ON KERNELS AND NUCLEI OF RANK METRIC CODES

GUGLIELMO LUNARDON\textsuperscript{1}, ROCCO TROMBETTI\textsuperscript{1}, AND YUE ZHOU\textsuperscript{2}

Abstract. For each rank metric code $C \subseteq K^{m \times n}$, we associate a translation structure, the kernel of which is showed to be invariant with respect to the equivalence on rank metric codes. When $K$ is a finite field $\mathbb{F}_q$ and $C$ is a maximum rank distance code with minimum distance $d < \min\{m, n\}$, its kernel is proved to be $\mathbb{F}_q$. For an arbitrary linear rank metric code, we also propose and investigate other two invariants which are called its middle nucleus and right nucleus. For a linear maximum rank distance code in $\mathbb{F}_q^{m \times n}$ with $m \leq n$, we show that its right nucleus must be a finite field under the condition $\max\{d, m - d + 2\} \geq \left\lceil \frac{n}{2} \right\rceil + 1$ and its middle nucleus is always a finite field. For three types of rank metric codes in $\mathbb{F}_2^{n \times n}$ derived from an arbitrary quadratic APN function on $\mathbb{F}_2^n$, we get similar results on their kernels and middle (right) nuclei. For several known maximum rank distance codes, their middle (right) nuclei are calculated.

1. Introduction

Let $K$ be a field. The set $K^{m \times n}$ of all $m \times n$ matrices over $K$ is a $K$-vector space. The rank metric distance on the $K^{m \times n}$ is defined by

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

for $A, B \in K^{m \times n}$, where $\operatorname{rk}(C)$ stands for the rank of $C$.

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

$$d(C) = \min_{A, B \in C, A \neq B}\{d(A, B)\}.$$

When $C$ is a $K$-linear subspace of $K^{m \times n}$, we say that $C$ is a $K$-linear code and its dimension $\dim_K(C)$ is defined to be the dimension of $C$ as a subspace over $K$.

There are several interesting structures in finite geometry, cryptography and coding theory, which can be equivalently described in the context of rank metric codes. First, a quasifield is an algebraic structure with two binary operations which are often called its addition and multiplication. Quasifields are quite similar to skewfields, but with some weaker conditions. Quasifields of finite order are strongly related to translation planes in finite geometry. A quasifield of order $q^n$ with kernel $\mathbb{F}_q$ can be viewed as a subset $C$ of $q^n$ matrices in $\mathbb{F}_q^{n \times n}$ satisfying that the zero matrix is in $C$ and $d(C) = n$. This subset $C$ is often called a spreadset. In particular, when $C$ is $\mathbb{F}_q$-linear, it defines a finite semifield, which is a quasifield with

\textsuperscript{1}Dipartimento di Matematica e Applicazioni “R. Caccioppoli”, Università degli Studi di Napoli “Federico II”, I-80126 Napoli, Italy
\textsuperscript{2}Lehrstuhl für Diskrete Mathematik, Optimierung und Operations Research, Universität Augsburg, 86135 Augsburg, Germany

E-mail addresses: lunardon@unina.it, rtrombet@unina.it, yue.zhou.ovgu@gmail.com.
Date: June 9, 2016.
two-sided distributivity. For more details on quasifields and semifields, we refer to \[15, 16, 20\].

Another interesting topic is from cryptography and coding theory: A function \(f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}\) is called almost perfect nonlinear (abbreviated to APN), if \(\#\{x : f(x + a) + f(x) = b\} = 0\) or \(2\) for all \(a \in \mathbb{F}_{2^n}\) and \(b \in \mathbb{F}_{2^n}\). APN functions are of interest in the design of S-boxes, which are basic components of symmetric key algorithms. Except for the six families of APN monomials, most known families of APN functions are quadratic, i.e. \(f(x) = \sum_{i \leq j} a_{ij}x^{2^i} + 2^j\). It is easy to see that the map given by \(x \mapsto f(x + a) + f(x) + f(a)\) for each nonzero \(a\) can be viewed as a matrix \(M_a\) of rank \(n - 1\) in \(\mathbb{F}_{2}^{n\times n}\). Furthermore, all \(M_a\) together with the zero matrix form a \(\mathbb{F}_2\)-linear code \(C\) in \(\mathbb{F}_{2}^{n\times n}\) and \(d(C) = n - 1\). We refer to \[30\] for a recent survey on APN functions.

Rank metric codes are also useful in the construction of error correcting codes for random network coding and of some transversal designs \[18, 33\].

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 \[9\]. When the equality holds, we call \(C\) a maximum rank distance (MRD for short) code. It is clear that the spreadset derived from a quasifield of order \(q^n\) is an MRD code in \(\mathbb{F}_q^{n\times n}\) and its minimum distance is \(n\). For MRD codes with minimum distance less than \(\min\{m,n\}\), there are a few known constructions. The first and most famous family is due to Gabidulin \[12\] and Delsarte \[9\] who found it independently. This family is later generalized by Kshevetskiy and Gabidulin in \[19\], and we often call them Generalized Gabidulin codes. Recent constructions of MRD codes can be found in \[7, 13, 23, 32\]. Also, in \[24\] some relationship between linear MRD codes and different geometric objects like linear sets of a projective space and generalized Segre varieties were pointed out.

In general, it is difficult to tell whether two rank metric codes with the same parameters are equivalent or not. For quasifields, in particular for semifields, there are several classical invariants such as kernel, left, right and middle nuclei. Originally they are defined as algebraic substructures of quasifields or semifields. However they can also be translated into the language of matrices. For more information on the nuclei of finite semifields, we refer to \[25\]. These invariants are quite useful in telling the equivalence between two semifields, and many classification results on semifields are also based on certain assumptions on the sizes of their nuclei; see \[25, 26, 27, 28\] for instance. Hence it is quite natural to ask whether there are also such invariants for other rank metric codes, especially for MRD codes and the codes derived from quadratic APN functions.

The organization and the main results of this paper are as follows: In Section 2 we introduce several important concepts including the equivalence on rank metric codes together with translation structures. In Section 3 we associate with a rank metric code \(C\) a point-line incidence translation structure \(\mathcal{I}(C)\), i.e., an incidence structure with an equivalence relation defined on the set of lines and with a group acting sharply transitively on its points. We investigate properties of the kernel \(K\) of such an incidence structure. In particular, when \(C\) is an MRD codes in \(\mathbb{F}_q^{n\times n}\) with minimum distance \(d < \min\{m,n\}\), the kernel \(K\) is proved to be \(\mathbb{F}_q^n\). For three types of rank metric codes derived from a quadratic APN function on \(\mathbb{F}_2^n\), we
obtain similar results on their kernels. Then the middle nucleus and right nucleus of a linear rank metric code is introduced and proved to be invariants under codes equivalence in Section 4. Relations between the middle nucleus and the right one of a rank metric code is investigated. We show that the middle nucleus of an MRD code over \( \mathbb{F}_q \) is always a finite field; when \( \max\{d, m - d + 2\} \geq \left\lceil \frac{m}{2} \right\rceil + 1 \), its right nucleus is a finite field. For the codes derived from APN functions on \( \mathbb{F}_{2^n} \) with \( n > 2 \), we get similar results. In Section 5, we determine the middle (right) nuclei of generalized (twisted) Gabidulin codes with \( m = n \). In the end, we introduce the middle nuclei spectrum and the right nuclei spectrum as new invariants of rank metric codes, which could be potentially useful for distinguishing inequivalent codes and calculating their automorphism groups.

2. Preliminaries

In this section, we introduce several important concepts and results on rank metric codes and basic facts on translation structures.

First, let us fix several notations. For any matrix \( M \), we use \( M^t \) to denote the transpose of \( M \) and \( \text{rk}(M) \) is the rank of \( M \). We also use \( 0_{m,n} \) to denote an \( m \times n \) zero matrix over a field. If the numbers of rows and columns are clear from the context, we simply write it as \( 0 \). We always use Latin letters in bold, such as \( x, y, z \) to represent (row) vectors.

Let \( C \) be a rank metric code in \( \mathbb{K}^{m \times n} \). The adjoint code of \( C \) is the code 
\[
C^\top := \{ X^t \mid X \in C \}.
\]

Let \( \langle \cdot, \cdot \rangle \) be the symmetric bilinear form on the set of \( m \times n \) matrices defined by 
\[
\langle M, N \rangle := \text{Tr}(MN^t).
\]
The Delsarte dual code of a \( \mathbb{K} \)-linear code \( C \) is 
\[
C^\perp := \{ M \in \mathbb{K}^{m \times n} : \langle M, N \rangle = 0 \text{ for all } N \in C \}.
\]

One important result proved by Delsarte [9] is that the Delsarte dual code of a linear MRD code is still MRD. Also, if \( d > 1 \), then 
\[
d(C^\perp) = \min\{m, n\} - d + 2.
\]
For the trivial case \( d = 1 \), \( C = \mathbb{K}^{m \times n} \) and \( C^\perp \) consists of a zero matrix.

For any matrix \( M \) over a field \( \mathbb{K} \) and \( \gamma \in \text{Aut}(\mathbb{K}) \), we define \( M^\gamma = (m^\gamma_{ij}) \).

Let \( m, n \) be two integers larger than 1. An isometry on \( \mathbb{K}^{m \times n} \) is a bijection which preserves the rank distance. In [8] Theorem 3.4], it is proved that if \( \varphi \) is an isometry on \( \mathbb{K}^{m \times n} \), then there are \( A \in \text{GL}(m, \mathbb{K}), B \in \text{GL}(n, \mathbb{K}), C \in \mathbb{K}^{m \times n} \) and \( \gamma \in \text{Aut}(\mathbb{K}) \) such that 
\[
\varphi(X) = AX^\gamma B + C
\]
for all \( X \in \mathbb{K}^{m \times n} \), or (when \( m = n \))
\[
\varphi(X) = A(X^t)^\gamma B + C
\]
for all \( X \in \mathbb{K}^{m \times n} \).

As the isometries on \( \mathbb{K}^{m \times n} \) keep the rank distance, following the definition in [5] we should use isometry as the equivalence on rank metric codes. However, for convenience, we use the following two definitions in this paper. Two rank metric
codes $C_1$ and $C_2 \subseteq \mathbb{K}^{m \times n}$ are equivalent if there are $A \in \text{GL}(m, \mathbb{K})$, $B \in \text{GL}(n, \mathbb{K})$, $C \in \mathbb{K}^{m \times n}$ and $\gamma \in \text{Aut}(\mathbb{K})$ such that

\begin{equation}
C_2 = \{ AX^\gamma B + C \mid X \in C_1 \}.
\end{equation}

When $m = n$, we say that $C_1$ and $C_2$ are strongly equivalent if $C_2$ is equivalent either to $C_1$ or to $C_1^T$. Therefore, if $m \neq n$, isometry and equivalence are the same; otherwise $m = n$, isometry is the same as strong equivalence.

An equivalence map from a rank metric code $C$ to itself is called an automorphism. All automorphisms together form the automorphism group of $C$.

When $C_1$ and $C_2$ are linear, by letting $X = 0$ in (4) we see that $C \in C_2$ and $C_2 - C := \{ Y - C : Y \in C_2 \} = C_2$, which means that we may always assume that $C = 0$.

The first example of a linear MRD code of $m \times n$ matrices existing for arbitrary value of the minimum distance $d$, was exhibited by Delsarte in [9] and independently by Gabidulin in [12], and it was later generalized by Kshevetskiy and Gabidulin in [19]. We often call them (generalized) Gabidulin codes.

