Advances in Mathematics of Communications
Volume 12, No. 4, 2018, 707–721
doi:10.3934/amc.2018042

SELF-DUALITY OF GENERALIZED TWISTED GABIDULIN CODES

Kamil Otal† and Ferruh Özbudak*

Department of Mathematics and Institute of Applied Mathematics
Middle East Technical University, 06800, Ankara, Turkey

Wolfgang Willems

Otto-von-Guericke-Universität, Magdeburg, Germany
& Universidad del Norte, Barranquilla, Colombia

(Communicated by Michael Kiermaier)

Abstract. Self-duality of Gabidulin codes was investigated in [10] and the authors provided an if and only if condition for a Gabidulin code to be equivalent to a self-dual maximum rank distance (MRD) code. In this paper, we investigate the analog problem for generalized twisted Gabidulin codes (a larger family of linear MRD codes including the family of Gabidulin codes). We observe that the condition presented in [10] still holds for generalized Gabidulin codes (an intermediate family between Gabidulin codes and generalized twisted Gabidulin codes). However, beyond the family of generalized Gabidulin codes we observe that some additional conditions are required depending on the additional parameters. Our tools are similar to those in [10] but we also use linearized polynomials, which leads to further tools and direct proofs.

1. Introduction

1.1. Maximum rank distance codes. Let q be a prime power, $\mathbb{F}_q$ be the finite field of q elements and $\mathbb{F}_q^{m\times n}$ be the set of $m\times n$ matrices over $\mathbb{F}_q$. The function d defined by

$$d(A,B) := \operatorname{rank}(A-B)$$

on $\mathbb{F}_q^{m\times n}\times\mathbb{F}_q^{m\times n}$ is a metric called the *rank distance* on $\mathbb{F}_q^{m\times n}$. A subset $\mathcal{C}$ of $\mathbb{F}_q^{m\times n}$, including at least two matrices, with the rank distance is called a *rank metric code*. By "a code" we always mean "a rank metric code" unless otherwise stated. The *minimum distance* $d(\mathcal{C})$ of a code $\mathcal{C}$ is naturally defined by $d(\mathcal{C}) := \min\{d(A,B) : A,B\in\mathcal{C} \text{ and } A\neq B\}$. We call a code $K-$*linear* if it is also a vector space over K, where K is a subfield of $\mathbb{F}_q$. In particular, $\mathbb{F}_q-$linear codes are called *linear* and $K-$linear codes are called *additive* if K is a prime field. A tight upper bound for rank metric codes is given in the following.

Proposition 1. [3] *Let $\mathcal{C}\subseteq\mathbb{F}_q^{m\times n}$ be a rank metric code, then*

$$|\mathcal{C}| \leq q^{\max\{m,n\}(\min\{m,n\}-d(\mathcal{C})+1)}.$$

2010 *Mathematics Subject Classification:* Primary: 11T71; Secondary: 94B05.
Key words and phrases: Rank metric codes, self-dual maximum rank distance codes, generalized twisted Gabidulin codes, linearized polynomials.

† The current affilitaion is: TÜBİTAK BİLGEM UEKAE, 41470, Gebze/Kocaeli, Turkey.
* Corresponding author: Ferruh Özbudak.

The bound given in Proposition 1 is called the *Singleton-like bound*. A rank metric code is called *maximum rank distance (MRD) code* if it meets the Singleton-like bound. MRD codes have several applications in random network coding, space-time coding, distributed storage, MIMO communication and cryptology .

The classification of $\mathbb{F}_q^{m\times n}$ with respect to the rank metric was given in [16, Theorem 3.4]. This idea is utilized to define an equivalence notion between two rank metric codes as follows: Two codes $\mathcal{C},\mathcal{C}' \subseteq \mathbb{F}_q^{m\times n}$ are called *equivalent* if there exist $X \in \mathrm{GL}(m,\mathbb{F}_q)$, $Y \in \mathrm{GL}(n,\mathbb{F}_q)$ and $Z \in \mathbb{F}_q^{m\times n}$ such that

$$\mathcal{C}' = X\mathcal{C}^\sigma Y + Z := \{XC^\sigma Y + Z : C \in \mathcal{C}\} \text{ when } m \neq n,$$
$$\mathcal{C}' = X\mathcal{C}^\sigma Y + Z \text{ or } \mathcal{C}' = X(\mathcal{C}^\sigma)^\intercal Y + Z := \{X(C^\sigma)^\intercal Y + Z : C \in \mathcal{C}\} \text{ when } m = n$$

for some automorphism σ of $\mathbb{F}_q$ acting on the entries of $C \in \mathcal{C}$, where the superscript $\intercal$ denotes the transpose of matrices. If both $\mathcal{C}$ and $\mathcal{C}'$ are additive, then Z must be the zero matrix. Similarly, if $\mathcal{C}$ and $\mathcal{C}'$ are both linear, then σ can be taken as the identity without loss of generality. Therefore, the following corollary can be used as a definition of equivalence for linear codes: Two linear codes $\mathcal{C},\mathcal{C}' \subseteq \mathbb{F}_q^{m\times n}$ are equivalent if there exist $X \in \mathrm{GL}(m,\mathbb{F}_q)$ and $Y \in \mathrm{GL}(n,\mathbb{F}_q)$ such that

$$\begin{aligned} &\mathcal{C}' = X\mathcal{C}Y \text{ when } m \neq n,\\ &\mathcal{C}' = X\mathcal{C}Y \text{ or } \mathcal{C}' = X(\mathcal{C}^\intercal)Y \text{ when } m = n. \end{aligned} \tag{1}$$

Additionally, in case $m = n$ we call the equivalence *proper* if $\mathcal{C}' = X\mathcal{C}Y$ for some $X, Y \in \mathrm{GL}(n,\mathbb{F}_q)$.

Let $\mathrm{trace}(X)$ denote the classical matrix trace of a square matrix X over $\mathbb{F}_q$. The transformation from $\mathbb{F}_q^{m\times n} \times \mathbb{F}_q^{m\times n}$ to $\mathbb{F}_q$ given by $(A,B) \mapsto \mathrm{trace}(BA^\intercal)$ is a symmetric bilinear form, and corresponds to the classical inner product when we write matrices in $\mathbb{F}_q^{m\times n}$ as vectors in $\mathbb{F}_q^{mn}$. Using this bilinear form, we define the *dual code* $\mathcal{C}^\perp$ of a linear code $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ as follows.

$$\mathcal{C}^\perp := \{A \in \mathbb{F}_q^{m\times n} : \mathrm{trace}(BA^\intercal) = 0 \text{ for all } B \in \mathcal{C}\}. \tag{2}$$

Note that $\mathcal{C}^\perp$ is a linear code, $\dim(\mathcal{C}) + \dim(\mathcal{C}^\perp) = mn$ and $d(\mathcal{C}^\perp) = \min\{m,n\} - d(\mathcal{C}) + 2$. Hence, if $\mathcal{C}$ is an MRD code, then so is $\mathcal{C}^\perp$. We want to remark that some other duality notions can be defined using different symmetric bilinear forms. For more information about duality we refer to [14].

1.2. RELATED WORK. We briefly summarize the history of constructions of MRD codes with respect to the equivalence given in equation (1) as follows.

- 1978 and 1985: **Gabidulin codes** were discovered in [3] and independently in [6].
- 2005: A generalization of Gabidulin codes, known as **generalized Gabidulin codes**, was given in [7].
- 2016: Another generalization of Gabidulin codes, called **twisted Gabidulin codes**, were discovered in [15]. A particular case of this family was independently discovered also in [11].
- 2016: A more general family including both generalized Gabidulin codes and twisted Gabidulin codes, known as **generalized twisted Gabidulin codes**, was remarked in [15] and investigated in [9].

In the literature, there are also non-linear constructions of MRD codes (see for instance [2, 5, 12, 13]). However, in this paper we only focus on linear codes since we are interested in duality questions.

