_m))^T : f \in \mathcal{G}_{k,s}\}$$

is the original generalized Gabidulin code consisting of $m \times n$ matrices. To get the minimum distance of this code, we only have to concentrate on the number of the roots of each $f \in \mathcal{G}_{k,s}$.

In $\mathcal{G}_{k,s}$, we see all its members are of the form $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$, where $a_i \in \mathbb{F}_{q^n}$. A polynomial of this form is called a linearized polynomial (also a $q$-polynomial because its exponents are all powers of $q$). They are equivalent to $\mathbb{F}_q$-linear transformations from $\mathbb{F}_{q^n}$ to itself. We refer to [13] for their basic properties.

In the rest of this paper, we restrict ourselves to the set of linearized polynomials which define MRD codes.

Very recently, Sheekey [16] made a breakthrough in the construction of new linear MRD codes using linearized polynomials.

Definition 1.2. Let $n, k, h \in \mathbb{Z}^+$ and $k < n$. Let $\eta$ be in $\mathbb{F}_{q^n}$ such that $N_{q^n/q}(\eta) \neq (-1)^{nk}$. Then the set

$$\mathcal{H}_{k}(\eta, h) = \{a_0 x + a_1 x^q + \ldots a_{k-1} x^{q^{k-1}} + \eta a^{h} x^k : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

is an $\mathbb{F}_q$-linear MRD code of size $q^{nk}$, which is called a twisted Gabidulin code.

Another recent progress is a family of nonlinear MRD codes in $\mathbb{F}_q^{3 \times 3}$ with minimum distance 1 constructed by Cossidente, Marino and Pavese in [4].

In this paper, we construct a new family of $\mathbb{F}_q$-linear MRD codes which contains the generalized Gabidulin codes and the twisted Gabidulin codes. The organization of this paper is as follows: In Section 2, we give a brief introduction of the Delsarte dual codes and the adjoint codes of MRD codes. In Section 3, we present our new family of MRD codes. Finally, we consider the equivalence between different members of our new family of MRD codes.

2. DUAL AND ADJOINT CODES OF MRD CODES

We define a symmetric bilinear form on the set of $m \times n$ matrices by

$$\langle M, N \rangle := \text{Tr}(M N^T),$$

where $N^T$ is the transpose of $N$. The Delsarte dual code of an $\mathbb{F}_q$-linear code $\mathcal{C}$ is

$$\mathcal{C}^\perp := \{M \in \mathbb{F}_q^{m \times n} : \langle M, N \rangle = 0, \forall N \in \mathcal{C}\}.$$

One important result proved by Delsarte [6] is that the dual code of an MRD code is still MRD. As we are considering MRD codes using linearized polynomials, we give the definition of dual code in the form of polynomials; see [16] too.
We define the bilinear form $b$ on $q$-polynomials by

$$b(f, g) = \text{Tr}_{q^n/q} \left( \sum_{i=0}^{n-1} f_i g_i \right),$$

where $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ and $g(x) = \sum_{i=0}^{n-1} b_i x^{q^i} \in \mathbb{F}_{q^n}[x]$. The Delsarte dual code $C^\perp$ of a set of $q$-polynomials $C$ is

$$C^\perp = \{ f : b(f, g) = 0, \forall g \in C \}.$$

Let $C$ be an MRD codes in $K^{m \times n}$. It is obvious that $\{ M^T : M \in C \}$ is also an MRD codes, because the ranks of $M^T$ and $M$ are the same. When $K = \mathbb{F}_q$ and $m = n$, we can also interpret the transposes of matrices into an operation on linearized polynomials.

Following the terminology in [10], we define the adjoint of a linearized polynomial $f = \sum_{i=0}^{n-1} a_i x^{q^i}$ by $\hat{f} := \sum_{i=0}^{n-1} a_i x^{q^{-i}}$. If $C$ is an MRD codes consisting of $q$-polynomials, then the adjoint code of $C$ is $\hat{C} := \{ \hat{f} : f \in C \}$. In fact, the adjoint of $f$ is equivalent to the transpose of the matrix derived from $f$. This result can be found in [19].

### 3. Generalized twisted Gabidulin codes

The following lemma plays a key role in our construction of new MRD codes.

**Lemma 3.1.** Let $q$ be a prime power, and $k, l, m$ and $n \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$ and $k \leq l$. Let $U$ be an $\mathbb{F}_{q^m}$-subspace of $\mathbb{F}_{q^m}^n$ and $\dim_{\mathbb{F}_q}(U) = k$. Then

$$\dim_{\mathbb{F}_q}(U \cap \mathbb{F}_{q^m}^l) \leq k.$$  

**Proof.** Assume that (1) is not true, i.e. there exists $u_0, u_1, \ldots, u_k$ are linear independent over $\mathbb{F}_q$. It implies that the $\mathbb{F}_q$-rank of the matrix

$$M = \begin{pmatrix}
    u_{0} & u_{1} & \ldots & u_{k} \\
    u_{0}^q & u_{1}^q & \ldots & u_{k}^q \\
    \ldots & \ldots & \ldots & \ldots \\
    u_{0}^{q^{m-1}} & u_{1}^{q^{m-1}} & \ldots & u_{k}^{q^{m-1}}
\end{pmatrix}$$

is $k + 1$. Hence there exists at least one $(k + 1) \times (k + 1)$ submatrix $N$ of $M$, such that $\det(N) \neq 0$. As $\dim_{\mathbb{F}_{q^m}}(U) = k$, the $\mathbb{F}_{q^m}$-rank of the matrix

$$M' = \begin{pmatrix}
    u_{0} & u_{1} & \ldots & u_{k} \\
    u_{0}^m & u_{1}^m & \ldots & u_{k}^m \\
    \ldots & \ldots & \ldots & \ldots \\
    u_{0}^{q^{m(n-1)}} & u_{1}^{q^{m(n-1)}} & \ldots & u_{k}^{q^{m(n-1)}}
\end{pmatrix}$$

is less than or equal to $k$. Hence the determinant of any $(k + 1) \times (k + 1)$ submatrix of $M'$ is zero.