Precisely, a generalized Gabidulin code is defined as follows: It is well-known that, under a given basis of $F_{q^n}$ over $F_q$, each element $a$ of $F_{q^n}$ can be written as a (column) vector $v(a)$ in $F_q^n$. Let $\alpha_1, \ldots, \alpha_m$ be a set of linear independent elements of $F_{q^n}$ over $F_q$, where $m \leq n$. Then

\begin{equation}
\{ (v(f(\alpha_1)), \ldots, v(f(\alpha_m)))^T : f \in G_{k,s} \}
\end{equation}

is the original generalized Gabidulin code, where

\begin{equation}
G_{k,s} = \{ a_0 x + a_1 x^{q^s} + \ldots a_{k-1} x^{q^{s(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in F_{q^n} \},
\end{equation}

with $n, k, s \in \mathbb{Z}^+$ satisfying $k < n$ and $\gcd(n, s) = 1$. To get the minimum distance of this code, we only have to look at the number of the roots of each $f \in G_{k,s}$.

All members of $G_{k,s}$ are of the form $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$, where $a_i \in F_{q^n}$. 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 $F_q$-linear transformations from $F_{q^n}$ to itself, i.e., elements of $E = \text{End}_{F_q}(F_{q^n})$. We refer to [21] for their basic properties.

A semifield $S$ is an algebraic structure satisfying all the axioms of a skewfield except (possibly) the associative law of multiplication. It is not difficult to show that the additive group of a semifield $S$ is an elementary abelian group; see [17]. The additive order of the nonzero elements in $S$ is called the characteristic of $S$. Hence, any finite semifield can be represented by $(F_q, +, *)$ with a prime power $q$. Here $(F_q, +)$ is the additive group of the finite field $F_q$ and $x * y = \omega(x, y)$, where $\omega$ is a mapping from $F_q \times F_q$ to $F_q$ satisfying that

\begin{align*}
(x + y) * z &= x * z + y * z, \\
x * (y + z) &= x * y + x * z
\end{align*}

for all $x, y, z \in F_q$. That means the map $x \mapsto x * y$ as well as $x \mapsto y * x$ also give rise to two linearized polynomials over a certain subfield of $F_q$. By definition, these two maps must be invertible. Hence, from them we can derive two MRD codes consisting of nondegenerate matrices. For instance, if we take the finite field $F_{p^n}$ which is obviously a semifield, then we can get a set of $p^n$ matrices in $F_{p^n}^{m \times n}$ defined by the (left, right) multiplication in $F_{p^n}$. 
The left, middle and right nucleus of a semifield \( S \) are the following subsets:

\[
N_l(S) = \{ a \in S : (a * x) * y = a * (x * y) \text{ for all } x, y \in S \},
\]

\[
N_m(S) = \{ a \in S : (x * a) * y = x * (a * y) \text{ for all } x, y \in S \},
\]

\[
N_r(S) = \{ a \in S : (x * y) * a = x * (y * a) \text{ for all } x, y \in S \}.
\]

For a rank metric code \( C \in \mathbb{F}_q^{m \times n} \) provided that \( C \) is finite, the rank weight distribution of \( C \) is a sequence of numbers

\[
A_j := \# \{ M : M \in C, \text{rk}(M) = j \}
\]

for \( j = 0, 1, \ldots, \min\{m, n\} \). In general, it is difficult to determine the rank weight distribution of a given code. However, MRD codes with the same parameters have the same rank weight distribution which is completely known. Without loss of generality, we assume that \( m \geq n \) and \( C \) is an MRD code in \( \mathbb{F}_q^{m \times n} \) with minimum distance \( d \). Of course \( A_j = 0 \) for \( j < d \). In [9, 12], it is proved that

\[
A_{d+\ell} = \binom{n}{d+\ell} \sum_{t=0}^{\ell} (-1)^{\ell-t} \binom{\ell}{t} q^{\binom{\ell-t}{2}} q^{m(\ell-t)} - 1,
\]

for \( \ell = 0, 1, \ldots, n - d \), where \( \binom{n}{d} \) is the Gaussian binomial coefficient. As all MRD codes with the same parameters have the same rank distribution, from \( \mathcal{G}_{1,s} \subseteq \mathcal{G}_{2,s} \subseteq \ldots, \mathcal{G}_{n,s} \) we can derive the following result without doing complicated calculation of [7].

**Lemma 2.1.** Let \( C \) be an MRD code in \( \mathbb{F}_q^{m \times n} \) with minimum distance \( d \). Assume that \( 0 \in C \). For any \( 0 \leq \ell \leq n - d \), we have \( A_{d+\ell} > 0 \), i.e. there always exists at least one matrix \( C \in C \) such that \( \text{rk}(C) = d + \ell \).

Finally we turn to the introduction of a particular incidence structure which is called a translation structure.

Let \( P \) be a nonempty set, whose elements are called points, and let \( L \) be a family of subsets of \( P \), whose elements are called lines or blocks. The pair \((P, L)\) forms an incidence structure. A permutation on \( P \) is called a collineation of the incidence structure \((P, L)\), if it is also a permutation on \( L \) and preserves the incidence relation.

An incidence structure \( \mathbb{T} = (P, L) \) with parallelism is a point-line geometry endowed with an equivalence relation defined on the set \( L \) of lines. We denote this relation with the symbol \( || \). A translation of \( \mathbb{T} \) is a collineation \( \tau \) such that \( L' || L \) for all lines \( L \) of \( \mathbb{T} \). The translations of \( \mathbb{T} \) form a group \( T \). We call \((\mathbb{T}, T)\) a translation structure if

(a) the group \( T \) acts sharply transitively on the points of \( \mathbb{T} \);

(b) if \( L \) is a line of \( T \), then the stabilizer \( T_L \) of \( L \) in \( T \) is transitive on the points of \( L \).

The group \( T \) is called the translation group of \( \mathbb{T} \). We say that \( \mathbb{T} \) is a central translation structure when \( T \) is abelian. Two translation structures \( T_1 \) and \( T_2 \) are said to be isomorphic if they are isomorphic as incidence structures, i.e., there is a one-to-one map \( \sigma \) from the points (lines) of \( T_1 \) to the points (lines) of \( T_2 \) such that a point \( x \) is in a line \( L \) if and only if \( \sigma(x) \) is in \( \sigma(L) \).

Translation planes are classical examples of a translation structure in which two points are incident with a unique line. Translation structures were introduced by André in [2]. Also in [2], the following canonical representation is given for \((\mathbb{T}, T)\).
Let \( x \) be a fixed point of \( T \). For any line \( L \) incident with \( x \), define \( T_L = \{ \tau \in T : L \tau = L \} \) and put \( S = \{ T_L : L \text{ is incident with } x \} \).

For each line \( M \) of \( T \) there is an element \( \tau \) of \( T \) and a line \( L \) incident with \( x \) such that \( M = L \tau \). Thus the coset \( T_L \tau \) is the set of the elements of \( T \) which map \( x \) to a point of \( M \) and for each point \( y \) of \( M \) there is exactly one element \( \mu \) of \( T_L \tau \) such that \( x^\mu = y \).

Let \( S(T, S) \) be the point-line structure whose points are the elements of \( T \) and whose lines are the cosets of elements of \( S \). For each point \( y \), let \( \tau_y \) be the element of \( T \) which maps \( x \) to \( y \). Let \( \beta_x \) be the map from \( T \) to \( S(T, S) \) defined by \( y \mapsto \tau_y \) and \( M \mapsto T_L \tau \) if and only if \( M = L \tau \). Then \( \beta_x \) is an isomorphism between \( T \) and \( S(T, S) \). It is worth noticing that the construction does not depend, up to isomorphism, on the choice of the point \( x \).

We say that the incidence structure \( S(T, S) \) satisfies the covering property, if

\[
\bigcup_{x \in L} T_L = T. 
\]

The kernel \( K \) of \( S \) is the set of all endomorphisms \( \kappa \) of \( T \) such that \( T^\kappa \subseteq T \) for all \( L \) incident with \( x \). If \( T \) is abelian, then \( K \) is a ring (not necessarily commutative) with identity. We will use the exponential notation so that the sum and the multiplication of \( K \) are defined by \( \tau^{n+\lambda} = \tau^n \tau^\lambda \) and \( \tau^{\kappa \lambda} = (\tau^\kappa)^\lambda \) for all \( \tau \in T \), and \( \lambda, \kappa \in K \). Then, the group \( T \) is a \( K \)-module and each element of \( S \) is a submodule of \( T \).

The following theorem was known as folklore in the theory of translation structures. However, a proof of it appears only recently in [3, Theorem 5].

**Theorem 2.2.** Let \( T_1, T_2 \) be two translation structures with translation groups \( T_1, T_2 \) respectively, and let \( \beta_x \) be the canonical isomorphism from \( T_1 \) to \( S(T_1, S_1) \), \( (i = 1, 2) \). For each isomorphism \( \alpha \) from \( T_1 \) to \( T_2 \) there is a semilinear map \( \sigma \) from \( T_1 \) to \( T_2 \) such that \( S_1 \alpha = S_2 \) and \( \sigma = \beta_x \alpha \beta_x^{-1} \).

3. **Translation structures from rank metric codes**

In this part, we define a translation structure from a set of \( m \times n \) matrices. Let \( \mathcal{C} \) be a subset of \( \mathbb{K}^{m \times n} \) and \( 0 \) denote the zero vector. We define

\[
S(\infty) := \{ (0, y) : y \in \mathbb{K}^n \}, \\
S(M) := \{ (x, xM) : x \in \mathbb{K}^m \}, \text{ for } M \in \mathcal{C}.
\]

Let \( S(\mathcal{C}) := \{ S(M) : M \in \mathcal{C} \cup \{ \infty \} \} \). From it we derive an incidence structure on \( \mathbb{K}^{m+n} \), in which the lines are defined by

\[
S(M) + (0, b), \text{ for } M \in \mathcal{C}, b \in \mathbb{K}^n, \\
S(\infty) + (a, 0), \text{ for } a \in \mathbb{K}^m.
\]

It is routine to verify that this is a translation structure and the additive group of \( \mathbb{K}^{m+n} \) is its translation group. Let us denote this translation structure by \( \mathcal{F}(\mathcal{C}) \).

According to definition, the kernel \( K \) of \( \mathcal{F}(\mathcal{C}) \) is the set of all endomorphisms of the group \( (\mathbb{K}^{m+n}, +) \) such that \( S(M)^\mu \subseteq S(M) \) for every \( M \in \mathcal{C} \cup \{ \infty \} \). For convenience, we also say that \( K \) is the kernel.

**Lemma 3.1.** Suppose that \( \mathcal{C}_1 \) and \( \mathcal{C}_2 \) are two equivalent rank metric codes in \( \mathbb{K}^{m \times n} \). Then the derived translation structures \( \mathcal{F}(\mathcal{C}_1) \) and \( \mathcal{F}(\mathcal{C}_2) \) are isomorphic. In particular, their kernels \( K_{\mathcal{C}_1} \) and \( K_{\mathcal{C}_2} \) are isomorphic.
Proof. Suppose that \( C_1 \) and \( C_2 \) are equivalent. By definition we have that \( C_2 = \{ AM^nB + C : M \in C_1 \} \) where \( A \in \mathbb{K}^{m \times m} \) and \( B \in \mathbb{K}^{n \times n} \) are nonsingular, \( C \in \mathbb{K}^{m \times n} \) and \( \sigma \in \text{Aut}(\mathbb{K}) \). By Theorem 2.2, the semilinear map

\[
\alpha : (x,y) \in \mathbb{K}^m \times \mathbb{K}^n \mapsto (x^\sigma A^{-1}, y^\sigma B + x^\sigma A^{-1} C) \in \mathbb{K}^m \times \mathbb{K}^n,
\]

is an isomorphism between \( \mathcal{T}(C_1) \) and \( \mathcal{T}(C_2) \) and \( K_{C_2} = \alpha^{-1} K_{C_1} \alpha \).