Self-duality of Gabidulin codes was considered in [10] and a criterion for being equivalent to a self-dual linear MRD code was given (see Theorem 2.3). The authors also provided an if and only if condition for a Gabidulin code to be equivalent to a self-dual MRD code.

1.3. OUR CONTRIBUTIONS. In this paper, we investigate the property that a generalized twisted Gabidulin code is equivalent to a self-dual code. We show in Theorem 3.6(1) that the conditions in [10] hold for generalized Gabidulin codes. Therefore, Theorem 3.6(1) may be seen as a natural generalization of [10, Theorem 4].

If we look at other generalized twisted Gabidulin codes (i.e. the ones which are not generalized Gabidulin), we observe that some additional conditions are required depending on the additional parameters (see Theorem 3.6(2)).

We want to emphasize that we use the linearized polynomial representation of codewords, whereas in [10] only the matrix representation came into play. Note that this linearized polynomial approach allows us to deal with additional tools and derive more direct proofs.

1.4. ORGANIZATION OF THE PAPER. In Section 2 we present the linearized polynomial representation of rank metric codes and then we introduce the family of generalized twisted Gabidulin codes using this representation. In addition, we develop some useful tools which are mostly in the linearized polynomial language.

In Section 3 we provide our main result, together with some important lemmas. Lastly we prove our main result in Section 4 examining the cases separately.

2. PRELIMINARIES

2.1. LINEARIZED POLYNOMIALS AND RANK METRIC CODES. A polynomial $f(x) \in \mathbb{F}_{q^n}[x]$ of the form

$$f(x) = \sum_{i=0}^{l} \alpha_i x^{q^i} \tag{3}$$

is called a *q-polynomial* (or, a *linearized polynomial*) over $\mathbb{F}_{q^n}$. We call l in (3) the *q-degree* of f if $\alpha_l \neq 0$. Some important facts about linearized polynomials are given below.

- $f(c\alpha + \beta) = cf(\alpha) + f(\beta)$ for all $c \in \mathbb{F}_q$ and $\alpha, \beta \in \overline{\mathbb{F}}_q$, where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$.
- The multiplicity of each root of f in $\overline{\mathbb{F}}_q$ is the same and equal to q^r where r is the smallest integer satisfying $\alpha_r \neq 0$.
- The set of roots of f in an extension field of $\mathbb{F}_{q^n}$ constitutes a vector space over $\mathbb{F}_q$. In particular, the set of roots of f in $\mathbb{F}_{q^n}$ is a subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. This set is called the *kernel* of f and denoted by $\ker(f)$. The *rank* of f is defined by $n - \dim(\ker(f))$ and denoted by $\operatorname{rank}(f)$.

For more information the reader is referred to [8].

Let $f(x) \in \mathbb{F}_{q^n}[x]$ be a q-polynomial of q-degree at most $n-1$. Let $\Gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n)$ be an ordered basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, for any $\alpha \in \mathbb{F}_{q^n}$ we have

$$\begin{aligned} f(\alpha) &= f(c_1\gamma_1 + c_2\gamma_2 + \cdots + c_n\gamma_n) \\ &= c_1 f(\gamma_1) + c_2 f(\gamma_2) + \cdots + c_n f(\gamma_n) \\ &= \begin{bmatrix} f(\gamma_1) & f(\gamma_2) & \ldots & f(\gamma_n) \end{bmatrix} \begin{bmatrix} c_1 & c_2 & \ldots & c_n \end{bmatrix}^{\mathsf{T}} \end{aligned}$$

$$= [\gamma_1\ \gamma_2\ \dots\ \gamma_n] \begin{bmatrix} f(\gamma_1)_{\gamma_1} & f(\gamma_2)_{\gamma_1} & \dots & f(\gamma_n)_{\gamma_1} \\ f(\gamma_1)_{\gamma_2} & f(\gamma_2)_{\gamma_2} & \dots & f(\gamma_n)_{\gamma_2} \\ \vdots & \vdots & \ddots & \vdots \\ f(\gamma_1)_{\gamma_n} & f(\gamma_2)_{\gamma_n} & \dots & f(\gamma_n)_{\gamma_n} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} \tag{4}$$

for some $c_i \in \mathbb{F}_q$ and $1 \le i \le n$, where $f(\gamma_i)_{\gamma_j} \in \mathbb{F}_q$ denotes the coefficient of γ_j if $f(\gamma_i)$ is written as a linear combination of $\gamma_1, \dots, \gamma_n$ over $\mathbb{F}_q$ for all $1 \le i, j \le n$. Let $[f]_\Gamma$ denote the matrix given by $[f(\gamma_j)_{\gamma_i}]_{i,j} \in \mathbb{F}_q^{n\times n}$. Note that there is a one to one correspondence between f and $[f]_\Gamma$ with respect to the fixed ordered basis Γ. We also have $\mathrm{rank}(f) = \mathrm{rank}([f]_\Gamma)$. Moreover, the algebra $\mathbb{F}_q^{n\times n}$ with the matrix addition and the matrix multiplication is isomorphic to the algebra

$$\mathcal{L}_n := \{\alpha_0 x + \alpha_1 x^q + \dots + \alpha_{n-1} x^{q^{n-1}} : \alpha_0, \dots, \alpha_{n-1} \in \mathbb{F}_{q^n}\}$$

with the addition and the composition of polynomials modulo $x^{q^n} - x$, respectively. Note also that similar isomorphism ideas were known for a very long time [1, 4]. Various isomorphisms of $\mathcal{L}_n$ in detail are available in [17].

For $f(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i} \in \mathcal{L}_n$ we define the *adjoint polynomial* $\widehat{f}$ of f as

$$\widehat{f}(x) := \sum_{i=0}^{n-1} \alpha_{n-i}^{q^i} x^{q^i} \mod x^{q^n} - x. \tag{5}$$

Suppose that Γ is a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, namely $\Gamma = (\gamma, \gamma^q, \dots, \gamma^{q^{n-1}})$ for some normal element γ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then we define

$$t(x) := \mathrm{Tr}_{q^n/q}(\gamma^2)x + \mathrm{Tr}_{q^n/q}(\gamma^{1+q})x^q + \dots + \mathrm{Tr}_{q^n/q}(\gamma^{1+q^{n-1}})x^{q^{n-1}}, \tag{6}$$

where $\mathrm{Tr}_{q^n/q}$ denotes the trace function on $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ given by $\alpha \mapsto \alpha + \alpha^q + \dots + \alpha^{q^{n-1}}$, which we also consider as a function on $\overline{\mathbb{F}_q}$. The polynomial $t(x)$ together with adjoint polynomials play a crucial role in our results, especially in order to understand the transpose of $[f]_\Gamma$. We summarize this role in Proposition 2 below.

Lemma 2.1. *Let $t(x)$ be the polynomial as defined in (6). Then the following hold.*

1. $[x^q]_\Gamma = [\delta_{i-1,j}]_{1\le i,j\le n}$. *Hence* $\det([x^q]_\Gamma) = (-1)^{n+1}$ *and* $[x^q]_\Gamma^\intercal = [x^q]_\Gamma^{-1}$.
2. $[(x^{q^l}) \circ t(x)]_\Gamma = [t(x) \circ (x^{q^l})]_\Gamma = [(x^{q^{n-l}}) \circ t(x)]_\Gamma^\intercal$ *for all* $0 \le l \le n-1$.
3. $[\alpha x]_\Gamma^\intercal = [t \circ (\alpha x) \circ t^{-1}]_\Gamma$.

Proof.
1. The matrix representation $[x^q]_\Gamma = [\delta_{i-1,j}]_{1\le i,j\le n}$ is clear when we write $f(x) = x^q$ in equation (4). The other two statements are straightforward from this representation.
2. The first equality can be directly seen because each coefficient of $t(x)$ is in $\mathbb{F}_q$. The second equality can be observed when we write the statements explicitly using equation (4).
3. This statement with a proof is available in [10, Lemma 2].