However, as $\gcd(m, n) = 1$, after applying a row permutation on $M$, we get $M'$. It leads to a contradiction on the determinant of $N$. \qed

**Theorem 3.2.** Let $q$ be a prime power, and $m$ and $n \in \mathbb{Z}^+$ such that $\gcd(n, m) = 1$. Let $\mathcal{M}$ be an $\mathbb{F}_{q^m}$-linear MRD code as a set of $q^m$-polynomials over $\mathbb{F}_{q^m}$, and the size of $\mathcal{M}$ is $q^{mnk}$. Let $\tilde{\mathcal{M}}$ be the intersection of $\mathcal{M}$ and the set of $q$-polynomials over $\mathbb{F}_q$. Then $\tilde{\mathcal{M}}$ is an $\mathbb{F}_q$-linear MRD code if and only if $\# \tilde{\mathcal{M}} = q^{nk}$. 

Proof. Let $f$ be a nonzero element of $\widetilde{\mathcal{M}}$. That means $f$ is a $q^m$-linearized polynomial with no more than $q^m(k-1)$ roots. In other words, the kernel of $f$ is an $\mathbb{F}_{q^m}$-linear space of dimension $l$, where $l < k$. By Lemma 3.1, we know that the dimension of the kernel of $f$ in $\mathbb{F}_{q^n}$ is also less than or equal to $l$. Therefore $\widetilde{\mathcal{M}}$ is MRD if and only if it is of the size $q^{nk}$. □

Using Theorem 3.2, we can generalize the twisted Gabidulin codes.

**Theorem 4.3.** Let $n, k, s, h \in \mathbb{Z}^+$ satisfying $\gcd(n, s) = 1$ and $k < n$. Let $\eta$ be in $\mathbb{F}_{q^n}$ such that $N_{q^n/q^s}(\eta) \neq (-1)^{nk}$. Then the set

$$\mathcal{H}_{k,s}(\eta, h) = \{a_0 x + a_1 x^{q^s} + \cdots + a_{k-1} x^{q^{s(k-1)}} + \eta a_0^h x^{q^s} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

is an $\mathbb{F}_q$-linear MRD code of size $q^{nk}$. 

Proof. By Definition 1.2, we know that $\mathcal{H}_{k,s}(\eta, h) = \{a_0 x + a_1 x^{q^s} + \cdots + a_{k-1} x^{q^{s(k-1)}} + \eta a_0^h x^{q^s} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}$ is an MRD code of size $q^{nk}$. Clearly $\mathcal{H}_{k,s}(\eta, h) \leq \mathcal{H}(\eta, h)$ and $\# \mathcal{H}_{k,s}(\eta, h) = q^{nk}$. By Theorem 3.2 we complete the proof. □

We call the MRD codes constructed in Theorem 4.3 generalized twisted Gabidulin codes. When $s = 1$, $\mathcal{H}_{k,s}(\eta, h)$ is the twisted Gabidulin code $\mathcal{H}_{k}(\eta, h)$. When $\eta = 0$, $\mathcal{H}_{k,s}(\eta, h)$ is exactly the generalized Gabidulin code $\mathcal{G}_{k,s}$.

In particular, when $k = 1$, all elements in $\mathcal{H}_{1,s}(\eta, h)$ are

$$a_0 x + \eta a_0^h x^{q^s},$$

for $a_0 \in \mathbb{F}_{q^n}$. They actually define the multiplication of generalized twisted field, which is a presemifield found by Albert [1].

4. Equivalences of MRD codes

In the literature, there are different definitions of equivalence for rank metric codes; see [5, 14]. As we concentrate on MRD codes in the form of linearized polynomials, we use the following definition.

**Definition 4.1.** Let $\mathcal{C}$ and $\mathcal{C}'$ be two set of $q$-polynomials over $\mathbb{F}_{q^n}$. They are equivalent if there exists two permutation $q$-polynomials $L_1, L_2$ and $\rho \in \text{Aut}(\mathbb{F}_q)$ such that $\mathcal{C}' = \{L_1 \circ f' \circ L_2(x) : f \in \mathcal{C}\}$, where $(\sum a_i x^{q^i})^\rho := \sum a_i^\rho x^{q^i}$. The automorphism group of $\mathcal{C}$ consists of all $(L_1, L_2, \rho)$ fixing $\mathcal{C}$.

It is well-known and also not difficult to show directly that two MRD codes are equivalent if and only if their duals are equivalent.