By the definition of kernel, the following result is easy to get:

**Lemma 3.2.** Let \( I_{m+n} \) denote the identity matrix of order \( m+n \). The set of matrices \( \{ aI_{m+n} : a \in \mathbb{K} \} \), which forms a field isomorphic to \( \mathbb{K} \), belongs to the kernel \( K \) of \( \mathcal{T}(C) \).

By Lemma 3.2, the field \( \mathbb{K} \) is in the kernel \( K \) of \( \mathcal{T}(C) \). It is interesting and natural to ask whether \( K \) is necessarily a field and whether \( K \) contains some extra elements. We proceed to investigate these two questions in the rest part of this section.

**Lemma 3.3.** Assume that the zero matrix is in \( C \). Then each element in the kernel \( K \) of \( \mathcal{T}(C) \) can be expressed in the form

\[
\begin{pmatrix}
N_1 & O_{m,n} \\
O_{n,m} & N_2
\end{pmatrix},
\]

where \( N_1 \in \text{End}(\mathbb{K}^m,+) \), \( N_2 \in \text{End}(\mathbb{K}^n,+) \) and \( O_{m,n} \) (resp. \( O_{n,m} \)) denotes the zero map in \( \text{Hom}(\mathbb{K}^m,+) \) (resp. \( \text{Hom}(\mathbb{K}^n,+) \)).

**Proof.** Let \( \mu \) be an arbitrary element of \( K \). As an endomorphism of the additive group of \( \mathbb{K}^{m+n} \), \( \mu \) can be written as

\[
\begin{pmatrix}
N_1 & N_4 \\
N_3 & N_2
\end{pmatrix},
\]

where \( N_1 \in \text{End}(\mathbb{K}^m,+) \), \( N_2 \in \text{End}(\mathbb{K}^n,+) \), \( N_3 \in \text{Hom}(\mathbb{K}^n,+) \) and \( N_4 \in \text{Hom}(\mathbb{K}^m,+) \). Note that

\[
S(\infty)^\mu = \{ (yN_3, yN_2) : y \in \mathbb{K}^n \}.
\]

Together with \( S(\infty)^\mu \subseteq S(\infty) \), we get \( yN_3 = 0 \) for every \( y \in \mathbb{K}^n \). Hence \( N_3 \) is the zero mapping. Similarly we can also show that \( N_4 = O_{n,m} \) by looking at \( S(0_{m,n})^\mu \subseteq S(0_{m,n}) \).

**Proposition 3.4.** Let \( C \) be a rank metric code containing \( \mathbf{0} \).

(a) Let \( K \) and \( K^\top \) denote the kernels of \( \mathcal{T}(C) \) and \( \mathcal{T}(C^\top) \) respectively. Then

\[
K \cap \text{Aut}(\mathbb{K}^{m+n},+) \cong K^\top \cap \text{Aut}(\mathbb{K}^{m+n},+)
\]

(b) Assume that \( C \) is linear. The group of automorphisms of \( (\mathbb{K}^{m+n},+) \) fixing \( \mathcal{T}(C^\top) \) contains a subgroup which is isomorphic to \( K \cap \text{GL}(m+n,\mathbb{K}) \).

**Proof.** (a). By Lemma 3.3, we know that elements in \( K \cap \text{Aut}(\mathbb{K}^{m+n}) \) can be written as

\[
\begin{pmatrix}
N_1 & O_{m,n} \\
O_{n,m} & N_2
\end{pmatrix},
\]

where \( N_1 \in \text{Aut}(\mathbb{K}^m,+) \) and \( N_2 \in \text{Aut}(\mathbb{K}^n,+) \).

Due to the definition of kernels, for every \( M \in C \) and \( x \in \mathbb{K}^m \),

\[
(x,xM)^\mu = (xN_1,xMN_2) = (y,yN_1^{-1}MN_2) = (y,yM),
\]

for some \( y \in \mathbb{K}^n \). Thus \( (x,xM)^\mu \) is fixed by \( K \cap \text{Aut}(\mathbb{K}^{m+n}) \) and \( x \) is automatically fixed by \( K \cap \text{Aut}(\mathbb{K}^{m+n}) \).
where $y = xN_1$. Hence
\[ N_1^{-1}MN_2 = M, \]
which implies that
\[ N_2^tM^t(N_1^t)^{-1} = M^t. \]
Hence
\[ \mu' := \begin{pmatrix} (N_2^t)^{-1} \\ (N_1^t)^{-1} \end{pmatrix} \]
is in the kernel of $\mathcal{F}(C^\top)$. Therefore the map $\mu \mapsto \mu'$ is a bijection on the kernels of $\mathcal{F}(C)$ and $\mathcal{F}(C^\top)$.

(b). By Lemma 3.3, we know that elements in $K \cap \text{GL}(m + n, \mathbb{K})$ can be written as
\[ \begin{pmatrix} N_1 & O_{m,n} \\ O_{n,m} & N_2 \end{pmatrix}, \]
where $N_1 \in \text{GL}(m, \mathbb{K})$ and $N_2 \in \text{GL}(n, \mathbb{K})$.

By definition, we again have $N_1^{-1}MN_2 = M$.

Hence
\[ \text{Tr}(M((N_1^t)^{-1}NN_2^t)^t) = \text{Tr}(MN_2N_1^tN_1^{-1}) = \text{Tr}(N_1^{-1}MN_2^t) = \text{Tr}(M^t) = 0, \]
for each $M \in \mathcal{C}$ and $N \in \mathcal{C}^\perp$. Therefore, the map given by $N \mapsto (N_1^t)^{-1}NN_2^t$ is a group automorphism fixing $\mathcal{F}(C^\perp)$.

\[ \square \]

**Theorem 3.5.** Assume that a rank metric code $\mathcal{C}$ contains the zero matrix and
\[ \{xM : M \in \mathcal{C}\} = \mathbb{K}^n \]
for each nonzero $x \in \mathbb{K}^m$. Then the kernel $K$ of $\mathcal{F}(\mathcal{C})$ is a skewfield and each element of $K$ can be expressed in the form
\[ \begin{pmatrix} N_1 \\ N_2 \end{pmatrix}, \]
with $N_1 \in \text{Aut}((\mathbb{K}^m, +))$ and $N_2 \in \text{Aut}((\mathbb{K}^n, +))$. In particular, if $\mathbb{K}$ is finite, then the kernel $K$ is a finite field containing $\mathbb{K}$, $N_1 \in \text{GL}(m, \mathbb{K})$ and $N_2 \in \text{GL}(n, \mathbb{K})$.

**Proof.** Let $\mu$ be an arbitrary element of $K$. By Lemma 3.3, $\mu$ can be written in the form
\[ \begin{pmatrix} N_1 & O_{m,n} \\ O_{n,m} & N_2 \end{pmatrix}, \]
where $N_1 \in \text{End}((\mathbb{K}^m, +))$ and $N_2 \in \text{End}((\mathbb{K}^n, +))$.

**Claim:** Suppose that $\mu$ does not map all elements in $\mathbb{K}^{m \times n}$ to the zero vector. Then $N_2$ is not the zero map.

By way of contradiction, we assume that $N_2 = O_{n,n}$. Then we get
\[ S(M)^n = \{(xN_1, 0) : x \in \mathbb{K}^m\} \subseteq S(M), \]
for all $M \in \mathcal{C}$. It implies that $yM = 0$ for each $y \in \{xN_1 : x \in \mathbb{K}^m\}$ and any $M \in \mathcal{C}$. As $N_1 \neq O_{m,m}$, there exists a nonzero vector $z \in \{xN_1 : x \in \mathbb{K}^m\}$. Thus $\{zM : M \in \mathcal{C}\} = \{0\}$. It contradicts (10).
Next we proceed to show that both $N_1$ and $N_2$ are bijection. By way of contradiction, let us assume that $N_1$ is not invertible. There exists a nonzero vector $x \in \mathbb{K}^n$ such that $xN_1 = 0$. Thus, for any $M \in C$,
\[(xN_1, (xM)N_2) = (0, 0),\]
because of $S(M)^\mu \subseteq S(M)$. By (10), we see that $N_2$ must be the zero map which contradicts the proved claim.

Now we know that $N_1$ is invertible. Hence, for any nonzero vector $x$, the vector $y := xN_1$ is also nonzero. Again from $S(M)^\mu \subseteq S(M)$, we get
\[(xN_1, xMN_2) = (y, xMN_2) = (y, yM).\]
By the above equation, we see that the set $\{xMN_2 : M \in C\}$ and $\{yM : M \in C\}$ must be the same. By (10), we further obtain that
\[\mathbb{K}^n = \{xMN_2 : M \in C\} = \{zN_2 : z \in \mathbb{K}^n\}.\]
That means $N_2$ is also invertible.

To summarize, we have proved that $\mu \in K$ is always invertible. Together with the fact that $K$ is a ring, we show that $K$ is a skewfield.

When $\mathbb{K}$ is finite, it is clear that $K$ is also finite. Hence $K$ is a finite field. By Lemma 3.2 the set of matrices $\{aI_{m+n} : a \in \mathbb{K}\}$ forms a subfield of $K$ and $\mu$ is now also a $\mathbb{K}$-homomorphism of the vector space $\mathbb{K}^{m+n}$. Therefore $N_1$ and $N_2$ are both nondegenerate matrices over $\mathbb{K}$.

In fact, when (10) does not hold, there exist rank metric codes $C \subseteq \mathbb{K}^{m \times n}$ such that the kernel $K$ of $\mathbb{T}(C)$ is not a skewfield.

**Example 3.6.** Let $C$ be a set of matrices, each of which satisfies that the entries in its last row and last column are all 0. It is straightforward to verify that $\mathbb{T}(C)$ does not satisfy the covering property and its kernel $K$ contains the matrices
\[L_{a,b} = \begin{pmatrix} a & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & 0 \\ 0 & \cdots & a & 0 \\ 0 & 0 & 0 & b \end{pmatrix}\]
for $a, b \in \mathbb{K}$. As $L_{a,0}, L_{0,b}$ equals the zero matrix, its kernel $K$ cannot be a skewfield.

By Proposition 3.4 (a) and Theorem 3.5, we can directly get the following result.

**Corollary 3.7.** Let $C$ be a rank metric code in $\mathbb{K}^{m \times n}$. Assume that $C$ contains the zero matrix and (10) holds for $C$. Then there is a bijection between the kernels of $\mathbb{T}(C)$ and $\mathbb{T}(C^\top)$.

**Corollary 3.8.** Let $C_1$ and $C_2$ be in $\mathbb{K}^{m \times n}$. Assume that both $C_1$ and $C_2$ contain the zero matrix and (10) holds for $C_1$ and $C_2$. Suppose that $C_1$ is strongly equivalent to $C_2$. Then their kernels are of the same size.

**Proof.** If $C_1$ is equivalent to $C_2$, then the result follows directly from Lemma 3.1 if $C_1$ is equivalent to $C_2^\top$, then its kernel $K_{C_1}$ is isomorphic to the kernel $K_{C_2}$ of $\mathbb{T}(C_2^\top)$. Together with Corollary 3.7 we see that the kernels of $\mathbb{T}(C_1)$ and $\mathbb{T}(C_2)$ are of the same size.
3.1. Kernel of MRD codes. Now let us investigate the kernel of an MRD code over a finite field.