□

Proposition 2. *Let $t(x)$ be the polynomial as defined in (6). Then the following hold.*

1. *$t(x)$ is a self adjoint polynomial, i.e. $\widehat{t}(x) = t(x)$.*
2. *The associated matrix $[t]_\Gamma$ of t is an invertible and symmetric matrix.*
3. *For any $f \in \mathcal{L}_n$, we have $[f]_\Gamma^\intercal = [t \circ \widehat{f} \circ t^{-1}]_\Gamma$.*

Proof. 1. The statement is clear when the definition of $t(x)$ in (6) is used in (5).

2. Note that $[t]_\Gamma$ is the Gram matrix of the trace bilinear form $(\alpha, \beta) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \mapsto \mathrm{Tr}_{q^n/q}(\alpha\beta) \in \mathbb{F}_q$ with respect to the basis Γ, which is symmetric and non-degenerate.

3. Any $f \in \mathcal{L}_n$ can be written as $f(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i}$ for some $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_{q^n}$. Therefore,

$$\begin{aligned}
[f(x)]_\Gamma^\intercal &= \left[\sum_{i=0}^{n-1} \alpha_i x^{q^i}\right]_\Gamma^\intercal \\
&= \left[\sum_{i=0}^{n-1} (\alpha_i x) \circ (x^{q^i})\right]_\Gamma^\intercal \\
&= \sum_{i=0}^{n-1} \left[(\alpha_i x) \circ (x^{q^i})\right]_\Gamma^\intercal \\
&= \sum_{i=0}^{n-1} \left[x^{q^i}\right]_\Gamma^\intercal [\alpha_i x]_\Gamma^\intercal \\
&= \sum_{i=0}^{n-1} \left[x^{q^{-i}}\right]_\Gamma [\alpha_i x]_\Gamma^\intercal && \text{(by Lemma 2.1(1))} \\
&= \sum_{i=0}^{n-1} \left[x^{q^{-i}}\right]_\Gamma [t(x)]_\Gamma \, [\alpha_i x]_\Gamma \, [t^{-1}(x)]_\Gamma && \text{(by Lemma 2.1(3))} \\
&= \sum_{i=0}^{n-1} [t(x)]_\Gamma \left[x^{q^{-i}}\right]_\Gamma [\alpha_i x]_\Gamma \, [t^{-1}(x)]_\Gamma && \text{(by Lemma 2.1(2))} \\
&= \sum_{i=0}^{n-1} [t(x)]_\Gamma \left[\alpha_i^{q^{-i}} x^{q^{-i}}\right]_\Gamma [t^{-1}(x)]_\Gamma \\
&= [t(x)]_\Gamma \left(\sum_{i=0}^{n-1} \left[\alpha_i^{q^{-i}} x^{q^{-i}}\right]_\Gamma\right) [t^{-1}(x)]_\Gamma \\
&= [t(x) \circ \widehat{f}(x) \circ t^{-1}(x)]_\Gamma.
\end{aligned}$$

□

When we consider the algebra $\mathcal{L}_n$ as the ambient space instead of the algebra $\mathbb{F}_q^{n\times n}$ we observe that the equivalence in (1) for linear codes appears as follows: If $\mathcal{C}$ and $\mathcal{C}'$ are two linear subspaces of $\mathcal{L}_n$ over $\mathbb{F}_q$, then $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if and only if there exist in $\mathcal{L}_n$ invertible polynomials g and h such that

$$\begin{aligned}
\mathcal{C}' &= g \circ \mathcal{C} \circ h := \{g(x) \circ f(x) \circ h(x) \mod x^{q^n} - x : f(x) \in \mathcal{C}\}, \text{ or} \\
\mathcal{C}' &= g \circ \widehat{\mathcal{C}} \circ h := \{g(x) \circ \widehat{f}(x) \circ h(x) \mod x^{q^n} - x : f(x) \in \mathcal{C}\},
\end{aligned} \tag{7}$$

where the $\circ$ operation denotes the composition, i.e., $f_1(x) \circ f_2(x) = f_1(f_2(x)) \mod x^{q^n} - x$ for $f_i \in \mathcal{L}_n$. Note that $\circ$ is associative on $\mathcal{L}_n$. Furthermore, the minimum distance $d(\mathcal{C})$ is indeed the minimum non-zero rank of the elements in $\mathcal{C}$ because $\mathcal{C}$ is closed under addition.

To present rank metric codes we usually prefer $\mathcal{L}_n$ as the ambient space instead of $\mathbb{F}_q^{n\times n}$, since we make use of properties of linearized polynomials in general. In case we need the matrix expansion, we use the notation $[f]_\Gamma$ for $f \in \mathcal{L}_n$.

Recall that the norm function $\mathrm{Norm}_{q^n/q}$ on $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given by $\alpha \mapsto \alpha^{1+q+\cdots+q^{n-1}}$, which we also consider as a function on $\overline{\mathbb{F}_q}$. Now using the norm function we define generalized twisted Gabidulin codes.

Theorem 2.2. [15, 9] *Let k, h, s be nonnegative integers and $\eta \in \mathbb{F}_{q^n}$ satisfying $1 \le k \le n-1$, $\gcd(n,s) = 1$ and $\mathrm{Norm}_{q^n/q}(\eta) \neq (-1)^{nk}$, where* gcd *denotes the greatest common divisor of integers. Then*
(8)
$$\mathcal{H}_{n,k,s}(\eta,h) := \{\alpha_0 x + \alpha_1 x^{q^s} + \cdots + \alpha_{k-1} x^{q^{s(k-1)}} + \eta\alpha_0^{q^h} x^{q^{sk}} : \alpha_0,\ldots,\alpha_{k-1} \in \mathbb{F}_{q^n}\}$$
is an MRD code of minimum distance $n-k+1$.

$\mathcal{H}_{n,k,s}(\eta,h)$ is called a *generalized twisted Gabidulin code*. Note that h becomes useless when $\eta = 0$. In this case the code is also called a *generalized Gabidulin code* and denoted by $\mathcal{G}_{n,k,s}$. Generalized Gabidulin codes were first considered in [7]. The codes $\mathcal{G}_{n,k,1}$ which form a sub-family of the generalized Gabidulin codes were discovered earlier in [3, 6]. Usually they are called *Gabidulin codes*.

2.2. KEY TOOLS FOR SELF-DUALITY. Next we present some basic results, which we will use in the following section while investigating self-duality of generalized twisted Gabidulin codes. From now on, we fix the following assumptions and notations.

- γ is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$,
- $\Gamma = (\gamma, \gamma^q, \ldots, \gamma^{q^{n-1}})$ is a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ constructed by γ,
- q is odd ([10, Theorem 1] indicates that no self-dual MRD codes exist when q is even),
- $m = n$ and n is even (no self-dual codes exist when n is odd; recall also that $\dim(\mathcal{C}) + \dim(\mathcal{C}^\perp) = n^2$),
- $n \ge 4$ (note that for $n = 2$, [10, Proposition 1] determines completely all MRD codes which are equivalent to a self-dual code.).

We use the following theorem to characterize the codes which are properly equivalent to self-dual codes.

Theorem 2.3. [10, Theorem 2] *Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times n}$ be a linear rank metric code. Then $\mathcal{C}$ is properly equivalent to a self-dual code if and only if there are symmetric matrices $A, B \in \mathbb{F}_q^{n\times n}$ such that $\det(A), \det(B) \in (\mathbb{F}_q^\star)^2$ and $\mathcal{C}^\perp = A\mathcal{C}B$.*

The next lemma provides some essential information about linearized monomials $\alpha x^{q^i} \in \mathcal{L}_n$, where $\alpha \in \mathbb{F}_{q^n}$ and $0 \le i \le n-1$. It is a slightly extended version of [10, Lemma 4].