Let us look at the dual code of $\mathcal{H}_{k,s}(\eta, h)$. It is readily to verify that

$$\mathcal{H}_{k,s}^\perp(\eta, h) = \left\{b_0 x - \frac{1}{\eta} b_0^h x^{q^s} + \sum_{i=k+1}^{n-1} b_i x^{q^i} : b_i \in \mathbb{F}_{q^n}\right\}.$$

By applying $x \mapsto x^{q^{n-k}}$ on it, we get

$$\left\{-\frac{1}{\eta^{q^{n-k}}} b_0^h x^{q^s} + \sum_{i=1}^{n-k-1} b_i a_i x^{q^i} + b_0^{(n-k)} x^{q^{(n-k)}}, b_0, a_i \in \mathbb{F}_{q^n}\right\}.$$

Multiplying them by some constant and by certain change of variables, we get the following result.
Proposition 4.2. The Delsarte dual code of $\mathcal{H}_{k,s}(\eta, h)$ is equivalent to the code $\mathcal{H}_{n-k,s}(-\eta^n, n-h)$.

Similarly, it is straightforward to prove the following result about the adjoint code of a generalized twisted Gabidulin code.

Proposition 4.3. The adjoint code of $\mathcal{H}_{k,s}(\eta, h)$ is equivalent to $\mathcal{H}_{k,s}(1/\eta, sk-h)$.

In [10], Sheekey proved that $G_{k,s}$ and $\mathcal{H}_{k,1}(\eta, h)$ are equivalent if and only if $k \in \{1, n-1\}$ and $h \in \{0, 1\}$. The equivalence between $\mathcal{H}_{k,1}(\eta, h)$ and $\mathcal{H}_{k,1}(\nu, j)$, and the automorphism groups of $G_{k,1}$ and $\mathcal{H}_{k,1}(\eta, h)$ are also completely determined.

The main results of this section consist of several Theorems. They all together before considering the equivalence between distinct members in the generalized twisted Gabidulin codes, we introduce some concepts and tools.

Let $C$ be a set of $q$-polynomial over $\mathbb{F}_{q^n}$. The universal support $S(C)$ of $C$ is defined to be the following subset of $\{0, 1, \ldots, n-1\}$.

$$S(C) := \{i : \text{there exists } f \in C \text{ such that the } q^i\text{-coefficient of } f \text{ is not zero}\}.$$ Assume that there exist $B$ such that

$$\left\{\sum_{i \in B} h_i(a)x^{q^i} : a \in \mathbb{F}_{q^n}\right\} \subseteq C,$$

in which all $h_i$ are permutations of $\mathbb{F}_{q^n}$. Then we call $B$ an independent support of $C$. For example, $\{0, 1\}$ and $\{1\}$ are both independent supports of $\{a_0x + (a_0^2 + a_1)x^q : a_0, a_1 \in \mathbb{F}_{q^n}\}$.

Let $A$ and $B$ be two subsets of $\{0, 1, \ldots, n-1\}$. We define another subset $A^B$ of $\{0, 1, \ldots, n-1\}$ by

$$A^B := \{k : \text{there exists a unique pair } (i, j) \in A \times B \text{ such that } k \equiv i + j \pmod{n}\}.$$ For instance, $\{1, 2\}^{\{0, 1\}} = \{1, 3\}$. In the rest of this section, all calculations of integers and indices are taken modulo $n$, because we are essentially considering the terms $x^{q^i}$ of polynomials in $\mathbb{F}_{q^n}[x]/(x^{q^n} - x)$.

Lemma 4.4. Let $C_1$ and $C_2$ be two set of $q$-polynomials. If $C_1$ and $C_2$ are equivalent, then there exists a subset $A$ of $\{0, 1, \ldots, n-1\}$ such that

$$A^B \subseteq S(C_2),$$

for every independent support $B$ of $C_1$.

Proof. As $C_1$ and $C_2$ are equivalent, there exist permutation $q$-polynomials $L_1$, $L_2$ and $\rho \in \text{Aut}(\mathbb{F}_q)$ such that $C_1 = \{L_1 \circ f^\rho \circ L_2(x) : f \in C_2\}$. We use $\tau$ to denote this maps from $C_1$ to $C_2$, i.e. $\tau(f(x)) := L_1 \circ f^\rho \circ L_2(x)$.

Let $A$ be the universal support of $\{\tau(ax) : a \in \mathbb{F}_{q^n}\}$ and $B$ an independent support of $C_1$. Then

$$A^B \subseteq S(\{\tau(\sum_{j \in B} h_j(a)x^{q^j}) : a \in \mathbb{F}_{q^n}\}) \subseteq S(C_2),$$

where all $h_j$ are permutations of $\mathbb{F}_{q^n}$. Here the first “$\subseteq$” comes from the fact that the coefficients of $q^{i+j}$, where $(i, j) \in A \times B$ and $i + j \in A^B$, are the image of a nonzero map on $\{h_j(a) : a \in \mathbb{F}_{q^n}\}$. \qed
Lemma 4.5. Let $L_1, L_2$ be two permutation $q$-polynomials over $\mathbb{F}_{q^n}$ and $\rho \in \text{Aut}(\mathbb{F}_q)$. If
\[
\{ax : a \in \mathbb{F}_{q^n}\} = \{L_1(a^\rho L_2(x)) : a \in \mathbb{F}_{q^n}\},
\]
then $L_1(x) = cx^r$ and $L_2(x) = dx^{q^r}$ for certain integer $r$ and $c, d \in \mathbb{F}_{q^n}$.