**Theorem 3.9.** Let $\mathcal{C}$ be an MRD codes in $\mathbb{F}_q^{m \times n}$. Then $\mathcal{V}(\mathcal{C})$ satisfies the covering property, i.e., for any nonzero vector $x \in \mathbb{F}_q^m$ and any $y \in \mathbb{F}_q^n$, there is at least one matrix $M \in \mathcal{C}$ such that $xM = y$.

**Proof.** Without loss of generality, we assume that $x = (1,0,\ldots,0)$; otherwise we choose an invertible matrix $L$ such that $xL = (1,0,\ldots,0)$ and left multiply its inverse matrix $L^{-1}$ by $M \in \mathcal{C}$ to get another MRD code.

Assume, by way of contradiction, that there is an element $y \in \mathbb{F}_q^n$ such that $xM \neq y$ for all $M \in \mathcal{C}$. Suppose that the minimum rank distance of $\mathcal{C}$ is $d$ and $m \leq n$. It means that there are $q^{n(m-d+1)}$ matrices in $\mathcal{C}$.

For each $z \in \mathbb{F}_q^n$, we take $U_z := \{ M \in \mathcal{C} : xM = z \}$. It is clear that

$$\sum_{z \in \mathbb{F}_q^n} \#U_z = q^{n(m-d+1)},$$

and

$$\#U_y = 0.$$

From them, we can derive that

$$\max_{z \in \mathbb{F}_q^n}\{ \#U_z \} \geq \frac{q^{n(m-d+1)}}{q^n - 1} > q^{n(m-d)}.$$

Let $\bar{z}$ be the vector such that $\#U_{\bar{z}} = \max_{z \in \mathbb{F}_q^n}\{ \#U_z \}$.

Now let us look at the matrices in $U_{\bar{z}}$. As $x = (1,0,\ldots,0)$, the first row of each $M \in U_{\bar{z}}$ equals $\bar{z}$. By (12), there must exist two matrices $M$ and $M'$ in $U_{\bar{z}}$ such that the first $m - d + 1$ rows are the same. It follows that the rank of $M - M'$ is at most $d - 1$, which contradicts the assumption that $\mathcal{C}$ is an MRD code.

For the $m > n$ case, we can similarly prove that there exist two matrices $M$ and $M'$ in which the first $\lfloor \frac{m}{n} (n-d)+1 \rfloor$ are the same, which contradicts the minimum distance of $\mathcal{C}$. \qed

Theorem 3.9 can also be derived from the fact that any MRD code of $\mathbb{F}_q^{m \times n}$ with minimum distance $d$ is an $(n-d+1)$-design of index 1 in $\mathbb{F}_q^{m \times n}$; see [9, Section 5] for more details.

**Corollary 3.10.** Let $\mathcal{C}$ be an MRD code in $\mathbb{F}_q^{m \times n}$ such that $d < \min\{m,n\}$. Then, the kernel $K$ of $\mathcal{V}(\mathcal{C})$ is $\mathbb{F}_q$.

**Proof.** By Lemma 3.2, $K$ contains a subfield isomorphic to $\mathbb{F}_q$. By Theorems 3.9 and 3.9, we know that $K$ is a finite field. Let us say $K = \mathbb{F}_{q^r}$ for a positive integer $r$. According to the definition of a kernel, all $S(M)$ can be viewed as a vector space over $K$. That means each matrix $M$ in $\mathcal{C}$ can also be viewed as a matrix over $\mathbb{F}_{q^r}$. It implies that $r$ divides $m$ and $n$. However, by Lemma 2.1, there exist matrices of rank $\min\{m,n\}$ and $\min\{m,n\} - 1$ in $\mathcal{C}$. Therefore $r$ must be 1. \qed

It is worth pointing out that when $\min\{m,n\} = d$, the kernel of $\mathcal{V}(\mathcal{C})$ can be strictly larger than $\mathbb{F}_q$. For instance, when $m = n = d$, an MRD code $\mathcal{C}$ is exactly a semifield, and the kernel of $\mathcal{V}(\mathcal{C})$ corresponds to the so-called left nucleus of the semifield. There always exist semifields of order $q^m$ with left nucleus larger than $q$; for instance the famous Albert’s twisted fields [11, 4].
When \( C \) is not an MRD code, there are also examples whose kernels are strictly larger than \( \mathbb{F}_q \).

**Example 3.11.** Let \( n = 4 \). Let \( C \) be a set of \( 4 \times 4 \) matrices over \( \mathbb{F}_q \) derived form the following set of linearized polynomials in \( \mathbb{F}_q[X] \):

\[
\{a_0X + a_1X^q : a_0, a_1 \in \mathbb{F}_q^4\}.
\]

Let \( c \) be an element of \( \mathbb{F}_q^2 \). For any \( a_0, a_1, x \in \mathbb{F}_q^n \), we always have

\[
a_0(cx) + a_1(cx)q^2 = c(a_0x + a_1xq^2).
\]

It implies that \( \mathbb{F}_q^2 \) is a subfield of the kernel of \( C \).

### 3.2. Kernels of APN functions.

In the final part of this section, we proceed to look at the kernels of three translation structures derived from a quadratic APN function.

Let \( f \) be a function on \( \mathbb{F}_2^n \) defined by

\[
f(x) = \sum_{i<j} a_{ij} x^i y^j.
\]

We define

\[
B_f(x, y) := f(x + y) + f(x) + f(y).
\]

If \( y \) is fixed and \( x \) is viewed as an indeterminate, then \( B_f(x, y) \) is a linearized polynomial in \( x \).

For any \( a \in \mathbb{F}_2^n \), the map given by \( x \mapsto B_f(x, a) \) is additive on \( \mathbb{F}_2^n \), which means that under a basis of \( \mathbb{F}_2^n \) over \( \mathbb{F}_2 \), this map can be expressed as a matrix \( M_a \in \mathbb{F}_2^{n \times n} \). Meanwhile, each \( a \in \mathbb{F}_2^n \) is uniquely mapped to a vector \( a \) in \( \mathbb{F}_2^n \). In the rest of this section, we follow this way to denote the corresponding elements of \( x, y, z, \cdots \in \mathbb{F}_2^n \) by \( x, y, z, \cdots \in \mathbb{F}_2^n \).

When \( f \) is APN and \( a \neq 0 \), the rank of \( M_a \) is \( n - 1 \). It is also easy to check that \( M_a + M_b = M_{a+b} \). Hence the set

\[
C_f := \{M_a : a \in \mathbb{F}_2^n\}
\]

is a linear code in \( \mathbb{F}_2^{n \times n} \).

To investigate the kernels of \( C_f \) and \( C_f^\top \) for quadratic APN functions \( f \), we need to introduce several concepts and lemmas.

For a \( q \)-polynomial \( f = \sum_{i=0}^{n-1} a_i X^q^i \in \mathbb{F}_q^n[X] \), its *adjoint* is defined by \( \hat{f} := \sum_{i=0}^{n-1} a_{q^n-i} X^{q^n-i} \). Let \( \text{Tr} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q \) be the trace map. It is not difficult to check that, for any \( x, y \in \mathbb{F}_q^n \),

\[
\text{Tr}(xf(y) - y\hat{f}(x)) = 0.
\]

For \( a, b, c, d \in \mathbb{F}_q^n \), if we consider a basis \( \mathcal{B} \) of \( \mathbb{F}_q^n \) over \( \mathbb{F}_q \), then \( a, b, c, d \) can be written as four vectors \( a, b, c, d \) in \( \mathbb{F}_q^n \) and

\[
\langle (a, b), (c, d) \rangle := \text{Tr}(ad - bc)
\]

defines a nondegenerate alternating bilinear form. If we choose \( \mathcal{B} \) to be a trace-orthogonal basis, then \( \langle (a, b), (c, d) \rangle = a \cdot d - b \cdot c \) where \( \cdot \) is the usual dot product of vectors. Let \( M \) and \( N \) be two \( n \times n \) matrices over \( \mathbb{F}_q \) corresponding to \( f \) and \( \hat{f} \) respectively. The \( n \)-dimensional subspaces \( \{(x, xM) : x \in \mathbb{F}_q^n\} \) and \( \{(x, xN) : x \in \mathbb{F}_q^n\} \) are orthogonal if and only if \( M = N^T \), since \( \langle (x, xM), (y, yN) \rangle = xN^Ty^T - xM^Ty^T \).
\[ xMy^t = x(N^T - M)y^t. \] Therefore \( \hat{f} \) corresponds to a transpose of the matrix defined by \( f \) over \( \mathbb{F}_q \), \( f = \hat{f} \) if and only if the matrix \( M \) is symmetric.

Similarly to the adjoint of a linearized polynomial, we can also show that there exists a unique \( \hat{B}_f(X, Y) \in \mathbb{F}_{2^n}[X, Y]/(X^{2^k} - X, Y^{2^k} - Y) \) such that

\[
\text{Tr}(zB_f(x, y)) = \text{Tr}(x\hat{B}_f(z, y)) = \text{Tr}(y\hat{B}_f(z, x)),
\]

for all \( x, y, z \in \mathbb{F}_{2^n} \). By definition, the map given by \( z \mapsto \hat{B}_f(z, a) \) corresponds to \( M_a^t \). It is also direct to check that the matrix defined by the map \( y \mapsto \hat{B}_f(z, y) \) is symmetric for each \( z \). We can also equivalently write this map as \( y \mapsto zM_y^t \). For convenience, we use \( \tilde{M}_z \) to denote the matrix derived from the linear map \( y \mapsto zM_y^t \), i.e. \( zM_y^t = y\tilde{M}_z \).

In fact, it is straightforward to verify that the matrix defined by the linear map \( y \mapsto \hat{B}_f(z, y) \) is equivalent to the matrix derived by the alternating bilinear forms \( \text{Tr}(zB_f(x, y)) \) for every \( z \).

To summarize, the two maps given by \( y \mapsto \hat{B}_f(z, y) \) and \( y \mapsto zM_y^t \) respectively, and the alternating bilinear form \( \text{Tr}(zB_f(x, y)) \) are essentially different representations of a same object. By symmetry,

\[
\text{Tr}(y\hat{B}_f(z, y)) = zM_y^t \cdot y = y\tilde{M}_z y^t = 0,
\]

for any \( y \) and \( z \in F_2^n \).

In [11], Edel investigated the \( F_2 \)-linear space \( \mathcal{B}_f := \{ \text{Tr}(zB_f(x, y)) : z \in \mathbb{F}_{2^n} \} \) and obtained the following results.

**Lemma 3.12.** Let \( f \) be a quadratic APN functions over \( \mathbb{F}_{2^n} \).

(a) The dimension of \( \mathcal{B}_f \) over \( \mathbb{F}_2 \) is \( n \).

(b) When \( n \) is odd, every matrix \( \tilde{M}_a \) derived from the alternating bilinear form in \( \mathcal{B}_f \) is of rank \( n - 1 \);

(c) When \( n \) is even, there are more than \( 2^{n-1} \) nondegenerate elements in \( \mathcal{B}_f \). Hence there is a basis of \( \mathcal{B}_f \) consisting of nondegenerate alternating bilinear forms.

By Lemma 3.12, we can prove the following results.

