Advances in Mathematics of Communications
Volume X, No. 0X, 200X, X–XX

# ALGEBRAIC STRUCTURES OF MRD CODES

Javier de la Cruz

Departamento de Matemáticas
Universidad del Norte
Km 5 Vía Puerto Colombia, Barranquilla, Colombia

Michael Kiermaier

Mathematisches Institut
Universität Bayreuth
95440 Bayreuth, Germany

Alfred Wassermann

Mathematisches Institut
Universität Bayreuth
95440 Bayreuth, Germany

Wolfgang Willems

Institut für Algebra und Geometrie
Otto-von-Guericke Universität
Postfach 4120
39016 Magdeburg, Germany

In memory of Axel Kohnert

Abstract. Based on results in finite geometry we prove the existence of MRD codes in $(\mathbb{F}_q)_{n,n}$ with minimum distance $n$ which are essentially different from Gabidulin codes. The construction results from algebraic structures which are closely related to those of finite fields. Some of the results may be known to experts, but to our knowledge have never been pointed out explicitly in the literature.

## 1. Introduction

Let $\mathbb{F}_q$ denote a finite field with $q$ elements and let $V = (\mathbb{F}_q)_{m,n}$ be the $\mathbb{F}_q$-vector space of matrices over $\mathbb{F}_q$ of type $(m, n)$. On $V$ we define the so-called rank metric distance by

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

for $A, B \in V$. Clearly, the distance d is a translation invariant metric on $V$. A subset $\mathcal{C} \subseteq V$ endowed with the metric d is called a rank metric code with minimum distance

$$\mathrm{d}(\mathcal{C}) = \min\{\mathrm{d}(A, B) \mid A \neq B \in V\}.$$

For $m \geq n$, an MRD (maximum rank distance) code $\mathcal{C} \subseteq V$ satisfies the following two conditions:

2010 *Mathematics Subject Classification:* Primary: 94B99, 16Y60; Secondary: 15B33.
*Key words and phrases:* MRD codes, rank distance, network coding, quasifields, semifields.
The authors wish to thank Colciencias, Bogotá, Universidad del Norte, Barranquilla, and COST Action IC 1104 for financial support.

(i) $|\mathcal{C}| = q^{km}$ and
(ii) $\mathrm{d}(\mathcal{C}) = n - k + 1$.

Note that an MRD code is a rank metric code which is maximal in size given the minimum distance, or in other words it achieves the Singleton bound for the rank metric distance (see [4, 6]).

Delsarte was the first who proved in [4] the existence of linear MRD codes for all $q, m, n$ and $1 \leq k \leq n$. His construction (in the notation of Gabidulin [6]) runs as follows: Let $a_1, \dots, a_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$ and let $C$ be the $\mathbb{F}_{q^m}$-linear code defined by the generator matrix

$$G = \begin{pmatrix} a_1 & \dots & a_n \\ a_1^q & \dots & a_n^q \\ \vdots & \dots & \vdots \\ a_1^{q^{k-1}} & \dots & a_n^{q^{k-1}} \end{pmatrix},$$

where $1 \leq k \leq n$. Each code word $c \in C$ is a vector in $(\mathbb{F}_{q^m})^n$. If we choose a fixed basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ then $c$ may be regarded as a matrix in $V = (\mathbb{F}_q)_{m,n}$. Thus we obtain an $\mathbb{F}_q$-linear code $\mathcal{C}$ in $V$. The code $\mathcal{C}$, which is usually called a Gabidulin code (although first discovered by Delsarte), is an $\mathbb{F}_q$-linear MRD code of size $q^{km}$ with minimum distance $d = n - k + 1$. At this point we may naturally ask: Is there any other MRD code which is essentially different from a Gabidulin code, i.e., which does not allow an isometry to a Gabidulin code.

**Definition 1.** a) A bijective map $\varphi : (\mathbb{F}_q)_{m,n} \longrightarrow (\mathbb{F}_q)_{m,n}$ is called an isometry if $\varphi$ preserves the rank metric distance, i.e.,

$$\mathrm{d}(A, B) = \mathrm{d}(\varphi(A), \varphi(B))$$

for all $A, B \in (\mathbb{F}_q)_{m,n}$.
b) Two codes $\mathcal{C}$ and $\mathcal{C}'$ in $(\mathbb{F}_q)_{m,n}$ are equivalent if there exists an isometry $\varphi$ with $\varphi(\mathcal{C}) = \mathcal{C}'$. If one of the codes is additively closed resp. an $\mathbb{F}_q$-vector space, we require in addition that $\varphi$ is additive resp. $\mathbb{F}_q$-linear.