Proof. Let $L_1(x) = \sum_{i=0}^{n-1} c_i x^{q^i}$ and $L_2(x) = \sum_{i=0}^{n-1} d_i x^{q^i}$, where $c_i$ and $d_i \in \mathbb{F}_{q^n}$. Then
\[
L_1(a^\rho L_2(x)) = \sum_{j=0}^{n-1} c_j \left( \sum_{i=0}^{n-1} a^\rho d_i x^{q^i} \right)^{q^j} = \sum_{l=0}^{n-1} \left( \sum_{j=0}^{n-1} c_j (a^\rho d_{l-j})^{q^j} \right) x^{q^l}.
\]
It implies that, when $l \neq 0$, the coefficient of $x^{q^l}$ in $L_1(a^\rho L_2(x))$ always equals 0, i.e.
\[
\sum_{j=0}^{n-1} c_j d_{l-j}^q a^\rho = 0,
\]
for all $a \in \mathbb{F}_{q^n}$. That means $c_j d_{l-j} = 0$ for all $j$ and $l \neq 0$. Therefore, there exists a unique integer $r$ between 0 and $n-1$ such that $c_r$ and $d_{n-r}$ are nonzero and all the rest $c_i$ and $d_i$ are zero.

When $k = 1$, $\mathcal{H}_{k,s}(\eta, g)$ is exactly generalized twisted field and the equivalence between $\mathcal{H}_{1,s}(\eta, g)$ and $\mathcal{H}_{1,t}(\theta, h)$ is exactly the isomorphism between two generalized twisted fields. This problem is completely solved; see [2, 3]. For $k = n - 1$, we can convert the equivalence between $\mathcal{H}_{n-1,s}(\eta, g)$ and $\mathcal{H}_{n-1,t}(\theta, h)$ into the equivalence between their Delsarte duals.

Next result is a necessary condition for the inequivalence between different generalized twisted Gabidulin codes.

Theorem 4.6. Let $n, k, s, t, g, h, l \in \mathbb{Z}^+$ satisfying $\gcd(n,s) = \gcd(n,t) = 1$ and $s \equiv lt \pmod{n}$. Let $\eta$ and $\theta$ be in $\mathbb{F}_{q^n}$ satisfying $N_{q^{s}/q^r}(\eta) \neq (−1)^{nk}$ and $N_{q^{t}/q^r}(\theta) \neq (−1)^{nk}$.

(a) If $\eta = \theta = 0$, $1 < k < n - 1$ and $s \equiv \pm t \pmod{n}$, then $\mathcal{H}_{k,s}(\eta, g)$ and $\mathcal{H}_{k,t}(\theta, h)$ are not equivalent.

(b) If $\eta = 0$, $\theta \neq 0$, $2 < k < n - 2$ and $s \equiv \pm t \pmod{n}$, then $\mathcal{H}_{k,s}(\eta, g)$ and $\mathcal{H}_{k,t}(\theta, h)$ are not equivalent.

(c) If both $\eta$ and $\theta$ are nonzero, $4 < k < n - 4$ and $s \equiv \pm t \pmod{n}$, then $\mathcal{H}_{k,s}(\eta, g)$ and $\mathcal{H}_{k,t}(\theta, h)$ are not equivalent.

Proof. According to Proposition 4.2, the Delsarte dual of $\mathcal{H}_{n-k,s}(\eta, g)$ is equivalent to $\mathcal{H}_{k,s}(−\eta^{q^s}, n−g)$. As two MRD codes are equivalent if and only if their Delsarte duals are equivalent, we can assume that $k \leq \lfloor \frac{n}{2} \rfloor$.

Assume that $\mathcal{H}_{k,s}(\eta, g)$ and $\mathcal{H}_{k,t}(\theta, h)$ are equivalent. We use $\tau$ to denote the map from $\mathcal{H}_{k,s}(\eta, g)$ to $\mathcal{H}_{k,t}(\theta, h)$, i.e. there exist linearized permutation polynomials $L_1(x), L_2(x)$ and $\rho \in \text{Aut}(\mathbb{F}_q)$ such that $\tau(f(x)) := L_1 \circ f^\rho \circ L_2(x)$ for $f \in \mathcal{H}_{k,s}(\eta, g)$. As in the proof of Lemma 4.4, we let $A$ be the universal support of $\{\tau(ax) : a \in \mathbb{F}_{q^n}\}$.

(a) First we look at the $\eta = \theta = 0$ case, which means that $\mathcal{H}_{k,s}(\eta, g)$ and $\mathcal{H}_{k,t}(\theta, h)$ are both generalized Gabidulin codes.
In this case, we take
\[ T_s := \{ \{ is \} : i = 0, \ldots, k - 1 \}, \]
which is a set of independent supports of \( H_{k,s}(0, g) \) and
\[ S(H_{k,s}(0, h)) = \{ it : i = 0, \ldots, k - 1 \}. \]
If \( j \in A \), then \( j + is \in A^{(is)} \). Together with Lemma 4.4, we have
\[ \{ j + is : i = 0, \ldots, k - 1 \} = \bigcup_{B \in T_s} \{ j \}^B \subseteq \bigcup_{B \in T_s} A^B \subseteq S(H_{k,t}(\theta, h)). \]
Hence
\[ \{ j + is : i = 0, \ldots, k - 1 \} \subseteq \{ it : i = 0, \ldots, k - 1 \}. \]
Letting \( j \equiv ut \pmod{n} \) and plugging \( s \equiv lt \pmod{n} \) into the above equation, we have
\[ \{ u + il : i = 0, \ldots, k - 1 \} = \{ i : i = 0, \ldots, k - 1 \}. \]
According to our assumption, we know that \( 1 < l < n - 1 \). If \( l \leq \lfloor \frac{n}{2} \rfloor \), then we consider the sequence of integers \( u, u+l, u+2l, \ldots \). As both \( l \) and \( k \) are less than or equal to \( \lfloor \frac{n}{2} \rfloor \), \( l \geq 2 \) and \( u \in \{ 0, 1, \ldots, k - 1 \} \), there must exist an \( \alpha \in \{ 0, 1, \ldots, k - 1 \} \) such that \( u + \alpha l \geq k \) and \( u + (\alpha - 1)l \leq k - 1 \). It is a contradiction to (4).
If \( l \geq \lfloor \frac{n}{2} \rfloor \), then similarly we consider the sequence \( u + (k - 1)l, u + (k - 2)l, \ldots \). We can also find an integer \( \beta \in \{ 0, 1, \ldots, k - 1 \} \) such that \( u + (k - 1 - \beta)l < 0 \) and \( u + (k - \beta)l \geq 0 \), which is a contradiction to (4).