**Lemma 3.13.** Let \( f \) be a quadratic APN function on \( \mathbb{F}_{2^n} \). Then

\[
\# \{ B_f(x, a) : x, a \in \mathbb{F}_{2^n} \} > 2^{n-1}, \tag{13}
\]

and

\[
\# \{ \hat{B}_f(x, a) : x, a \in \mathbb{F}_{2^n} \} > 2^{n-1}. \tag{14}
\]

**Proof.** By definition, \( H_a := \{ B_f(x, a) : x \in \mathbb{F}_{2^n} \} \) is an \( (n - 1) \)-dimensional subspace of \( \mathbb{F}_2^n \) for each nonzero \( a \).

By way of contradiction, let us assume that all \( H_a \) are the same for all nonzero \( a \), i.e., \( \# \{ B_f(x, a) : x, a \in \mathbb{F}_{2^n} \} = 2^{n-1} \). That means there exists a nonzero element \( b \in \mathbb{F}_{2^n} \), such that

\[
\text{Tr}(bB_f(x, y)) = 0
\]

for all \( x \) and \( y \) in \( \mathbb{F}_{2^n} \). However it implies that the dimension of \( \mathcal{B}_f \) is at most \( n - 1 \) over \( \mathbb{F}_2 \), which contradicts Lemma 3.12 (a). By a similar argument, (14) can also be obtained. \( \square \)

Next we look at the kernels of \( \mathcal{I}(C_f) \) and \( \mathcal{I}(C_f^\top) \).
Theorem 3.14. Let $f$ be a quadratic APN function on $\mathbb{F}_2^n$ with $n > 2$. Then the kernels $K_{C_f}$ and $K_{C_{f'}}$ of the translation structures $\mathcal{T}(C_f)$ and $\mathcal{T}(C_{f'})$ both equal $\mathbb{F}_2$.

Proof. We only prove the result for $\mathcal{T}(C_{f'})$. By a similar argument, one can prove the theorem for $\mathcal{T}(C_f)$. We will also see another simple proof for $\mathcal{T}(C_f)$ in the next section.

It is clear that the kernel $K_{C_{f'}}$ of $\mathcal{T}(C_{f'})$ contains $\mathbb{F}_2$, i.e. the zero map and the identity map. Let $F$ be the largest field in $K_{C_{f'}}$ and $m = \log_2(\#F)$. As the ranks of $M_a$ are all $n - 1$ for nonzero $a$ and $M_a$ can be viewed as a vector space over $F$, $m$ should divide $n$ and $n - 1$. Hence $F = \mathbb{F}_2$ and there is no other bijection in $K_{C_{f'}}$.

Now we have to show that there is also no degenerate map in $K_{C_{f'}}$. By Lemma 3.3 for an arbitrary element $\mu$ of $K_{C_{f'}}$, $\mu$ can be written as a $2n \times 2n$ matrix

$$
\begin{pmatrix}
N_1 & 0 \\
0 & N_2
\end{pmatrix}
$$

over $\mathbb{F}_2$, where $N_1, N_2 \in \mathbb{F}_2^{n \times n}$.

Similarly as in the proof of Theorem 3.5, we can prove the following claim.

Claim 1: Suppose that $\mu$ does not map all elements in $\mathbb{F}_2^{n \times n}$ to the zero vector. Then $N_2$ is not the zero matrix in $\mathbb{F}_2^{n \times n}$.

By way of contradiction, we assume $N_2 = 0_{n,n}$. Then we get

$$
S(M_a^t)^a = \{(xN_1, 0) : x \in \mathbb{F}_2^n\} \subseteq S(M_a^t),
$$

for all $M_a \in C_f$. It implies that

$$
yM_a^t = 0
$$

for each $y \in \{xN_1 : x \in \mathbb{F}_2^n\}$ and any $M_a \in C_f$. As $\mu$ is not the zero mapping, there exist a nonzero $b$ in $\{xN_1 : x \in \mathbb{F}_2^n\}$. Together with (16), we have

$$
bM_a^t x^t = b \cdot (xM_a) = 0,
$$

for all $a \in \mathbb{F}_{2^n}$ and $x \in \mathbb{F}_2^n$. By (13), we know that

$$
\# \{xM_a : x, a \in \mathbb{F}_{2^n}\} > 2^{n-1},
$$

which means that $b$ must be $0$. It is a contradiction.

Claim 2: If $\mu$ is not a permutation, then $N_1$ and $N_2$ are both degenerate.

By $S(M_a^t)^a \subseteq S(M_a^t)$, we have

$$
xM_a^t N_2 = xN_1 M_a^t,
$$

for all $x$ and $a$. Hence

$$
\# \{xM_a^t N_2 : x, a \in \mathbb{F}_2^n\} = \# \{xN_1 M_a^t : x \in \mathbb{F}_2^n, a \in \mathbb{F}_{2^n}\}.
$$

By (14), we have

$$
\# \{xM_a^t : x \in \mathbb{F}_2^n, a \in \mathbb{F}_{2^n}\} = \# \{\tilde{B}_f(x, a) : x, a \in \mathbb{F}_{2^n}\} > 2^{n-1}.
$$

Thus $N_1$ must be degenerate; otherwise by (14), $N_2$ is also nondegenerate and $\mu$ is a permutation, which contradicts the assumption.

As $N_1$ is degenerate, there exists nonzero vector $x$ such that $xN_1 = 0$ and (18) becomes

$$
xM_a^t N_2 = 0 M_a^t = 0,
$$

for all $x$ and $a$. Hence

$$
\# \{xM_a^t N_2 : x, a \in \mathbb{F}_2^n\} = \# \{xN_1 M_a^t : x \in \mathbb{F}_2^n, a \in \mathbb{F}_{2^n}\}.
$$

By (14), we have

$$
\# \{xM_a^t : x \in \mathbb{F}_2^n, a \in \mathbb{F}_{2^n}\} = \# \{\tilde{B}_f(x, a) : x, a \in \mathbb{F}_{2^n}\} > 2^{n-1}.
$$

Thus $N_1$ must be degenerate; otherwise by (14), $N_2$ is also nondegenerate and $\mu$ is a permutation, which contradicts the assumption.

As $N_1$ is degenerate, there exists nonzero vector $x$ such that $xN_1 = 0$ and (18) becomes

$$
xM_a^t N_2 = 0 M_a^t = 0,
$$

for all $x$ and $a$. Hence

$$
\# \{xM_a^t N_2 : x, a \in \mathbb{F}_2^n\} = \# \{xN_1 M_a^t : x \in \mathbb{F}_2^n, a \in \mathbb{F}_{2^n}\}.
$$

By (14), we have

$$
\# \{xM_a^t : x \in \mathbb{F}_2^n, a \in \mathbb{F}_{2^n}\} = \# \{\tilde{B}_f(x, a) : x, a \in \mathbb{F}_{2^n}\} > 2^{n-1}.
$$

Thus $N_1$ must be degenerate; otherwise by (14), $N_2$ is also nondegenerate and $\mu$ is a permutation, which contradicts the assumption.
for all $a$. Assume, by way of contradiction, that $N_2$ is nondegenerate. It follows that the map $a \mapsto xM_a^t$, i.e. $aM_a$ or $B_f(x, a)$ is constantly zero. Hence the map $a \mapsto B_f(x, a)$ defines a zero matrix in $\mathbb{F}_2^{n \times n}$. However it implies that the dimension of $B_f$ is at most $n - 1$ over $\mathbb{F}_2$, which contradicts Lemma 3.12 (a). This concludes the proof of Claim 2.

Now we assume that $\mu$ is neither a permutation nor the zero map. By Claim 1, we know that $N_2 \neq 0$. From (19), we deduce that
\[ \# \{ xM_a^t : x \in \mathbb{F}_2^n, a \in \mathbb{F}_2^n \} > 0. \]
Together with (19), we see $N_1 \neq 0$.

By Claim 2, $N_2$ is degenerate. Hence there exists a nonzero vector $z$ such that $N_2z^t = 0$. By (18), we have
\[ 0 = xM_a^tN_2z = xN_1M_a^tz = xN_1(zM_a)^t, \]
for any $x$ and $a$. Noting that the map $a \mapsto zM_a$ corresponds exactly to the matrix derived from $B_f(a, z)$, we get $\{ zM_a : a \in \mathbb{F}_2^n \} = 2^{n-1}$. It means that $xN_1$ can only take at most one nonzero value. Since $N_1 \neq 0$, we see that $\text{rk}(N_1) = 1$.

In the end, let us consider the sum of the identity matrix $I_{2n, 2n}$ and a non-bijective map $\mu \in K_{\tilde{C}_f^\ast}$, where
\[ \mu = \begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix}. \]
Recall that at the very beginning of this proof, we have shown that $I_{2n, 2n}$ is the unique invertible matrix in $K_{\tilde{C}_f^\ast}$. As the kernel is closed under addition, $I_{2n, 2n} + \mu$ must be in $K_{\tilde{C}_f^\ast}$ and $\text{rk}(N_1 + I_{n, n}) = 1$. However, as a full-rank matrix, $I_{n, n}$ cannot be written as a sum of two matrices of rank 1, because $n > 2$. Therefore there is no such $\mu \in K_{\tilde{C}_f^\ast}$ and $K_{\tilde{C}_f^\ast} = \mathbb{F}_2$.

Let us define
\[ \tilde{C}_f := \{ \tilde{M}_z : z \in \mathbb{F}_2^n \}, \]
which is also a linear rank metric code in $\mathbb{F}_2^{n \times n}$. It is natural to ask what is the kernel of $\mathcal{F}(\tilde{C}_f)$. By an analogous approach in the proof of Theorem 3.14, we can show that its kernel $K_{\tilde{C}_f^\ast}$ is a field. By Lemma 3.12, we can further prove $K_{\tilde{C}_f^\ast} \cong \mathbb{F}_2$ for odd $n$. In next section, we will give a short proof of it and further show that $K_{\tilde{C}_f^\ast} \cong \mathbb{F}_2$ or $\mathbb{F}_4$ for even $n$.

4. Nuclei of a Rank Metric Code

Let $C \subseteq \mathbb{K}^{m \times n}$ be a linear rank metric code. We define the *middle nucleus* of $C$ as the following set of matrices of order $n$:
\[ N_m(C) = \{ Z \in \mathbb{K}^{m \times m} : ZC \in C \text{ for all } C \in C \}. \]
In the same way we say that the *right nucleus* of $C$ is the following set:
\[ N_r(C) = \{ Y \in \mathbb{K}^{n \times n} : CY \in C \text{ for all } C \in C \}. \]

In particular, when $C$ defines a finite semifield $\mathbb{S}$, $N_m(C)$ (resp. $N_r(C)$) is exactly the middle (resp. right) nucleus of $\mathbb{S}$. In [22], the middle nucleus (resp. right nucleus) is called left (resp. right) *idealiser* of $C$.

It is straightforward to note that these sets define two subgroups of the automorphism group of the translation structure $\mathcal{F}(C)$ fixing $S(0)$ and $S(\infty)$, respectively.
The middle and right nuclei of semifields are invariants under isotopism, which is the most widely investigated equivalence on semifields. They also play very important roles in distinguishing and the classification of semifields. Hence, it is natural to consider their properties for general rank metric codes.

**Proposition 4.1.** For two equivalent linear rank metric codes \( C_1 \) and \( C_2 \) in \( \mathbb{K}^{m \times n} \), their right (resp. middle) nuclei are also equivalent.