Lemma 2.4. *Let $t(x) \in \mathcal{L}_n$ be the linearized polynomial defined in equation (6). Then the following statements hold.*

1. $\det[t(x)]_\Gamma \notin (\mathbb{F}_q^\star)^2$ *and* $\det[\alpha x]_\Gamma = \mathrm{Norm}_{q^n/q}(\alpha)$ *for all* $\alpha \in \mathbb{F}_{q^n}$.
2. $[t(x) \circ (\alpha x)]_\Gamma$ *and* $[(\alpha x) \circ t^{-1}(x)]_\Gamma$ *are symmetric for all* $\alpha \in \mathbb{F}_{q^n}$.
3. *The following statements are equivalent.*
   (a) $[t(x) \circ (x^{q^l}) \circ (\alpha x)]_\Gamma$ *is symmetric,*
   (b) $[(\alpha x) \circ (x^{q^l}) \circ t^{-1}(x)]_\Gamma$ *is symmetric,*
   (c) *either* $l = n/2$ *and* $\alpha \in \mathbb{F}_{q^{n/2}}^\star$, *or* $l = 0$ *and* $\alpha \in \mathbb{F}_{q^n}^\star$.

Proof. 1. The first statement is exactly [10, Lemma 4(v)], where also a proof is available. The second statement is coming from the following correspondence. Let

- $F_1 = \mathbb{F}_{q^n}$, with the usual addition and multiplication of the field,
- $F_2 = \{\alpha x : \alpha \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}[x]$, with the addition and composition of polynomials,
- $F_3 = \{[\alpha x]_\Gamma : \alpha \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_q^{n\times n}$, with the addition and multiplication of matrices.

Then there is an isomorphism between any two of these three mathematical structures, namely

$$\begin{array}{ccccc} F_1 & \leftrightarrow & F_2 & \leftrightarrow & F_3 \\ \alpha & \leftrightarrow & \alpha x & \leftrightarrow & [\alpha x]_\Gamma. \end{array}$$

Now, let $g(y) = y^n + g_{n-1}y^{n-1} + \ldots + g_1 y + g_0 \in \mathbb{F}_q[y]$ be the characteristic polynomial of $[\alpha x]_\Gamma$ for some $\alpha \in \mathbb{F}_{q^n}$. Then the isomorphism between F_1 and F_3 implies that $g(y)$ is also the characteristic polynomial of $\alpha \in \mathbb{F}_{q^n}$. Hence,

$$\det[\alpha x]_\Gamma = (-1)^n g_0 = \mathrm{Norm}_{q^n/q}(\alpha).$$

2. The statement can be verified directly applying Proposition 2(3) to obtain the transpose of each statement.
3. The statement is exactly [10, Lemma 4(viii)] and a proof is available there.

□

Now we introduce another important result, which is a generalization of [10, Lemma 3(iv)].

Lemma 2.5. *For linearized monomials αx^{q^l} we can determine* $\mathrm{trace}([\alpha x^{q^l}]_\Gamma)$ *for all $0 \le l \le n-1$ and $\alpha \in \mathbb{F}_{q^n}$ as follows.*

1. $\mathrm{trace}([\alpha x]_\Gamma) = \mathrm{Tr}_{q^n/q}(\alpha)$.
2. $\mathrm{trace}([\alpha x^{q^l}]_\Gamma) = 0$ *for all* $1 \le l \le n-1$.

Lemma 2.5 can be seen evident considering cyclic algebras constructed by the isomorphism given in equation (4). Note also that Lemma 2.5 was remarked in [15] as a well-known fact. However, especially the proof of Lemma 2.5(1) is not available neither in [10] nor in [15]. Hence we give an elementary proof of the lemma below.

Proof. Let $A = [\alpha x]_\Gamma$. Using normality of Γ we obtain

$$\alpha\gamma^{q^{j-1}} = \sum_{i=1}^{n} A_{ij}\gamma^{q^{i-1}} \Rightarrow \alpha^{q^{n-j}}\gamma^{q^{n-1}} = \sum_{i=1}^{n} A_{ij}\gamma^{q^{i-j-1}}$$
$$\Rightarrow \sum_{j=1}^{n} \alpha^{q^{n-j}}\gamma^{q^{n-1}} = \sum_{j=1}^{n}\sum_{i=1}^{n} A_{ij}\gamma^{q^{i-j-1}}.$$

The left hand side of the last statement is clearly $\mathrm{Tr}_{q^n/q}(\alpha)\gamma^{q^{n-1}}$. The right hand side can be rewritten by taking j from i to $i+n-1$ and hence we obtain the following.

(9)
$$\mathrm{Tr}_{q^n/q}(\alpha)\gamma^{q^{n-1}} = \left(\sum_{i=1}^{n} A_{i,i}\right)\gamma^{q^{n-1}} + \left(\sum_{i=1}^{n} A_{i,i+1}\right)\gamma^{q^{n-2}} + \cdots + \left(\sum_{i=1}^{n} A_{i,i-1}\right)\gamma.$$

The statements of the lemma can be observed from equation (9) as follows.

1. In equation (9), the coefficient of each γ^{q^i} for all $0 \leq i \leq n-1$ is clearly in $\mathbb{F}_q$. Also remember that Γ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The uniqueness of the coefficients in $\mathbb{F}_q$ with respect to a fixed basis implies
$$\mathrm{Tr}_{q^n/q}(\alpha) = \sum_{i=1}^{n} A_{i,i},$$
which completes the first part of the proof.
2. Note that $\alpha x^{q^l} = (\alpha x) \circ (x^{q^l})$ and
$$[x^{q^l}]_\Gamma = [x^q]_\Gamma^l = [\delta_{i-1,j}]_{1\leq i,j\leq n}^l = [\delta_{i-l,j}]_{1\leq,i,j\leq n}$$
which implies $[\alpha x^{q^l}]_\Gamma = A[\delta_{i-l,j}]_{1\leq,i,j\leq n}$. Thus we have
$$\mathrm{trace}([\alpha x^{q^l}]_\Gamma) = \sum_{i=1}^{n} A_{i,i+l},$$
which is zero for $1 \leq l \leq n-1$ according to the equation (9).

□

2.3. AUTOMORPHISM GROUPS OF RANK METRIC CODES. Now we introduce the proper automorphism group and full automorphism group of a rank metric code. Let $\mathcal{C}$ be a linear code in $\mathcal{L}_n$, then the set of pairs $(g(x), h(x))$ in $\mathcal{L}_n \times \mathcal{L}_n$ satisfying

$$\mathcal{C} = g(x) \circ \mathcal{C} \circ h(x) \tag{10}$$

forms a group under the multiplication defined by

$$(g_1(x), h_1(x))(g_2(x), h_2(x)) = (g_1(x) \circ g_2(x), h_2(x) \circ h_1(x)). \tag{11}$$

This group is called the *proper automorphism group* of $\mathcal{C}$ and denoted by $\mathrm{Aut}^{(p)}(\mathcal{C})$.

Similarly, the *full automorphism group* of $\mathcal{C}$ is defined as the group generated by the union of $\mathrm{Aut}^{(p)}(\mathcal{C})$ and the set of $[g(x), h(x)]$ couples satisfying

$$\mathcal{C} = g(x) \circ t^{-1}(x) \circ \widehat{\mathcal{C}} \circ t(x) \circ h(x) \tag{12}$$

and denoted by $\mathrm{Aut}(\mathcal{C})$. We may determine this set up more explicitly as follows: Define

$$(g, h) : f \mapsto g \circ f \circ h,$$
$$[g, h] : f \mapsto g \circ t \circ \widehat{f} \circ t^{-1} \circ h.$$

on the set of automorphisms of $\mathcal{C} \subseteq \mathcal{L}_n$ and extend the multiplication in equation (11) from $\mathrm{Aut}^{(p)}(\mathcal{C})$ to $\mathrm{Aut}(\mathcal{C})$ as

- $[g_1, h_1][g_2, h_2] = (g_1 \circ t \circ \widehat{h_2} \circ t^{-1}, t \circ \widehat{g_2} \circ t^{-1} \circ h_1)$,
- $[g_1, h_1](g_2, h_2) = [g_1 \circ t \circ \widehat{h_2} \circ t^{-1}, t \circ \widehat{g_2} \circ t^{-1} \circ h_1]$,
- $(g_1, h_1)[g_2, h_2] = [g_1 \circ g_2, h_2 \circ h_1]$.