(b) Now we consider the case in which \( \eta = 0 \) and \( \theta \neq 0 \). We take
\[ T_s := \{ \{ is \} : i = 0, \ldots, k - 1 \}, \]
which consists of independent supports of \( H_{k,s}(0, g) \) and
\[ S(H_{k,s}(\theta, h)) = \{ it : i = 0, \ldots, k \}. \]
Similarly as in the proof of (a), if \( j \in A \), then we have (3) which implies that
\[ \{ j + is : i = 0, \ldots, k - 1 \} \subseteq \{ it : i = 0, \ldots, k \}. \]
Letting \( j \equiv ut \pmod{n} \) and plugging \( s \equiv lt \pmod{n} \) into the above equation, we have
\[ \{ u + il : i = 0, \ldots, k - 1 \} \subseteq \{ i : i = 0, \ldots, k \}. \]
As in the proof of (a), we first consider the \( 2 \leq l \leq \lfloor \frac{n}{2} \rfloor \) case. We look at the sequences of integers \( u, u + l, \ldots, u + (k - 1)l \). There must exist an \( \alpha \) such that \( u + \alpha l > k \) and \( u + (\alpha - 1)l \leq k \), otherwise \( u + (k - 1)l \leq k \) which means \( k \leq 2 \), \( l = 2 \) and \( u = 0 \). It contradicts our assumption that \( k > 2 \). Hence (5) does not hold.
For the \( \lfloor \frac{n}{2} \rfloor < l \leq n - 2 \) case, following the approach in the proof of (a), we can show that (5) is not satisfied.

(c) Finally, we consider the case in which both \( \eta \) and \( \theta \) are nonzero. We take
\[ T_s := \{ \{ is \} : i = 1, \ldots, k - 1 \}, \]
which consists of independent supports of \( H_{k,s}(\eta, g) \) and
\[ S(H_{k,s}(\theta, h)) = \{ it : i = 0, \ldots, k \}. \]
Similarly as in the proof of (a), if \( j \in A \), then we have
\[
\{ j + is : i = 1, \ldots, k - 1 \} = \bigcup_{B \in T_s} \{ j \}^B \subseteq \bigcup_{B \in T_s} A^B \subseteq S(H_{k,t}(\theta, h)).
\]
which implies that
\[
\{ j + is : i = 1, \ldots, k - 1 \} \subseteq \{ it : i = 0, \ldots, k \}.
\]
Letting \( j \equiv ut \pmod{n} \) and plugging \( s \equiv lt \pmod{n} \) into the above equation, we have
\[
\{ u + il : i = 1, \ldots, k - 1 \} \subseteq \{ i : i = 0, \ldots, k \}.
\]
As in the proof of \((a)\), we first consider the \( 2 \leq l \leq \lfloor n/2 \rfloor \) case. We look at the sequences of integers \( u + 1, u + 2l, \ldots, u + (k - 1)l \). Again, there must exist an \( \alpha \) such that \( u + \alpha l > k \) and \( u + (\alpha - 1)l \leq k \), otherwise \( u + (k - 1)l \leq k \) which implies two possible values of \( u \) and \( k \):
- \( u = 0 \) and \( k \leq \frac{1}{l} \leq 2 \);
- \( u = -l \) and \( k \leq \frac{2l}{l - 1} \leq 4 \).
Both of them contradict our assumption that \( k > 4 \). Thus \((7)\) is not satisfied.
For the \( \lfloor n/2 \rfloor < l \leq n - 2 \) case, following the approach in the proof of \((a)\) and looking at the sequence \( u + (k - 1)l, u + (k - 2)l, \ldots, u + 1 \), we can again show that \((7)\) does not hold.

For \( k = 2 \) or \( n - 2 \), we can prove the following result.

**Theorem 4.7.** Let \( n, k, s, t, g, h \in \mathbb{Z}^+ \) satisfying \( \gcd(n, s) = \gcd(n, t) = 1 \) and \( k = 2 \) or \( n - 2 \). Let \( \eta \) and \( \theta \) be in \( \mathbb{F}_{q^n} \) satisfying \( N_{q^n/q^t}(\eta) \neq (-1)^{nk} \) and \( N_{q^n/q^t}(\theta) \neq (-1)^{nk} \). Assume that \( s \neq \pm t \pmod{n} \). If
- at least one \( \eta \) and \( \theta \) is nonzero, or
- \( n \neq 5 \),
then \( H_{k,s}(\eta, g) \) and \( H_{k,t}(\theta, h) \) are not equivalent.