In odd characteristic, already in the 1950s of the last century L.-K. Hua has classified all bijective maps $\varphi$ from $(\mathbb{F}_q)_{m,n}$ onto itself such that $\varphi$ and $\varphi^{-1}$ preserve the distance between adjacent matrices, i.e., between all pairs of matrices $A, B$ with $\operatorname{rank} A - B = 1$ In even characteristic, this has been done by Z.-X. Wan in the 1960s. For isometries the result can be stated as follows (see Theorem 3.4 in [17]):

**Theorem 1.** (Hua, Wan) *If $\varphi$ is an isometry of $(\mathbb{F}_q)_{m,n}$ with $m, n \geq 2$, then there exist matrices $X \in \mathrm{GL}(m, q), Y \in \mathrm{GL}(n, q)$ and $Z \in (F_q)_{m,n}$ such that*

$$\varphi(A) = XA^\sigma Y + Z \quad \textit{for all } A \in (\mathbb{F}_q)_{m,n}$$

*where $\sigma$ is an automorphism of the field $\mathbb{F}_q$ acting on the entries of $A$, or, but only in case $m = n$,*

$$\varphi(A) = X(A^t)^\sigma Y + Z \quad \textit{for all } A \in (\mathbb{F}_q)_{n,n}$$

*where $A^t$ denotes the transpose of $A$.*
*If $\varphi$ is additive, then obviously $Z = 0$. In addition $\sigma = \mathrm{id}$ in case $\varphi$ is $\mathbb{F}_q$-linear.*

In the recent paper [14] Morrison has rediscovered Hua's result in case that $\varphi$ is linear resp. semi-linear.

Note that up to equivalence in the above sense Gabidulin codes only depend on $q, m, n$ and $k$, but not on the chosen vector $(a_1, \dots, a_n) \in \mathbb{F}_{q^m}^n$.

If we specialize the Gabidulin construction to $k = 1$ and $m = n$, then a Gabidulin code $\mathcal{G}$ is a linear code of dimension $n$ such that $A - B$ is always regular for $A \neq B$ in $\mathcal{G}$. In particular, all $0 \neq A \in \mathcal{G}$ are regular since the zero matrix is in $\mathcal{G}$. If $\mathcal{G}$ is defined by $(a_1, \dots, a_n) \in \mathbb{F}_{q^n}^n$ and we choose $a_1, \dots, a_n$ as an $\mathbb{F}_q$-basis $B$ of $\mathbb{F}_{q^n}$ then

$$\mathcal{G} = \langle S \rangle \cup \{0\}$$

where $\langle S \rangle$ denotes the group generated by a Singer cycle $S$ in $\mathrm{GL}(n, q)$ which is the matrix defining the multiplication by a primitive element in $\mathbb{F}_{q^n}$ with respect to the basis $B$. Finally, observe that $\langle S \rangle \cup \{0\}$ is isomorphic to the field $\mathbb{F}_{q^n}$ where the addition and multiplication are the standard ones in the ring of square matrices. In this special case we may already ask whether there are linear MRD codes which are not isomorphic to finite fields.

In what follows we do not insist that everything is new. Many facts may have been proved earlier or are at least folklore in the community of specialists on finite quasifields/semifields/division algebras. However the link between rank metric codes with special parameters and quasifields/semifields/division algebras does not seem to have been pointed out in the existing literature so far.