**Proof.** Suppose that \( C_1 \) and \( C_2 \) are equivalent. By definition this means that there exists \( \gamma \in \text{Aut}(\mathbb{K}) \), \( A \in \text{GL}(m, \mathbb{K}) \) and \( B \in \text{GL}(n, \mathbb{K}) \) such that

\[
C_2 = \{ AM^\top B : M \in C_1 \}.
\]

An element \( Z \in \mathbb{K}^{m \times m} \), belongs to the middle nucleus \( N_m(C_1) \) if and only if \( AZ^\top A^{-1} \) belongs to \( N_m(C_2) \); this means that \( N_m(C_1) \) and \( N_m(C_2) \) are also equivalent. A similar argument can be used to prove that also \( N_r(C_1) \) is equivalent to \( N_r(C_2) \). This concludes the proof. \( \square \)

Of course, we can also define middle and right nuclei for nonlinear codes. However, through the proof of Proposition 4.1 we see that the nuclei of nonlinear codes are not necessarily invariants under the isometry. Therefore, in the rest of this section, we are only interested in linear rank metric codes.

As \( C \) is \( \mathbb{K} \)-linear, it is routine to verify that \( N_m(C) \) and \( N_r(C) \) are subrings of \( \mathbb{K}^{m \times m} \) and \( \mathbb{K}^{n \times n} \), respectively. Moreover, they both contain the zero map and \( \mathbb{K} \) as a subfield. Hence, the code \( C \) can be seen as a left module (resp. a right module) over \( N_m(C) \) (resp. \( N_r(C) \)).

Regarding the adjoint and Delsarte dual operation we have the following results.

**Proposition 4.2.** Let \( C \) be a linear rank metric code in \( \mathbb{K}^{m \times n} \). Let \( C^\top \) (resp. \( C^\perp \)) be the adjoint (resp. Delsarte dual) code of \( C \). Then the following statements hold:

(a) \( N_m(C^\top) = N_r(C^\top) = N_m(C)^\top \)
(b) \( N_m(C^\perp) = N_r(C^\perp) = N_m(C)^\perp \)

**Proof.** By definition, (a) can be readily verified.

For (b), we first observe that if \( Z \in N_m(C) \) then \( Z^t \) belongs to \( N_m(C^\perp) \); indeed, let \( N \in C^\perp \), i.e., \( \text{Tr}(CN^t) = 0 \) for all \( C \in C \). We have

\[
\text{Tr}(C(Z^tN)^t) = \text{Tr}(CN^tZ) = \text{Tr}((CN^t)Z) = \text{Tr}(Z(CN^t)) = \text{Tr}((ZC)N^t) = 0
\]

for each \( C \in C \). Hence, \( N_m(C)^\top C^\perp \subseteq C^\perp \) from which it follows that \( N_m(C)^\top \subseteq N_m(C^\perp) \). Since the Delsarte dual operation is involutory, we have that \( N_m(C)^\top = N_m(C^\perp) \).

It is not difficult to see that the adjoint operation and the Delsarte duality commute, i.e., \( C^\perp = C^\top \). With this in mind we have the following

\[
N_r(C^\perp) = N_m(C^\perp) = N_m(C^\top) = N_m(C)^\perp = N_r(C)^\top.
\]

This concludes the proof. \( \square \)

As in previous section on kernels, we are curious about the conditions under which middle or right nucleus of a code is a field. In particular, it is interesting to see whether they are always fields for linear MRD codes and the codes derived from quadratic APN functions.
Lemma 4.3. Let $C$ be a linear rank metric code of $\mathbb{K}^{m \times n}$ with $m \leq n$ and its minimum distance $d \geq \left\lceil \frac{m}{2} \right\rceil + 1$. Assume that there is at least one invertible matrix in $C$. For any element $Z \in N_m(C)$, assume that there exists $C_0 \in C$ such that $ZC_0 = 0$. Then $Z$ is the zero matrix. In particular, when $C$ is a finite set, all nonzero matrices in $N_m(C)$ are invertible and $N_m(C)$ is a skewfield.

Proof. By $ZC_0 = 0$, the matrix $Z \in \mathbb{K}^{m \times m}$ can not have full rank. That means $d' < m$, where $d' := \text{rk}(Z)$.

By way of contradiction, we assume that $Z \neq 0$. As an invertible matrix $M$ is assumed to be in $C$, we have $ZM \neq 0$. Since $ZM \in C$, $\text{rk}(ZM) \geq d$ and $d' \geq d$.

Again from $ZC_0 = 0$ we also have that $\text{rk}(C_0) \leq m - d'$. Together with $d' \geq d$ we have

$$d \leq \text{rk}(C_0) \leq m - d' \leq m - d.$$

This contradicts the assumption that $d \geq \left\lceil \frac{m}{2} \right\rceil + 1$.

Now we suppose that $C$ is finite. If $Z$ is degenerate, then $ZM$ is not invertible anymore, which implies that $ZC \subseteq C$. Since $C$ is finite and linear, there exists a nonzero matrix $C_0$ such that $ZC_0 = 0$. From the previous part, we know that $Z$ must be zero. Hence the nonzero matrices in $N_m(C)$ are all nondegenerate. As $N_m(C)$ is also closed under addition and multiplication and it contains the identity matrix, $N_m(C)$ is a skewfield. \hfill \square

By a similar approach, we can also prove the following result for right nucleus.

Lemma 4.4. Let $C$ be a linear rank metric code of $\mathbb{F}_q^{m \times n}$ with $m \leq n$ and its minimum distance $d \geq \left\lceil \frac{m}{2} \right\rceil + 1$. Assume that there is at least one invertible matrix in $C$. For any element $Z \in N_r(C)$, assume that there exists $C_0 \in C$ such that $C_0Z = 0$. Then $Z$ is the zero matrix. In particular, when $C$ is a finite set, all nonzero matrices in $N_r(C)$ are invertible and $N_r(C)$ is a skewfield.

Theorem 4.5. Let $C$ be a linear MRD code in $\mathbb{F}_q^{m \times n}$ with $m \leq n$ and $d \geq 1$. Then the following statements hold:

(a) Its middle nucleus $N_m(C)$ is a finite field.

(b) When $\max\{d, m - d + 2\} \geq \left\lceil \frac{m}{2} \right\rceil + 1$, its right nucleus $N_r(C)$ is a finite field.

Proof. (a) When $d \geq \left\lceil \frac{m}{2} \right\rceil + 1$, it is already proved in Lemma 4.3 because $C$ is a finite set and there is at least one invertible matrix in $C$ by Lemma 2.1 when $d < \left\lceil \frac{m}{2} \right\rceil + 1$, we look at its Delsarte dual $C^\perp$. By (1), its distance

$$d(C^\perp) = m - d + 2 > m - \left\lceil \frac{m}{2} \right\rceil + 1 \geq \left\lceil \frac{m}{2} \right\rceil + 1.$$

Again by Lemma 4.3 we have $N_m(C^\perp)$ is a finite field. As $N_m(C^\perp) = N_m(C)^\top$ (Proposition 4.1(b)), $N_m(C)$ is also a finite field.

(b) When $d \geq \left\lceil \frac{m}{2} \right\rceil + 1$, we get it by Lemma 4.3 otherwise $m - d + 2 \geq \left\lceil \frac{m}{2} \right\rceil + 1$, we have that $N_r(C^\perp)$ is a finite field. From $N_r(C^\perp) = N_r(C)^\top$ (Proposition 4.1(b)), we see that $N_r(C)$ is also a finite field. \hfill \square

Remark 4.6. (a) When the minimum distance of an MRD code $C$ is $d = 1$, $C$ is the whole space $\mathbb{K}^{m \times n}$. Then $N_m(C) = \mathbb{K}^{m \times m}$ and $N_r(C) = \mathbb{K}^{n \times n}$.

(b) When the conditions in Theorem 4.5 are satisfied for a linear MRD code $C$, it can be viewed as a left vector space over $N_m(C)$ as well as a right vector space over $N_r(C)$. 
Corollary 4.7. Let $C$ be a linear MRD code in $\mathbb{F}_q^{n \times n}$. Then its middle nucleus and right nucleus are both finite fields.

In general, Theorem 4.5 (b) does not hold when $\max\{d, m - d + 2\} < \left\lceil \frac{n}{2} \right\rceil + 1$. Let us look at an example with $m = 2$, $n = 4$, $q = 2$ and $d = 2$.

Example 4.8. We define $B \subseteq \mathbb{F}_2^{2 \times 2}$ as

$$B := \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right\}.$$ 

A rank metric code $C \subseteq \mathbb{F}_2^{2 \times 4}$ is defined as

$$C := \{(B_1, B_2) : B_1, B_2 \in B\},$$

where $(B_1, B_2)$ stands for the $2 \times 4$ matrix whose first $2 \times 2$ block is $B_1$ and second $2 \times 2$ block is $B_2$.

It is readily verified that all nonzero matrix in $C$ is of full rank. As there are totally $16$ matrices in $C$ and $q^{\max\{m, n\}(\min\{m, n\} - d + 1)} = 16$, $C$ is an MRD code.

Let

$$Z = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$ 

Then $CZ \subseteq C$ for each $C \in C$. However $\text{rk}(Z) = 2$.

Now let us turn to $C_f$ derived from a quadratic APN function in Section 3.

Theorem 4.9. Let $f$ be a quadratic APN function on $\mathbb{F}_2^n$ with $n > 2$. Then $N_m(C_f)$ and $N_r(C_f)$ are both finite fields.

Proof. We only have to prove that all matrices in $N_m(C_f)$ and $N_r(C_f)$ are nondegenerate.

As $\text{rk}(M_a) = n - 1$ and $ZM_a \in C_f$ for all $a \neq 0$ and $Z \in N_m(C_f)$,

$$\text{rk}(Z) \in \{n - 1, n\}.$$ 

Suppose that there exist $M_a, M_b \in C_f$ such that $ZM_a = ZM_b$. Then $ZM_{a-b} = 0$. Since $n > 2$ and $\text{rk}(Z) \geq n - 1$, it follows that $M_{a-b} = 0$, i.e. $a = b$. Thus for any $Z \in N_m(C_f) \setminus \{0\}$,

$$\{ZM_a : a \in \mathbb{F}_{2^n}\} = C_f.$$ 

Finally let us show that $\text{rk}(Z) = n - 1$ is impossible. By way of contradiction, we assume that $\text{rk}(Z) = n - 1$. By (21), all the columns of every nonzero $M_a$ are in $\{Zy^t : y \in \mathbb{F}_2^n\}$ which is an $(n - 1)$-dimensional subspace, which implies that

$$\dim_{\mathbb{F}_2}\{M_a x^t : x, a \in \mathbb{F}_{2^n}\} \leq n - 1.$$

However, by (13),

$$\{M_a x^t : x, a \in \mathbb{F}_{2^n}\} > 2^{n-1}.$$ 

It is a contradiction.

By looking at the rows of $M_a$, we can similarly prove that all matrices in $N_m(C_f)$ are nondegenerate. $\square$
For a finite semifield $S$, Knuth [17] noted that there are other five semifields which can be derived from $S$ and there is a group $G$ isomorphic to $S_3$ acting on these 6 semifields. In fact, $G$ is generated by two operations on $S$: One is the dual operation mapping the multiplication $*$ in a semifield to $*$ which is defined by $x * d y := y * x$ for all $x$ and $y$; another one corresponds to the transpose of derived spreadset from a given semifield. This group $G$ can also be completely presented on matrices, or by Knuth's cubical arrays $(a_{ijk})$ over a finite field $\mathbb{F}_q$. More precisely, let $(S, +, *)$ be of order $q^n$ and assume that the maps $x \mapsto x * y$ and $y \mapsto x * y$ are both $\mathbb{F}_q$-linear. Let $\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$ be a basis of $\mathbb{F}_q^n$ over $\mathbb{F}_q$. Then $a_{ijk}$ is defined by

$$b_i * b_j = \sum_{k=1}^{n} a_{ijk} b_k,$$

for $i, j, k \in \{1, 2, \ldots, n\}$. Originally, Knuth proved that by applying any permutation in $S_3$ to the subscripts of the array $(a_{ijk})$, it still determines a semifield. It is worth pointing out that when the multiplication is commutative, there are just three semifields under the acting of $S_3$, because $(a_{ijk}) = (a_{jik})$. The left, right and middle nuclei of these six semifields are also permuted under $G$; see [25].