**Proof.** Assume that \( H_{k,s}(\eta, g) \) and \( H_{k,t}(\theta, h) \) are equivalent. We use \( \tau \) to denote the equivalence map from \( H_{k,s}(\eta, g) \) to \( H_{k,t}(\theta, h) \). As in Lemma 4.4, we let \( A \) be the universal support of \( \{ \tau(ax) : a \in \mathbb{F}_{q^n} \} \).

According to the assumption, now \( k = 2 \) or \( n - 2 \). By Proposition 4.2, the Delsarte dual of \( H_{n-2,s}(-\eta^{q^s}, n - g) \) is equivalent to \( H_{2,t}(-\eta^{q^s}, n - g) \). As two MRD codes are equivalent if and only if their Delsarte duals are equivalent, we only have to consider the case in which \( k = 2 \), i.e.
\[
H_{2,s}(\eta, g) = \{ a_0 x + a_1 x^{q^{2s}} + \eta q^s a_0 x^{q^{2s}} : a_0, a_1 \in \mathbb{F}_{q^n} \},
\]
\[
H_{2,t}(\theta, h) = \{ a_0 x + a_1 x^{q^{t}} + \theta q^s a_0 x^{q^{2t}} : a_0, a_1 \in \mathbb{F}_{q^n} \}.
\]

Depending on the value of \( \eta \) and \( \theta \), we divide the proof into three cases.

**Case 1.** If \( \eta = \theta = 0 \), then we take \( T := \{ \{0\}, \{s\} \} \) which consists of independent supports of \( H_{2,s}(0, g) \) and \( S(H_{2,t}(0, h)) = \{0, t\} \). It is not difficult to see that \((\mathbb{2})\) holds for every \( B \in T \) and \( S(H_{2,t}(0, h)) \) if and only if \( s = \pm t \). In fact, we can also get this result directly from Theorem 4.4 \((a)\).

**Case 2.** If \( \eta \) and \( \theta \) are both nonzero, the universal support of \( H_{2,t}(\theta, h) \) is \( S := \{0, t, 2t\} \) and we take \( T := \{0, 2s\}, \{s\} \) consisting of the independent supports of \( H_{2,s}(\eta, g) \).
Assume that \( s \not\equiv \pm t \pmod{n} \). We proceed to show the nonexistence of \( A \) satisfying \( A \subseteq \{s, t \pm s, 2t \pm s\} \) for every \( B \in \mathcal{T} \) and \( \mathcal{S} \).

First from \( A^{(s)} \in \mathcal{S} \), we see that \( A \subseteq \{-s, t - s, 2t - s\} \). If \( A = \{-s\} \), then
\[
A^{(0,2s)} = \{-s, s\},
\]
which cannot be a subset of \( \mathcal{S} = \{0, t, 2t\} \). Similarly we can show that \( A \not= \{t - s\} \) or \( \{2t - s\} \).

Assume that \( A = \{t - s, 2t - s\} \). Then
\[
A^{(0,2s)} = \begin{cases} 
\{t - s, t + s, 2t - s, 2t + s\}, & t \not\equiv \pm 2s \pmod{n}; \\
\{s, 2t + s\}, & t \equiv 2s, t \not\equiv -2s \pmod{n}; \\
\{t + s, 2t - s\}, & t \equiv -2s, t \not\equiv 2s \pmod{n}; \\
\emptyset, & t \equiv 2s \equiv -2s \pmod{n}.
\end{cases}
\]

In the first case, \( A^{(0,2s)} \) cannot belong to \( \mathcal{S} \). The second case is also not possible, because \( t \not\in \{s, 2t + s\} \). The third case cannot hold, because \( 2t \not\in \{t + s, 2t - s\} \).

The fourth case means \( 4s = n \), together the assumption that \( \gcd(n, s) = 1 \) we have \( n = 4, s = 1 \) and \( t = 2 \), which contradicts the assumption that \( \gcd(n, t) = 1 \).

Similarly, we can verify that \( A \) is neither \( A = \{-s, t - s\} \) nor \( A = \{-s, 2t - s\} \).

Finally, assume that \( A = \{-s, t - s, 2t - s\} \). Now we have
\[
A^{(0)} = \{-s, t - s, 2t - s\}, \\
A^{(2s)} = \{s, t + s, 2t + s\}.
\]

As \( t - s \) and \( t + s \) cannot be in \( \mathcal{S} = \{0, t, 2t\} \), if \( A^{(0,2s)} \subseteq \mathcal{S} \), then \( t \equiv 2s \) or \(-2s \) (mod \(n\)). If \( t \equiv 2s \), we have \( A^{(0,2s)} = \{-s, 5s\} \); if \( t \equiv -2s \), we have \( A^{(0,2s)} = \{s, -5s\} \). As they both should belong to \( \mathcal{S} = \{0, t, 2t\} \), we get \( n = 5 \) which has been excluded in our assumption.

**Case 3.** If \( \eta \not= 0 \) and \( \theta = 0 \), the universal support of \( \mathcal{H}_{2,t}(0, h) \) is \( \mathcal{S} := \{0, t\} \) and we take \( \mathcal{T} := \{\{0, 2s\}, \{s\}\} \) consisting of the independent supports of \( \mathcal{H}_{2,s}(\eta, g) \).

Again we assume that \( s \not\equiv \pm t \pmod{n} \) and show the nonexistence of \( A \) satisfying \( \mathcal{C} \) for every \( B \in \mathcal{T} \) and \( \mathcal{S} \).