In that way we create the full automorphism group $\mathrm{Aut}(\mathcal{C})$ of a rank metric code $\mathcal{C} \subseteq \mathcal{L}_n$. Therefore, taking only one fixed non-proper automorphism $[g, h]$ (if any exist), we observe that

$$\mathrm{Aut}(\mathcal{C}) = \langle \mathrm{Aut}^{(p)}(\mathcal{C}) \cup \{[g, h]\} \rangle.$$

Also note that the index of $\mathrm{Aut}^{(p)}(\mathcal{C})$ in $\mathrm{Aut}(\mathcal{C})$ is either one or two, since the square of a non-proper automorphism is proper. In particular, it is easy to show that the identity element of the full automorphism group of $\mathcal{L}_n$ is (x, x).

3. Self-duality of generalized twisted Gabidulin codes

From now on we fix $k = \dfrac{n}{2} > 1$ since we investigate self-duality and assumed $n \geq 4$ as mentioned at the beginning of Section 2.2.

The following lemma can be derived directly from Section 2 and Section 3 in [15] and [9, Theorem 4.4].

Lemma 3.1. *Two generalized twisted Gabidulin codes $\mathcal{H}_{n,\frac{n}{2},s}(\eta_1, h_1)$ and $\mathcal{H}_{n,\frac{n}{2},s}(\eta_2, h_2)$ are properly equivalent, i.e.,*

$$\mathcal{H}_{n,\frac{n}{2},s}(\eta_1, h_1) = f \circ \mathcal{H}_{n,\frac{n}{2},s}(\eta_2, h_2) \circ g$$

if and only if $h_1 = h_2$, $f(x) = \alpha x^{q^i}$, $g(x) = \beta x^{q^{-i}}$ and $\eta_1^{q^i} = \eta_2 \alpha^{q^{h_1}-1} \beta^{q^{i+h_1}-q^{s\frac{n}{2}+i}}$ for some $\alpha, \beta \in \mathbb{F}_{q^n}^\star$ and $0 \leq i \leq n-1$.

Corollary 1. *The proper automorphism group of the generalized twisted Gabidulin code $\mathcal{H}_{n,\frac{n}{2},s}(\eta, h)$ is*

$$\mathrm{Aut}^{(p)}(\mathcal{H}_{n,\frac{n}{2},s}(\eta, h))$$
$$= \left\{ (\alpha x^{q^i}, \beta x^{q^{-i}}) : \alpha, \beta \in \mathbb{F}_{q^n}^\star,\ 0 \leq i \leq n-1,\ \eta^{q^i} = \eta \alpha^{q^h-1} \beta^{q^{i+h}-q^{s\frac{n}{2}+i}} \right\}.$$

Corollary 2. *The proper automorphism group $\mathrm{Aut}^{(p)}(\mathcal{G}_{n,k,s})$ of a generalized Gabidulin code $\mathcal{G}_{n,k,s}$ is*

$$\mathrm{Aut}^{(p)}(\mathcal{G}_{n,k,s}) = \{(\alpha x^{q^i}, \beta x^{q^{-i}}) : \alpha, \beta \in \mathbb{F}_{q^n}^\star, 0 \leq i \leq n-1\}.$$

The following lemma is a slight generalization of [10, Corollary 1] from $\mathcal{G}_{n,k,1}$ to $\mathcal{G}_{n,k,s}$.

Lemma 3.2. $\mathrm{Aut}(\mathcal{G}_{n,k,s}) \neq \mathrm{Aut}^{(p)}(\mathcal{G}_{n,k,s})$ *if $k > 1$.*

Proof. On $\mathcal{L}_n$, using

$$(g, h) : f \mapsto g \circ f \circ h,$$
$$[g, h] : f \mapsto g \circ t \circ \widehat{f} \circ t^{-1} \circ h.$$

we observe that

$$\mathrm{Aut}(\mathcal{G}_{n,s,k}) = \langle \mathrm{Aut}^{(p)}(\mathcal{G}_{n,s,k}) \cup \left\{ [t^{-1}, t \circ (x^{q^{s(k-1)}})] \right\} \rangle.$$

The index $[\mathrm{Aut}(\mathcal{G}_{n,s,k}) : \mathrm{Aut}^{(p)}(\mathcal{G}_{n,s,k})]$ is obviously either 1 or 2. Suppose that the index is 1, i.e., $\mathrm{Aut}(\mathcal{G}_{n,s,k}) = \mathrm{Aut}^{(p)}(\mathcal{G}_{n,s,k})$. Then there exist $\alpha, \beta \in \mathbb{F}_{q^n}$ and $0 \leq i \leq n-1$ such that

$$(\alpha x^{q^i}, \beta x^{q^{-i}}) = [t^{-1}, t \circ (x^{q^{s(k-1)}})].$$

However, for $x \in \mathcal{G}_{n,s,k}$ we have

$$(\alpha x^{q^i}, \beta x^{q^{-i}})(x) = \alpha \beta^{q^i} x,$$
$$\left[t^{-1}, t \circ (x^{q^{s(k-1)}}) \right](x) = x^{q^{s(k-1)}}$$

which are clearly not equal if $k > 1$. Hence the assumption is false, i.e., $\mathrm{Aut}(\mathcal{G}_{n,s,k}) \neq \mathrm{Aut}^{(p)}(\mathcal{G}_{n,s,k})$. □

The following corollary summarizes some basic facts of $\mathrm{Aut}(\mathcal{G}_{n,k,s})$.

Corollary 3. *The orders of* $\mathrm{Aut}^{(p)}(\mathcal{G}_{n,k,s})$ *and* $\mathrm{Aut}(\mathcal{G}_{n,k,s})$ *are* $n(q^n-1)^2/(q-1)$ *and* $2n(q^n-1)^2/(q-1)$ *respectively. In particular, the orders of given elements* $(\alpha x^{q^i}, \beta x^{q^{-i}})$ *and* $[\alpha x^{q^i}, \beta x^{q^{-i}}]$ *in* $\mathrm{Aut}(\mathcal{G}_{n,k,s})$ *are* $\mathrm{lcm}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta), n)$ *and* $\mathrm{lcm}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta), n, 2)$ *respectively, where* lcm *denotes the least common multiple of the integers and* ord *denotes the multiplicative order of elements in* $\mathbb{F}_{q^n}$.

The following lemma is also available in [15, 9] and easy to prove directly by computation.

Lemma 3.3. *1. The adjoint* $\widehat{\mathcal{G}_{n,\frac{n}{2},s}}$ *of a generalized Gabidulin code* $\mathcal{G}_{n,\frac{n}{2},s}$ *is properly equivalent to itself.*

2. The adjoint $\widehat{\mathcal{H}_{n,\frac{n}{2},s}}(\eta,h)$ *of a generalized twisted Gabidulin code* $\mathcal{H}_{n,\frac{n}{2},s}(\eta,h)$ *is properly equivalent to* $\mathcal{H}_{n,\frac{n}{2},s}(\eta^{-q^{-h}}, s\frac{n}{2}-h)$ *when* η *is nonzero.*

Now we can explicitly determine the dual of a generalized twisted Gabidulin code in terms of another generalized twisted Gabidulin code.