In a similar way, we can also get a cubical array from a quadratic APN function $f$ by replacing $x * y$ with $B_f(x, y) = f(x + y) + f(x) + f(y)$. Under the permutation group $S_3$, we also get three set of matrices $C_f, C_f^T$ and $\tilde{C}_f$ from $C_f$, which we have already seen in Section 4.9. Now a natural question is: What are the relation between the kernels and the nuclei of them?

**Theorem 4.10.** Let $f$ be a quadratic APN function on $\mathbb{F}_{2^n}$ with $n > 2$. Then

(a) $N_m(C_f) \cong N_r(C_f^T) \cong K\tilde{C}_f$;
(b) $N_m(C_f^T) \cong N_r(C_f) \cong K\tilde{C}_f$;
(c) $N_m(\tilde{C}_f) \cong N_r(\tilde{C}_f) \cong K\tilde{C}_f^T$.

**Proof.** We only show (a) here. The other two statements can be similarly proved.

Let $Z \in N_r(C_f^T)$. By definition, there is a map $\zeta$ from $\mathbb{F}_{2^n}$ to itself such that

$$M^t_\zeta Z = M^t_\zeta(a).$$

As $M^t_{\zeta_{a+b}} = M^t_{a+b} + M^t_b Z = M^t_a Z + M^t_b Z = M^t_{\zeta(a)} + M^t_{\zeta(b)} = M^t_{\zeta_{a+b}}$, we know that $\zeta$ is also $\mathbb{F}_2$-linear on $\mathbb{F}_{2^n}$. Under the given basis $\mathcal{B}$, we use $N_Z$ to denote the derived matrix from $\zeta$.

Since $aM^t_{a} = a M_a$ for all $a \in \mathbb{F}_{2^n}$,

$$a\tilde{M}_a Z = a M^t_a Z = a M^t_\zeta(a) = a N_Z \tilde{M}_a.$$

It means that $(aN_Z, a\tilde{M}_a Z) \in \{ (y, y \tilde{M}_a) : y \in \mathbb{F}^n_a \}$. Hence the matrix

$$\left( \begin{array}{cc} N_Z & 0 \\ 0 & Z \end{array} \right)$$

is in $K\tilde{C}_f$. The converse statement also holds, i.e., given an element in $K\tilde{C}_f$, we also get a unique corresponding element in $N_r(C_f^T)$. As $N_r(C_f^T)$ is a field by Theorem 4.9, we have $N_r(C_f^T) \cong K\tilde{C}_f$.

By Proposition 4.11 we have $N_m(C_f)^T = N_r(C_f^T)$. Thus $N_m(C_f)$ is isomorphic to $N_r(C_f^T)$. \qed
**Corollary 4.11.** Let $f$ be a quadratic APN function on $\mathbb{F}_{2^n}$ for $n > 2$. Then $K_{\tilde{C}_f}$ is isomorphic to $\mathbb{F}_2$ or $\mathbb{F}_4$. If the second case occurs, then $n$ is even.

**Proof.** In [10], Dempwolff and Edel investigated the so-called dimensional dual hyperovals (abbreviated to DHO) derived from quadratic APN functions $f$. They defined the nucleus of the DHO, which is exactly the middle nucleus $N_m(C_f)$ of $C_f$ defined here. They also proved that $N_m(C_f)$ is $\mathbb{F}_2$ or $\mathbb{F}_4$. The second case occurs only when $n$ is even. By Theorem 4.10 we get the same result for $K_{\tilde{C}_f}$. $\square$

**Remark 4.12.** By Theorem 4.9 and Theorem 4.10 (b), we also have a short proof for $K_{\tilde{C}_f}$ being a field.

**Remark 4.13.** In Theorem 3.14, 4.9, 4.10 and Corollary 4.11 we all assume that $n > 2$. When $n = 2$, there is only one quadratic APN function $f(x) = x^3$ up to equivalence. Under a certain basis,

$$C_f = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\}.$$ 

It is then readily verified that $N_m(C_f) = \mathbb{F}_2^{2 \times 2}$,

$$N_f(C_f) = \left\{ \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} : c_1, c_2, c_3 \in \mathbb{F}_2 \right\},$$

and there are $2^3 = 8$ elements in its kernel

$$K_{\tilde{C}_f} = \left\{ \begin{pmatrix} c_1 & 0 & 0 & 0 \\ 0 & c_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & c_2 & c_3 \end{pmatrix} : c_1, c_2, c_3 \in \mathbb{F}_2 \right\}.$$ 

5. Nuclei of known linear MRD codes

Observe that when $n = m$, it does not matter which linear independent elements $\alpha_1, \ldots, \alpha_n$ are chosen in [3], because the derived codes are equivalent by multiplying a certain invertible matrix on the left. Thus a generalized Gabidulin code can be directly described as the set of polynomials in [3]. Now let us first restrict ourselves to MRD codes defined through sets of linearized polynomials.

Besides $G_{k, s}$ defined by [6], there are two other sets of linearized polynomials which define MRD codes for arbitrary values of $n$ and $k$. These were recently obtained in [32]. Precisely, Let $n, k, h \in \mathbb{Z}^+$ and $k < n$. Let $\eta$ be in $\mathbb{F}_{q^n}$ such that $N_{q^n, q^k}(\eta) \neq (-1)^{nk}$. Then the set

$$(22) \ \mathcal{H}_k(\eta, h) = \left\{ a_0 x + a_1 x^q + \cdots + a_{k-1} x^{q^{k-1}} + \eta a_0^q x\cdot x^q : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n} \right\}$$

is an $\mathbb{F}_q$-linear MRD code of size $q^{nk}$; these are called **twisted Gabidulin codes**.

Also in [32] the following generalization of these examples was mentioned. Let $n, k, s, h \in \mathbb{Z}^+$ satisfying that $\gcd(s, n) = 1$ and let $\eta$ be in $\mathbb{F}_{q^n}$ such that $N_{q^n, q^s}(\eta) \neq (-1)^{nk}$. Then the set

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

is an $\mathbb{F}_q$-linear MRD code of size $q^{nk}$. These sets $\mathcal{H}_{k, s}(\eta, h)$ latter are known as **generalized twisted Gabidulin codes** after [24], where they were intensively studied. Precisely, in [23] the automorphism group of a generalized twisted Gabidulin code
was completely determined and it was proven that the relevant family contains the two known classes \( G_{k,s} \) and \( \mathcal{H}_k(\eta, h) \) of MRD codes as proper subsets.

Let \( \mathcal{C} \) and \( \mathcal{C}' \) be two set of \( q \)-polynomials over \( \mathbb{F}_q^n \). It is clear that \( \mathcal{C} \) and \( \mathcal{C}' \) define two rank metric codes in \( \mathbb{F}_q^{n \times n} \) and they are equivalent if there exist two permutation \( q \)-polynomials \( L_1, L_2 \) and \( \rho \in \text{Aut}(\mathbb{F}_q) \) such that \( \mathcal{C}' = \{ L_1 \circ f^\rho \circ L_2(x) : f \in \mathcal{C} \} \), where \( (\sum a_i x^i)^\rho := \sum a_i^\rho x^i \). In particular, the automorphism group of the code derived from \( \mathcal{C} \) consists of all \((L_1, L_2, \rho)\) fixing \( \mathcal{C} \). From the proof of Theorem 4.4 in [23], the automorphism group of \( \mathcal{H}_k,s(\eta, h) \) can be completely determined.

**Theorem 5.1.** Let \( n, k, s, h \in \mathbb{Z}^+ \) satisfying \( \gcd(n, s) = 1 \) and \( 2 \leq k \leq n - 2 \). Let \( \eta \) be in \( \mathbb{F}_q^n \) satisfying \( N_{q^n/q^h}(\eta) \neq (-1)^{nk} \). Then \((L_1, L_2, \rho)\) is an automorphism of \( \mathcal{H}_k,s(\eta, h) \) if and only if there exist \( c, d \in \mathbb{F}_q^* \) and \( r \in \{0, 1, \ldots, n-1\} \) such that \( L_1 = cx^r \), \( L_2 = dx^{q^r-n} \) and

\[
\eta c^{q^{h-1}} d^{q^{r+h} - q^{r+s} k} = \eta^r q^r.
\]

In what follows we will determine the middle nucleus and the right one of \( \mathcal{H}_k,s(\eta, h) \). To this aim, it makes sense first to describe the nuclei in the context of \( q \)-polynomials over \( \mathbb{F}_q^n \).

Regard to this, denote by \( \mathcal{C} \subseteq \mathcal{E} \) the set of \( q \)-polynomials defining a code \( C \in \mathbb{F}_q^{n \times n} \). Clearly, we have that \( N_m(C) \cong N_m(\mathcal{C}) = \{ \varphi \in \mathcal{E} : f \circ \varphi \in \mathcal{C} \text{ for all } f \in \mathcal{C} \} \) and \( N_r(C) \cong N_r(\mathcal{C}) = \{ \varphi \in \mathcal{E} : \varphi \circ f \in \mathcal{C} \text{ for all } f \in \mathcal{C} \} \), where the symbol \( \circ \) stands for the composition of maps.

By Theorem 5.1 we can get the following results:

**Corollary 5.2.** Let \( \mathcal{H}_k,s(\eta, h) \) be a generalized twisted Gabidulin code. Then we have

(a) if \( \eta = 0 \), then \( \mathcal{H}_k,s(0, h) = G_{k,s} \) and \( N_m(G_{k,s}) = N_m(\mathcal{G}_{k,s}) \cong \mathbb{F}_{q^n} \);

(b) if \( \eta \neq 0 \), then \( N_m(\mathcal{H}_k,s(\eta, h)) \cong \mathbb{F}_q^{\gcd(n,sk-h)} \) and \( N_r(\mathcal{H}_k,s(\eta, h)) \cong \mathbb{F}_q^{\gcd(n,h)} \).

**Proof.** To determine the middle nucleus, we let \( \rho \) to be the identity map, \( L_1 = x \) and \( L_2 = dx \). If \( \eta = 0 \), then (23) is always satisfied; otherwise, (23) becomes

\[
\eta c^{q^{h-1}} d^{q^{r+h} - q^{r+s} k} = \eta,
\]

which holds if and only if \( d \in \mathbb{F}_q^{\gcd(n,sk-h)} \).