First from \( A^{(s)} \in \mathcal{S} \), we see that \( A \subseteq \{-s, t - s\} \). If \( A = \{-s\} \), then \( A^{(0,2s)} = \{-s, \} \not\subseteq \{0, t\} = \mathcal{S} \). If \( A = \{t - s\} \), then \( A^{(0,2s)} = \{t - s, t + s\} \not\subseteq \{0, t\} = \mathcal{S} \).

If \( A = \{-s, t - s\} \), then from
\[
A^{(0)} = \{-s, t - s\}, \\
A^{(2s)} = \{s, t + s\},
\]
and \( A^{(0,2s)} \subseteq \{0, t\} \), we see that \( A^{(0,2s)} \) must be an empty set. It implies that \( t \equiv 2s \equiv -2s \pmod{n} \). Hence \( n = 4 \) and \( t = 2 \), which contradicts the assumption that \( \gcd(n, t) = 1 \).

**Remark 1.** From the proof of Theorem 4.7, we see that \( n \not= 5 \) is only required for the case in which both \( \theta \) and \( \eta \) are nonzero.

When \( s \equiv \pm t \pmod{n} \), we can get the necessary and sufficient conditions for the equivalence between \( \mathcal{H}_{k,s}(\eta, g) \) and \( \mathcal{H}_{k,t}(\theta, h) \).

**Theorem 4.8.** Let \( n, k, s, t, g, h \in \mathbb{Z}^+ \) satisfying \( \gcd(n, s) = \gcd(n, t) = 1 \) and \( 2 \leq s \leq k \leq n - 2 \). Let \( \eta \) and \( \theta \) be in \( \mathbb{F}_{q^n} \) satisfying \( N_{q^n/q^s}(\eta) \not= (-1)^{nk} \) and \( N_{q^n/q^s}(\theta) \not= (-1)^{nk} \).
(a) When \( s \equiv t \pmod{n} \), \( H_{k,s}(\eta, g) \) and \( H_{k,t}(\theta, h) \) are equivalent if and only if \( g = h \) and there exists \( c, d \in \mathbb{F}_{q^n}^* \), \( \rho \in \text{Aut}(\mathbb{F}_q) \) and integer \( r \) such that
\[
\theta c^q h^{q^{-1} d^{r+h-q^{k+r}}} = \eta^q \rho^q \theta c^q h^{q^{-1} d^{r+h-q^{k+r}}},
\]
(b) When \( s \equiv -t \pmod{n} \), \( H_{k,s}(\eta, g) \) and \( H_{k,t}(\theta, h) \) are equivalent if and only if \( g = -h \) and there exists \( c, d \in \mathbb{F}_{q^n}^* \), \( \rho \in \text{Aut}(\mathbb{F}_q) \) and integer \( r \) such that
\[
\theta c^q h^{q^{-1} d^{r+h-q^{k+r}}} = \eta^q \rho^q \theta c^q h^{q^{-1} d^{r+h-q^{k+r}}},
\]

Proof. We assume that \( H_{k,s}(\eta, g) \) and \( H_{k,t}(\theta, h) \) are equivalent. We use \( \tau \) to denote the equivalence map from \( H_{k,s}(\eta, g) \) to \( H_{k,t}(\theta, h) \). As in Lemma 4.4, let \( A \) be the universal support of \( \{\tau(ax) : a \in \mathbb{F}_{q^n}\} \).

(a) When \( s \equiv t \pmod{n} \), \( A \) must be equal to \( \{0\} \). The reasons are as follows:

i) When \( \eta = \theta = 0 \), \( H_{k,s}(\eta, g) \) and \( H_{k,t}(\theta, h) \) are both generalized Gabidulin code \( G_{k,s} \). Let \( T(G_{k,s}) := \{\{is : i = 0, \ldots, k - 1\} \mid \text{is a collection of independent support of } G_{k,s}\} \). The universal support of \( G_{k,s} \) is \( S = \{is : i = 0, \ldots, k - 1\} \). It is straightforward to see that if \( 2 \) holds for \( A \), all \( B \in T(G_{k,s}) \) and \( S \), then \( A \) must be \( \{0\} \).

ii) When \( \eta \neq 0 \), from \( A(s) \subseteq S(H_{k,t}(\theta, h)) \) we can derive that \( A \subseteq \{-s, 0\} \).

Now we know that \( A = \{0\} \), which means that \( \tau \) maps \( \{a_0 x : a_0 \in \mathbb{F}_{q^n}\} \) to itself.

By Lemma 4.5, we know that \( L_1 = cx^q \) and \( L_2 = dx^{q^{k-r}} \) for certain \( r \), \( c \) and \( d \). Thus the image of \( H_{k,s}(\eta, g) \) is
\[
\{ct_0^q r^q d^q x + a_1 x^{q^r} + \cdots + a_{k-1} x^{q^{r(k-1)}} + c\rho_0^q a_0^{q^r} d^q x^{q^{r+k}} : a_i \in \mathbb{F}_{q^n}\}.
\]

It is the same as \( H_{k,t}(\theta, h) \) if and only if
\[
\theta(c^q h^{q^{-1} d^{r+h-q^{k+r}}}) = \eta^q \rho^q c^q h^{q^{-1} d^{r+h-q^{k+r}}},
\]
for all \( a_0 \in \mathbb{F}_{q^n}^* \). That means \( h = g \) and
\[
\theta c^q h^{q^{-1} d^{r+h-q^{k+r}}} = \eta^q \rho^q c^q h^{q^{-1} d^{r+h-q^{k+r}}},
\]