Lemma 3.4. *The dual code of a generalized twisted Gabidulin code* $\mathcal{H}_{n,\frac{n}{2},s}(\eta,h)$ *is*

$$\mathcal{H}^{\perp}_{n,\frac{n}{2},s}(\eta,h) = t\circ(x^{q^{s\frac{n}{2}}})\circ\mathcal{H}_{n,\frac{n}{2},s}(-\eta^{q^{s\frac{n}{2}-h}}, -h)\circ t^{-1}.$$

Proof. Let $\mathcal{C}' := t\circ(x^{q^{s\frac{n}{2}}})\circ\mathcal{H}_{n,\frac{n}{2},s}(-\eta^{q^{s\frac{n}{2}-h}}, -h)\circ t^{-1}$. Clearly

$$\dim\mathcal{C}' = \frac{n^2}{2} = n^2 - \frac{n^2}{2} = \dim\mathcal{L}_n - \dim\mathcal{H}_{n,\frac{n}{2},s}(\eta,h) = \dim\mathcal{H}^{\perp}_{n,\frac{n}{2},s}(\eta,h).$$

Hence it is enough to show that $\mathcal{C}'\subseteq\mathcal{H}^{\perp}_{n,\frac{n}{2},s}(\eta,h)$. For any $f\in\mathcal{H}_{n,\frac{n}{2},s}(\eta,h)$ and $g\in\mathcal{C}'$, we have

$$f\circ\left(t\circ\widehat{g}\circ t^{-1}\right) = \theta_0 x + \theta_1 x^q + \cdots + \theta_{n-1}x^{q^{n-1}}$$

for some $\theta_0,\theta_1,\ldots,\theta_{n-1}\in\mathbb{F}_{q^n}$. Then,

$$\mathrm{trace}[f\circ\left(t\circ\widehat{g}\circ t^{-1}\right)]_\Gamma = \mathrm{trace}[\theta_0 x]_\Gamma + \mathrm{trace}[\theta_1 x^q]_\Gamma + \cdots + \mathrm{trace}[\theta_{n-1}x^{q^{n-1}}]_\Gamma$$

Here, the right hand side is exactly $\mathrm{trace}[\theta_0 x]_\Gamma$ by Lemma 2.5(2). When we apply Lemma 2.5(1) and explicitly write θ_0 we observe that

$$\mathrm{trace}[\theta_0 x]_\Gamma = \mathrm{Tr}_{q^n/q}(\theta_0) = \mathrm{Tr}_{q^n/q}\left(\eta\alpha^{q^h}\beta^{q^{sk}} - \eta^{q^{n-h}}\alpha\beta^{q^{n-h-sk}}\right) = 0$$

for some α and β in $\mathbb{F}_{q^n}$. In conclusion we have

$$\mathrm{trace}\left([f]_\Gamma[g]_\Gamma^{\intercal}\right) = \mathrm{trace}[f\circ\left(t\circ\widehat{g}\circ t^{-1}\right)]_\Gamma = 0,$$

i.e. $\mathcal{C}'\subseteq\mathcal{H}^{\perp}_{n,\frac{n}{2},s}(\eta,h)$. Thus the proof is completed. □

Lastly we provide a technical lemma that we multiply use in the proof of the main theorem.

Lemma 3.5. *Let* $q\equiv 3 \mod 4$ *and* $n\equiv 2 \mod 4$. *If* $\zeta\in\mathbb{F}_{q^n}^{\star}$ *satisfies*

$$\zeta^{q^{n/2}-1} = -1, \tag{13}$$

then $\mathrm{Norm}_{q^n/q}(\zeta)$ *is a square in* $\mathbb{F}_q$.

Proof. Let $\mathrm{Norm}_{q^{n/2}/q}(\zeta) = c$, then $c^{q^{n/2}-1} = (-1)^{\frac{q^{n/2}-1}{q-1}} = -1 \neq 1$, i.e., $c \notin \mathbb{F}_{q^{n/2}}$ and hence $c \notin \mathbb{F}_q$. Additionally, equation (13) implies $\zeta^{q^{n/2}} = -\zeta$ and hence

$$\mathrm{Norm}_{q^n/q}(\zeta) = \zeta^{1+q+\ldots+q^{n/2-1}}(-\zeta)\cdot(-\zeta^q)\cdots(-\zeta^{q^{n/2-1}}) = (-1)^{n/2}c^2 = -c^2,$$

i.e., $c^2 \in \mathbb{F}_q$ (whereas $c \notin \mathbb{F}_q$). In other words, c^2 is a non-square in $\mathbb{F}_q$. On the other hand, also -1 is a non-square in $\mathbb{F}_q$ (since $q \equiv 3 \mod 4$ and $n \equiv 2 \mod 4$). Therefore, $\mathrm{Norm}_{q^n/q}(\zeta) = -c^2$ is a square in $\mathbb{F}_q$. □

Now we give the main theorem of this paper.

Theorem 3.6. *Let η be a non-zero element in $\mathbb{F}_{q^n}$ satisfying $\mathrm{Norm}_{q^n/q}(\eta) \neq 1$. Then the following hold.*

1. *If $\eta = 0$, then a generalized twisted Gabidulin code $\mathcal{H}_{n,\frac{n}{2},s}(\eta,h) = \mathcal{G}_{n,\frac{n}{2},s}$ is equivalent to a self-dual MRD code if and only if $n \equiv 2 \mod 4$ and $q \equiv 3 \mod 4$.*
2. *If $\eta \neq 0$, then a generalized twisted Gabidulin code $\mathcal{H}_{n,\frac{n}{2},s}(\eta,h)$ is*
   - *properly equivalent to a self-dual MRD code if and only if $n \equiv 2 \mod 4$, $q \equiv 3 \mod 4$, $h \in \{0, n/2\}$ and $\mathrm{Norm}_{q^n/q}(\eta)$ is a non-square in $\mathbb{F}_q^\star$.*
   - *non-properly equivalent to a self-dual MRD code if and only if $n \equiv 2 \mod 4$, $q \equiv 3 \mod 4$, $h \in \{0, n/2\}$ and $\mathrm{Norm}_{q^n/q}(\eta)$ is a square in $\mathbb{F}_q$.*

Note that the $\eta = 0$ case in Theorem 3.6 is a natural generalization of [10, Theorem 4].

4. Proof of Theorem 3.6

In this section we prove Theorem 3.6 considering the cases separately.

4.1. Case $\eta = 0$.

In this case the proof runs similar to that in [10].

($\Rightarrow$) : Suppose that $\mathcal{G}_{n,\frac{n}{2},s}$ is equivalent to a self-dual MRD code $\mathcal{C}$. Lemma 3.2 says that $\mathcal{G}_{n,\frac{n}{2},s}$ has non-proper automorphisms. Thus $\mathcal{G}_{n,\frac{n}{2},s}$ and $\mathcal{C}$ are properly equivalent without loss of generality. Next, using Lemma 3.4 and Theorem 2.3 we write

$$t(x) \circ (x^{q^s\frac{n}{2}}) \circ \mathcal{G}_{n,\frac{n}{2},s} \circ t^{-1}(x) = a(x) \circ \mathcal{G}_{n,\frac{n}{2},s} \circ b(x),$$

where $[a]_\Gamma, [b]_\Gamma$ are symmetric and $\det[a]_\Gamma, \det[b]_\Gamma \in (\mathbb{F}_q^\star)^2$. Now Corollary 2 implies that

$$\alpha x^{q^i} = a^{-1}(x) \circ t(x) \circ (x^{q^s\frac{n}{2}}) \quad \text{and} \quad \beta x^{q^{-i}} = t^{-1}(x) \circ b^{-1}(x) \tag{14}$$

for some $\alpha, \beta \in \mathbb{F}_{q^n}^\star$ and $0 \leq i \leq n-1$. Then

$$a(x) = t(x) \circ (x^{q^s\frac{n}{2}-i}) \circ (\alpha^{-1}x) \quad \text{and} \quad b(x) = (\beta^{-q^i}x) \circ (x^{q^i}) \circ t^{-1}(x). \tag{15}$$

Since a and b are symmetric, by Lemma 2.4(3) we deduce the following two possibilities:

$$i = 0 \text{ and } \alpha \in \mathbb{F}_{q^{n/2}}^\star, \quad \text{or} \quad i = \frac{n}{2} \text{ and } \beta \in \mathbb{F}_{q^{n/2}}^\star \tag{16}$$

(Recall that s is odd since $\gcd(s,n) = 1$, and that $\beta^{-q^{n/2}} \in \mathbb{F}_{q^{n/2}}^\star$ implies $\beta \in \mathbb{F}_{q^{n/2}}^\star$). Furthermore $\det[a]_\Gamma, \det[b]_\Gamma \in (\mathbb{F}_q^\star)^2$. So we can interpret both possibilities in (16) separately as follows.