To determine the right nucleus, we let \( \rho \) to be the identity map, \( L_2 = x \) and \( L_1 = cx \). Now if \( \eta = 0 \), then (23) is always satisfied; otherwise, we have

\[
\eta c^{q^{h-1}} = \eta,
\]

which holds if and only if \( c \in \mathbb{F}_q^{\gcd(n,h)} \). \( \Box \)

Now let us turn to linear MRD codes in \( \mathbb{F}_q^{m \times n} \) with \( m < n \). Most of MRD codes with \( 1 < k < n - 1 \) and \( m < n \) are in the following form:

\[
\left\{ \left( v(f(\alpha_1)), \ldots, v(f(\alpha_m)) \right)^T : f \in \mathcal{H}_k,s(\eta, h) \right\},
\]

where \( \alpha_1, \ldots, \alpha_m \) are linear independent. Several new constructions of MRD codes which are not in this form are presented recently in [13] and they are proved to be not equivalent to any Gabidulin code. However, we do not know whether they are equivalent to a generalized twisted Gabidulin code (24) or not.
Let $\xi$ be a primitive element of $\mathbb{F}_q^n$ and
$$H := \left\{ (v(f(1)), v(f(\xi)), \ldots, v(f(\xi^{n-1})))^T : f \in \mathcal{H}_{k,s}(\eta, h) \right\},$$
then by multiplying a suitable $m$ by $n$ matrix $L$ of full rank on the left of elements in $H$, we can get \[24\]. In another word, the MRD code \[24\] is the image of $H$ under a projection from $\mathbb{F}_q^{m \times n}$ to $\mathbb{F}_q^{m \times n}$.

In general we do not know the middle nucleus and the right nucleus of an arbitrary MRD defined as in \[24\]. However, when $\eta = 0$, i.e. $\mathcal{H}_{k,s}(\eta, h) = \mathcal{G}_{k,s}$, its middle and right nuclei are determined very recently in \[22\]; see \[29\] for the calculation of the middle nuclei too. We pointing out that, in \[22\], the (generalized) Gabidulin code is described as the adjoint of \[5\]. Hence the right (resp. left) idealiser there is exactly the middle (resp. right) nucleus of \[5\].

By Corollary \[5.2\] and the following lemma which can be directly obtained by definition, we can also easily show that the right nuclei of \[5\] always contains $\mathbb{F}_q^n$.

**Lemma 5.3.** Let $C$ be a rank metric code in $\mathbb{K}^{m \times n}$. Let $L$ be an $\ell \times m$ matrix in $\mathbb{K}^{\ell \times n}$ with $\ell < m$. Then
$$N_r(C) \subseteq N_r(\{LC : C \in C\}).$$

The middle nucleus of a projection of a given code, it seems difficult to get any general result similar to Lemma \[5.3\]. After a projection, the new middle nucleus is in the set of matrices of a smaller size. However, it is not necessary that the cardinality of the middle nucleus is getting smaller. For instance, the following result can also be obtained for the APN functions on $\mathbb{F}_{p^n}$ constructed in \[36\]. The middle nucleus, which is exactly the middle nucleus of the derived MRD code, is $\mathbb{F}_{p^{gcd(n,k)}}$ if $\sigma$ is nontrivial or $\mathbb{F}_{p^{2gcd(n,k)}}$ if $\sigma$ is trivial. If we project it to the last $n$ rows, then we only have the matrices corresponding to
$$(x, y) \mapsto (ay + bx).$$
It is easy to show that the middle nucleus of this new set of matrices is $\mathbb{F}_{p^n}$. Hence, if $2 \nmid gcd(n, k)$, the new middle nucleus is larger than the original one. Analogue results can also be obtained for the APN functions on $\mathbb{F}_{2^n}$ constructed in \[36\].

By looking at the projection of rank metric codes, we may also find some small structures just as we have shown for some semifields. The idea of projection and lifting have been already applied for several times in the constructions of APN functions and semifields; see \[5, 6, 14, 31, 35\].

As the middle nuclei and the right ones are both invariant with respect to the equivalence on rank metric codes, we may also consider the set of the middle (resp. right) nuclei of every projection of a rank metric code. More precisely, let $C$ be a rank metric code in $\mathbb{K}^{m \times n}$. For any $l \leq m$ and any $l$-dimensional subspace $U$ of $\mathbb{K}^n$, we choose a matrix $L_U \in \mathbb{K}^{l \times m}$ whose rows form a basis of $U$. It is not difficult to see that for a given subspace $U$, distinct ways of choosing $L_U$ do not affect $N_m(L_U C)$ and $N_r(L_U C)$ up to equivalence. The middle nuclei spectrum of a linear rank metric code $C \subseteq \mathbb{K}^{m \times n}$ is the multiset defined by
$$\{ \ast (l, N_m(L_U C)) : 1 < l < m, U \text{ is an } l \text{-dimensional subspace of } \mathbb{K}^m \ast \}. $$
Similarly, we can define the right nuclei spectrum of $C$. It is clear that these two spectra are both invariants with respect to the equivalence on rank metric codes. Hence they are useful for telling whether two codes are equivalent or not.

It is in general also not easy to compute these spectra for a linear rank metric code. We can use computer to get them for some MRD codes with small parameters.

**Example 5.4.** Let $q = 3$, $m = n = 4$, $k = 2$ and $s = h = 1$. Let $\eta$ be a root of $X^4 - X^3 - 1 \in \mathbb{F}_3[X]$. Then $\mathcal{H}_{k,s}(\eta, h)$ defines an MRD code $C$ in $\mathbb{F}_3^{4 \times 4}$.

For $l = 3$, there are totally 40 subspaces $U$ of dimension $l$ in $\mathbb{F}_3^4$. For each of such subspace $U$, our MAGMA program shows that $N_m(L_U C) \cong \mathbb{F}_3$ and $N_r(L_U C) \cong \mathbb{F}_3$. When $l = 2$ and 1, for each subspace $U$ of dimension $l$, we have $L_U C = \mathbb{F}_3^{l \times 1}$ from which it follows $N_m(L_U C) = \mathbb{F}_3^{l \times 1}$ and $N_r(L_U C) = \mathbb{F}_3^{4 \times 4}$.

If we take $\eta = 0$, then $\mathcal{H}_{k,s}(\eta, h) = \mathcal{G}_{k,s} = \mathcal{G}_{2,1}$. Let us use $C'$ to denote the MRD code in $\mathbb{F}_3^{4 \times 4}$ corresponding to it. For each subspace $U$ of dimension 3, Lemma 4.1 and Theorem 4.5 in [22] tell us that $N_m(L_U C') \cong \mathbb{F}_3$ and $N_r(L_U C') \cong \mathbb{F}_3$. Again when $l = 1, 2$, for each subspace $U$ of dimension $l$, we have $L_U C' = \mathbb{F}_3^{l \times 1}$ which means $N_m(L_U C') = \mathbb{F}_3^{l \times l}$ and $N_r(L_U C') = \mathbb{F}_3^{4 \times 4}$.

**Acknowledgment**

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

**References**

[1] A. A. Albert. Generalized twisted fields. Pacific Journal of Mathematics, 11:1–8, 1961.

[2] J. André. Über Parallelstrukturen. Teil II: Translationsstrukturen. Mathematische Zeitschrift, 76:155–163, 1961.

[3] L. Bader and G. Lunardon. Desarguesian spreads. Ricerche di Matematica, 60(1):15–37, Dec. 2010.

[4] M. Biliotti, V. Jha, and N. L. Johnson. The collineation groups of generalized twisted field planes. Geometriae Dedicata, 76:97–126, 1999.

[5] K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe. An APN permutation in dimension six. In Finite fields: theory and applications, volume 518 of Contemp. Math., pages 33–42. Amer. Math. Soc., Providence, RI, 2010.

[6] L. Budaghyan, C. Carlet, and G. Leander. Constructing new APN functions from known ones. Finite Fields and Their Applications, 15(2):150–159, Apr. 2009.

[7] A. Cossidente, G. Marino, and F. Pavese. Nonlinear maximum rank distance codes. preprint, 2015.

[8] J. de la Cruz, M. Kiermaier, A. Wassermann, and W. Willems. Algebraic structures of MRD codes. [arXiv:1507.08641] [cs, math], Jan. 2015.

[9] 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.

[10] U. Dempwolff and Y. Edel. Dimensional dual hyperovals and APN functions with translation groups. Journal of Algebraic Combinatorics, 39(2):457–496, June 2014.

[11] Y. Edel. Quadratic APN functions as subspaces of alternating bilinear forms. In Proceedings of the Contact Forum Coding Theory and Cryptography III, page 11–24, Brussel, 2011. The Royal Flemish Academy of Belgium for Science and the Arts.

[12] E. Gabidulin. Theory of codes with maximum rank distance. Problems of information transmission, 21:3–16, 1985.

[13] A.-L. Horlemann-Trautmann and K. Marshall. New criteria for MRD and Gabidulin codes and some rank metric code constructions. [arXiv:1507.08641] [cs, math], July 2015. arXiv: 1507.08641.
[14] X.-d. Hou, F. Özbudak, and Y. Zhou. Switchings of semifield multiplications. *Designs, Codes and Cryptography*, May 2015. Online.

[15] D. R. Hughes and F. C. Piper. *Projective planes*. Springer-Verlag, New York, 1973. Graduate Texts in Mathematics, Vol. 6.

[16] N. L. Johnson, V. Jha, and M. Biliotti. *Handbook of finite translation planes*, volume 289 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2007.

[17] D. E. Knuth. Finite semifields and projective planes. *Journal of Algebra*, 2:182–217, 1965.

[18] 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.

[19] 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.

[20] M. Lavrauw and O. Polverino. Finite semifields. In L. Storme and J. De Beule, editors, *Current research topics in Galois Geometry*, chapter 6, pages 131–160. NOVA Academic Publishers, 2011.

[21] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.

[22] D. Liebhold and G. Nebe. Automorphism groups of Gabidulin-like codes. [arXiv:1603.09565](https://arxiv.org/abs/1603.09565) [cs, math], Mar. 2016. arXiv: 1603.09565.

[23] G. Lunardon, R. Trombetti, and Y. Zhou. Generalized twisted Gabidulin codes. [arXiv:1507.07855](https://arxiv.org/abs/1507.07855) [cs, math], July 2015. arXiv: 1507.07855.

[24] G. Marino and O. Polverino. On the nuclei of a finite semifield. In *Theory and applications of finite fields*, volume 579 of *Contemp. Math.*, pages 123–141. Amer. Math. Soc., Providence, RI, 2012.

[25] G. Marino, O. Polverino, and R. Trombetti. Towards the classification of rank 2 semifields 6-dimensional over their center. *Designs, Codes and Cryptography*, 61(1):11–29, 2011.

[26] G. Menichetti. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. *Journal of Algebra*, 47(2):400–410, 1977.

[27] G. Menichetti. n-dimensional algebras over a field with a cyclic extension of degree n. *Geometriae Dedicata*, 6(1):69–94, 1966.

[28] 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.

[29] A. Pott. Almost perfect and planar functions. *Designs, Codes and Cryptography*, 78(1):141–195, Jan. 2016.

[30] A. Pott and Y. Zhou. Switching construction of planar functions on finite fields. In *Proceedings of the Third international conference on Arithmetic of finite fields*, WAIFI’10, page 135–150, Berlin, Heidelberg, 2010. Springer-Verlag.

[31] J. Sheekey. A new family of linear maximum rank distance codes. [arXiv:1504.01581](https://arxiv.org/abs/1504.01581) [math], Apr. 2015.

[32] D. Silva, F. R. Kschischang, and R. Koetter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, Sept. 2008.

[33] Z. Wan and L. Hua. *Geometry of Matrices*. World Scientific, Jan. 1996.

[34] Y. Yu, M. Wang, and Y. Li. A matrix approach for constructing quadratic APN functions. *Designs, Codes and Cryptography*, 73(2):587–600, Mar. 2014.

[35] Y. Zhou and A. Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43–60, Feb. 2013.