(b) When \( s \equiv -t \pmod{n} \), we first apply \( x \mapsto x^{q^k} \) on \( H_{k,t}(\theta, h) \) to get
\[
\{a_0^{q^k} x^{q^k} + a_1^{q^k} x^{q^{r(k-1)}} + \cdots + \theta b_0 x^{q^{h+k}} : a_i \in \mathbb{F}_{q^n}\}.
\]

It equals
\[
\{a_0 x + a_1 x^q + \cdots + \theta b_0 x^{q^{h-k}} : a_i \in \mathbb{F}_{q^n}\}.
\]

Using the result for \( s \equiv t \pmod{n} \), we have \( h = -g \) and
\[
\{a_0 x + a_1 x^q + \cdots + \theta b_0 x^{q^{h-k}} : a_i \in \mathbb{F}_{q^n}\}.
\]

Remark 2. Combining Theorems 4.6, 4.7 and 4.8 we completely determine the equivalence of different members of the generalized twisted Gabidulin codes except for the case in which both \( \eta \) and \( \theta \) are nonzero, and the parameters satisfy one of the following conditions:
It is worth noting that the first condition is a special case of the second one.

**Remark 3.** Theorems 4.8 (a) can also be directly used to completely determine the automorphism group of $\mathcal{H}_{k,s}(\eta, g)$.

**Remark 4.** In [5], the equivalence between MRD codes in $\mathbb{F}_{q}^{n \times n}$ are slightly different from ours. They use the isometries defined on $\mathbb{F}_{q}^{n \times n}$ by Wan and Hua in [17] to be the equivalence on MRD codes. In the language of linearized polynomials, besides the equivalence (Definition 4.1) between $\mathcal{C}'$ and $\mathcal{C}$, we also have to check the equivalence between $\mathcal{C}'$ and the adjoint code $\hat{\mathcal{C}}$ of $\mathcal{C}$.

However, even if we use the definition of equivalence on MRD codes in [5], by Theorems 4.6, 4.7, 4.8 and Proposition 4.3 we can still determine the equivalence between most of the generalized twisted Gabidulin codes.

ACKNOWLEDGMENT

This work is supported by the Research Project of MIUR (Italian Office for University and Research) “Strutture geometriche, Combinatoria e loro Applicazioni” 2012.

REFERENCES

[1] A. A. Albert. Generalized twisted fields. Pacific Journal of Mathematics, 11:1–8, 1961.
[2] A. A. Albert. Isotopy for generalized twisted fields. Anais da Academia Brasileira de Ciências, 33:265–275, 1961.
[3] M. Biliotti, V. Jha, and N. L. Johnson. The collineation groups of generalized twisted field planes. Geometriae Dedicata, 76:97–126, 1999.
[4] A. Cossidente, G. Marino, and F. Pavese. Nonlinear maximum rank distance codes. preprint, 2015.
[5] J. de la Cruz, M. Kiermaier, A. Wassermann, and W. Willems. Algebraic structures of MRD Codes. arXiv:1502.02711 [cs, math], Jan. 2015.
[6] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. Journal of Combinatorial Theory, Series A, 25(3):226–241, Nov. 1978.
[7] E. Gabidulin. Theory of codes with maximum rank distance. Problems of information transmission, 21:3–16, 1985.
[8] E. M. Gabidulin. Public-key cryptosystems based on linear codes over large alphabets: efficiency and weakness. In Codes and Cyphers, pages 17–31. Formara Limited, 1995.
[9] M. Gadouleau and Z. Yan. Properties of codes with the rank metric. In IEEE Global Telecommunications Conference 2006, pages 1–5, 2006.
[10] W. M. Kantor. Commutative semifields and symplectic spreads. Journal of Algebra, 270(1):96–114, 2003.
[11] R. Koetter and F. Kschischang. Coding for errors and erasure in random network coding, IEEE Transactions on Information Theory, 54(8):3579–3591, Aug. 2008.
[12] A. Kshevetskiy and E. Gabidulin. The new construction of rank codes. In International Symposium on Information Theory, 2005. ISIT 2005. Proceedings, pages 2105–2108, Sept. 2005.
[13] R. Lidl and H. Niederreiter. Finite fields, volume 20 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, second edition, 1997.
[14] K. Morrison. Equivalence for rank-metric and matrix codes and automorphism groups of gabidulin codes. IEEE Transactions on Information Theory, 60(11):7035–7046, 2014.
[15] A. Ravagnani. Rank-metric codes and their duality theory. Designs, Codes and Cryptography, pages 1–20, Apr. 2015.
[16] J. Sheekey. A new family of linear maximum rank distance codes. arXiv:1504.01581 [math], Apr. 2015.
[17] Z. Wan and L. Hua. *Geometry of Matrices*. World Scientific, Jan. 1996.

Dipartimento di Matematica e Applicazioni “R. Caccioppoli”, Università degli Studi di Napoli “Federico II”, 1-80126 Napoli, Italy

*E-mail address*: lunardon@unina.it

Dipartimento di Matematica e Applicazioni “R. Caccioppoli”, Università degli Studi di Napoli “Federico II”, 1-80126 Napoli, Italy

*E-mail address*: rtrombet@unina.it

Dipartimento di Matematica e Applicazioni “R. Caccioppoli”, Università degli Studi di Napoli “Federico II”, 1-80126 Napoli, Italy

*E-mail address*: yue.zhou.ovgu@gmail.com