- **Subcase 1.** Suppose that $i = 0$ and $\alpha \in \mathbb{F}_{q^{n/2}}^\star$. Then, on the first equation of (15) we observe that

– $\mathrm{Norm}_{q^n/q}(\alpha^{-1}) = [\alpha^{-1}x]_\Gamma$ is a square in $\mathbb{F}_q$, since $\alpha \in \mathbb{F}^\star_{q^{n/2}}$ and by Lemma 2.4(1),
– $\det[t]_\Gamma$ is a non-square in $\mathbb{F}_q$, by Lemma 2.4(1), and
– $\det[x^{q^s\frac{n}{2}}] = (-1)^{\frac{n}{2}}$, by Lemma 2.1(1).

Therefore, to obtain that $\det[a]_\Gamma$ is a square in $\mathbb{F}_q$, we must have that $(-1)^{\frac{n}{2}}$ is a non-square in $\mathbb{F}^\star_q$.

- **Subcase 2.** Suppose that $i = \frac{n}{2}$ and $\beta \in \mathbb{F}^\star_{q^{n/2}}$. Then, on the second equation of (15) we observe similarly that
  – $\mathrm{Norm}_{q^n/q}(\beta^{-q^i})$ is a square in $\mathbb{F}_q$,
  – $\det[t^{-1}]_\Gamma$ is a non-square in $\mathbb{F}_q$, and
  – $\det[x^{q^{\frac{n}{2}}}] = (-1)^{\frac{n}{2}}$.

  Therefore, to obtain that $\det[b]_\Gamma$ is a square in $\mathbb{F}_q$, we must again have that $(-1)^{\frac{n}{2}}$ is a non-square in $\mathbb{F}^\star_q$.

Consequently, we deduce that $(-1)^{n/2} \notin (\mathbb{F}^\star_q)^2$ for both cases and this occurs only if $n \equiv 2 \mod 4$ and $q \equiv 3 \mod 4$.

($\Leftarrow$) : Reverse steps of part ($\Rightarrow$) can be applied to finish the proof.

4.2. CASE $\eta \neq 0$ AND THE EQUIVALENCE IS PROPER. In this case the proof runs similar to the proof of the previous case but we use some additional properties, especially from Lemma 3.1.

($\Rightarrow$) : Suppose that $\mathcal{H}_{n,\frac{n}{2},s}(\eta, h)$ is properly equivalent to a self-dual MRD code $\mathcal{C}$. Then using Lemma 3.4 and Theorem 2.3 we obtain that

$$t \circ (x^{q^s\frac{n}{2}}) \circ \mathcal{H}_{n,\frac{n}{2},s}(-\eta^{q^s\frac{n}{2}-h}, -h) \circ t^{-1} = a \circ \mathcal{H}_{n,\frac{n}{2},s}(\eta, h) \circ b$$

for some invertible linearized polynomials $a(x), b(x) \in \mathcal{L}_n$, where $[a]_\Gamma$ and $[b]_\Gamma$ are symmetric matrices and $\det[a]_\Gamma, \det[b]_\Gamma$ are squares in $\mathbb{F}^\star_q$. Lemma 3.1 implies the equations

$$\alpha x^{q^i} = a^{-1}(x) \circ t(x) \circ (x^{q^s\frac{n}{2}}) \quad \text{and} \quad \beta x^{q^{-i}} = t^{-1}(x) \circ b^{-1}(x)$$

for some $\alpha, \beta \in \mathbb{F}^\star_{q^n}$ and $0 \leq i \leq n-1$. Note that this set of equations is exactly the set of equations in (14) which according to the arguments in Section 4.1 implies that

$$n \equiv 2 \mod 4 \quad \text{and} \quad q \equiv 3 \mod 4. \tag{17}$$

In addition, Lemma 3.1 also implies that $h \in \{0, \frac{n}{2}\}$ and

$$-1 = \alpha^{1-q^h}\beta^{q^s\frac{n}{2}+i-q^{h+i}}\eta^{q^i-q^s\frac{n}{2}-h}. \tag{18}$$

We analyze the possibilities in (16) on equation (18) for $h = 0$ and $h = n/2$ separately as follows.

- **Subcase 1.** Suppose that $h = 0$.
  – **Subcase 1.1.** In case $i = n/2$ and $\beta \in \mathbb{F}^\star_{q^{n/2}}$, equation (18) implies that $-1 = \beta^{1-q^{n/2}} = 1$, a contradiction.
  – **Subcase 1.2.** In case $i = 0$ and $\alpha \in \mathbb{F}^\star_{q^{n/2}}$, we observe from the equations in (15) and Lemma 2.4(1) that $\mathrm{Norm}_{q^n/q}(\beta)$ is a non-square in $\mathbb{F}_q$ since $\det([b]_\Gamma)$ is a square in $\mathbb{F}_q$. On the other hand, equation (18) reduces to $-1 = \beta^{q^{n/2}-1}\eta^{1-q^{n/2}}$. For $\zeta = \beta/\eta$ we get

$$\zeta^{q^{n/2}-1} = -1.$$

Considering (17) and using Lemma 3.5 we deduce that $\mathrm{Norm}_{q^n/q}(\zeta)$ is a square in $\mathbb{F}_q$. Combining both we see that $\mathrm{Norm}_{q^n/q}(\eta) = \dfrac{\mathrm{Norm}_{q^n/q}(\beta)}{\mathrm{Norm}_{q^n/q}(\zeta)}$ is a non-square in $\mathbb{F}_q$.

- **Subcase 2.** Suppose that $h = n/2$.
  - **Subcase 2.1.** In case $i = 0$ and $\alpha \in \mathbb{F}^{\star}_{q^{n/2}}$, equation (18) implies that $-1 = \alpha^{1-q^{n/2}} = 1$, a contradiction.
  - **Subcase 2.2.** In case $i = n/2$ and $\beta \in \mathbb{F}^{\star}_{q^{n/2}}$, we observe from the equations in (15) and Lemma 2.4(1) that $\mathrm{Norm}_{q^n/q}(\alpha)$ is a non-square in $\mathbb{F}_q$. On the other hand, equation (18) reduces to $-1 = \alpha^{1-q^{n/2}}\eta^{q^{n/2}-1}$. Taking $\zeta = \alpha/\eta$ we get
$$\zeta^{q^{n/2}-1} = -1$$
again. Considering (17) and using Lemma 3.5 we deduce that $\mathrm{Norm}_{q^n/q}(\zeta)$ is a square in $\mathbb{F}_q$. Combining both we see that $\mathrm{Norm}_{q^n/q}(\eta) = \dfrac{\mathrm{Norm}_{q^n/q}(\alpha)}{\mathrm{Norm}_{q^n/q}(\zeta)}$ is a non-square in $\mathbb{F}_q$.

($\Leftarrow$) : Reverse steps of part ($\Rightarrow$) can be applied to complete the proof.

4.3. CASE $\eta \neq 0$ AND THE EQUIVALENCE IS NON-PROPER. In this case our proof is similar to the case in Section 4.2 with some differences.

($\Rightarrow$) : Suppose that $\mathcal{H}_{n,\frac{n}{2},s}(\eta, h)$ is non-properly equivalent to a self-dual MRD code $\mathcal{C}$. Then $\widehat{\mathcal{H}}$ and $\mathcal{C}$ are properly equivalent. Using Lemma 3.3 and Theorem 2.3 we get
$$\mathcal{H}^{\perp}_{n,\frac{n}{2},s}\left(\eta^{-q^{-h}}, s\frac{n}{2} - h\right) = a \circ \mathcal{H}_{n,\frac{n}{2},s}\left(\eta^{-q^{-h}}, s\frac{n}{2} - h\right) \circ b$$
and according to Lemma 3.4 we obtain
$$t \circ \left(x^{q^{s\frac{n}{2}}}\right) \circ \mathcal{H}_{n,\frac{n}{2},s}\left(-\eta^{-q^{s\frac{n}{2}-2h}}, h - s\frac{n}{2}\right) \circ t^{-1} = a \circ \mathcal{H}_{n,\frac{n}{2},s}\left(\eta^{-q^{-h}}, s\frac{n}{2} - h\right) \circ b$$
for some invertible linearized polynomials $a(x), b(x) \in \mathcal{L}_n$, where $[a]_\Gamma$ and $[b]_\Gamma$ are symmetric matrices and $\det[a]_\Gamma, \det[b]_\Gamma$ are squares in $\mathbb{F}^{\star}_q$. Then by Lemma 3.1 we obtain that
$$\alpha x^{q^i} = a^{-1}(x) \circ t(x) \circ (x^{q^{s\frac{n}{2}}}) \quad \text{and} \quad \beta x^{q^{-i}} = t^{-1}(x) \circ b^{-1}(x)$$
for some $\alpha, \beta \in \mathbb{F}^{\star}_{q^n}$ and $0 \leq i \leq n-1$, similarly. Note that this set of equations is exactly the set of equations in (14) which according to the arguments in Section 4.1 implies that $n \equiv 2 \mod 4$ and $q \equiv 3 \mod 4$. In addition, Lemma 3.1 also implies that $h \in \{0, \frac{n}{2}\}$ and
$$-1 = \alpha^{1-q^{s\frac{n}{2}-h}}\beta^{q^{s\frac{n}{2}+i}-q^{s\frac{n}{2}+i-h}}\eta^{q^{s\frac{n}{2}}-q^{i-h}}. \tag{19}$$
We analyze the possibilities in (16) on equation (19) for $h = 0$ and $h = n/2$ separately as follows.

- **Subcase 1.** Suppose that $h = 0$.
  - **Subcase 1.1.** In case $i = n/2$ and $\beta \in \mathbb{F}^{\star}_{q^{n/2}}$ we see by equation (15) that $\mathrm{Norm}_{q^n/q}(\alpha)$ is a non-square in $\mathbb{F}_q$. Furthermore equation (19) leads to
$$\alpha^{q^{n/2}-1} = -1.$$

Using Lemma 3.5 we deduce that $\mathrm{Norm}_{q^n/q}(\alpha)$ is a square in $\mathbb{F}_q$, contradiction.

– **Subcase 1.2.** In case $i = 0$ and $\alpha \in \mathbb{F}^{\star}_{q^{n/2}}$, equation (19) reduces to

$$\eta^{q^{n/2}-1} = -1, \tag{20}$$

since $\alpha^{q^{n/2}-1} = 1$. By Lemma 3.5 we deduce that $\mathrm{Norm}_{q^n/q}(\eta)$ is a square in $\mathbb{F}_q$.

- **Subcase 2.** Suppose that $h = n/2$.
  – **Subcase 2.1.** In case $i = 0$ and $\alpha \in \mathbb{F}^{\star}_{q^{n/2}}$ we see by equation (15) that $\mathrm{Norm}_{q^n/q}(\beta)$ is a non-square in $\mathbb{F}_q$. However, equation (19) reduces to

$$\beta^{q^{n/2}-1} = -1.$$

Hence, by Lemma 3.5, $\mathrm{Norm}_{q^n/q}(\beta)$ is a square in $\mathbb{F}_q$, a contradiction.

  – **Subcase 2.2.** In case $i = n/2$ and $\beta \in \mathbb{F}^{\star}_{q^{n/2}}$, equation (19) leads to equation (20), which again means that $\mathrm{Norm}_{q^n/q}(\eta)$ is a square in $\mathbb{F}_q$.

($\Leftarrow$) : Reverse steps of part ($\Rightarrow$) complete the proof.

ACKNOWLEDGMENTS

The research of the first and second authors has been funded by METU Coordinatorship of Scientific Research Projects via grant for projects BAP-01-01-2016-008 and BAP-07-05-2017-007. The first author also has been supported by TÜBİTAK BİDEB via the program 2211A. The third author would like to thank METU for its warm-hearted hospitality and generous financial support during his stay at the University in January 2016. The authors also thank the referees for their insightful and fruitful remarks.

REFERENCES

[1] L. Carlitz, A note on the Betti-Mathieu group, *Portugaliae Math.,* **22** (1963), 121–125.
[2] A. Cossidente, G. Marino and F. Pavese, Non-linear maximum rank distance codes, *Des. Codes Cryptogr.*, **79** (2016), 597–609.
[3] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, *J. Comb. Theory A*, **25** (1978), 226–241.
[4] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. Math.*, **11** (1896), 65–120.
[5] N. Durante and A. Siciliano, Non-linear maximum rank distance codes in the cyclic model for the field reduction of finite geometries, *Electron. J. Comb.,* **24** (2017), Paper 2.33, 18 pp.
[6] E. M. Gabidulin, The theory with maximal rank metric distance, *Probl. Inform. Transm.,* **21** (1985), 1–12.
[7] A. Kshevetskiy and E. Gabidulin, The new construction of rank codes, *Proceedings of Int. Symp. on Inf. Theory,* (ISIT 2005), 2105–2108.
[8] R. Lidl and H. Niederreither, *Introduction to Finite Fields and Their Applications,* Revised Edition, Cambridge University Press, Cambridge, 1994.
[9] G. Lunardon, R. Trombetti and Y. Zhou, Generalized twisted Gabidulin codes, arXiv:1507.07855v2.
[10] G. Nebe and W. Willems, On self-dual MRD codes, *Adv. in Math. of Comm.*, **10** (2016), 633–642.
[11] K. Otal and F. Özbudak, Explicit constructions of some non-Gabidulin linear MRD codes, *Adv. in Math. of Comm.*, **10** (2016), 589–600.
[12] K. Otal and F. Özbudak, Additive rank metric codes, *IEEE Trans. Inf. Theory*, **63** (2017), 164–168.
[13] K. Otal and F. Özbudak, Some new non-additive maximum rank distance codes, *Finite Fields Appl.*, **50** (2018), 293–303.

[14] A. Ravagnani, Rank-metric codes and their duality theory, *Des. Codes Cryptogr.*, **80** (2016), 197–216.
[15] J. Sheekey, A new family of linear maximum rank distance codes, *Adv. in Math. of Comm.*, **10** (2016), 475–488.
[16] Z.-X. Wan, *Geometry of Matrices*, In memory of Professor L.K. Hua (1910-1985), World Scientific, Singapore, 1996.
[17] B. Wu and Z. Liu, Linearized polynomials over finite fields revisited, *Finite Fields Appl.*, **22** (2013), 79–100.

Received June 2017; revised February 2018.

E-mail address: kamil.otal@gmail.com
E-mail address: ozbudak@metu.edu.tr
E-mail address: willems@ovgu.de