## 2. On the structure of MRD codes with $k = 1$ and $n = m$

In this section we connect MRD codes in case $k = 1$ and $m = n$ with well-known objects in finite geometry. Recall that an MRD code $\mathcal{C}$ in $(\mathbb{F}_q)_{n,n}$ of minimum distance $n$ is a maximal set of matrices such that $\det(A - B) \neq 0$ for all $A \neq B$ in $\mathcal{C}$. Replacing $\mathcal{C}$ by the translate $\mathcal{C} - B = \{A - B \mid A \in \mathcal{C}\}$ for some fixed $B \in \mathcal{C}$ we may assume that the zero matrix is an element of $\mathcal{C}$. Hence all matrices in $\mathcal{C}$ different from zero are invertible. Replacing $\mathcal{C}$ by $B^{-1}\mathcal{C}$ for some $B \neq 0$ in $\mathcal{C}$ we may further assume that the identity matrix $I$ is an element in $\mathcal{C}$. So far we have changed $\mathcal{C}$ by a rank metric distance preserving isometry which is not linear if $0 \notin \mathcal{C}$.

Furthermore, since $|\mathcal{C}| = q^n$ and $\det A \neq 0$ for all $0 \neq A \in \mathcal{C}$ we see that $\mathcal{C} \setminus \{0\}$ acts regularly on the non-zero vectors of $W = \mathbb{F}_q^n$, i.e. $\mathcal{C} \setminus \{0\}$ acts transitively without fixed points on the non-zero vectors of $W$. In particular, if we fix a vector $0 \neq w_0 \in W$, then for any $w \in W$ there exists exactly one $A(w) \in \mathcal{C}$ such that $w_0 A(w) = w$. In the following we always take $w_0 = e_1 = (1, 0, \dots, 0)$. Thus the first row of $A(w)$ is equal to $w$. In particular, we may write

$$\mathcal{C} = \{A(w) \mid w \in W\}, \tag{1}$$

where $A(0) = 0$ and $A(e_1) = I$. The latter follows by the fact that there is a $w \in W$ with $A(w) = I$ and $\det(A(e_1) - A(w)) = 0$ since the first row of $A(e_1)$ and $A(w) = I$ coincide.

In finite geometry, such a system of linear maps is called a spreadset in $W$ (see [5, 8]), or a spreadset over $\mathbb{F}_q$. Note that conversely a spreadset in $(\mathbb{F}_q)_{n,n}$ defines an MRD code $\mathcal{C}$ in $(\mathbb{F}_q)_{n,n}$ with minimum distance $n$. Spreadsets in $W$ give rise to a multiplication $\circ$ on $W$ defined by

$$w \circ w' = wA(w') \tag{2}$$

for $w, w' \in W$.

With this multiplication and the standard vector addition $W$ carries the structure of a quasifield ([5], section 5.1) which is defined as follows.

**Definition 2.** a) A set $\mathcal{Q}$ with two operations $+, \circ : \mathcal{Q} \times \mathcal{Q} \longrightarrow \mathcal{Q}$ is called a (right) quasifield if the following holds.

(i) $(\mathcal{Q}, +)$ is an abelian group with neutral element 0 which satisfies $0 \circ a = 0 = a \circ 0$ for all $a \in \mathcal{Q}$.
(ii) There is an identity $e$ in $\mathcal{Q}$ such that $e \circ a = a \circ e = a$ for all $a \in \mathcal{Q}$.
(iii) For all $a, b \in \mathcal{Q}$ with $a \neq 0$ there exists exactly one $x \in \mathcal{Q}$ such that $a \circ x = b$.
(iv) For all $a, b, c \in \mathcal{Q}$ with $a \neq b$ there exists exactly one $x \in \mathcal{Q}$ such that $x \circ a = x \circ b + c$.
(v) $(a + b) \circ c = a \circ c + b \circ c$ for all $a, b, c \in \mathcal{Q}$ (right distributivity).

b) We call

$$\operatorname{Ker} \mathcal{Q} = \{c \in \mathcal{Q} \mid c \circ (a + b) = c \circ a + c \circ b,\ c \circ (a \circ b) = (c \circ a) \circ b \text{ for all } a, b \in \mathcal{Q}\}$$

the kernel of the quasifield $\mathcal{Q}$.
c) A quasifield $\mathcal{Q}$ which satisfies also the left distributivity law is called a semifield $\mathcal{S}$. If $\mathcal{S}$ is not a field, we say that $\mathcal{S}$ is a proper semifield.
d) A quasifield with associative multiplication is called a nearfield. In particular, the non-zero elements of a nearfield form a group with respect to $\circ$.

**Definition 3.** Let $\mathcal{S}$ be a semifield.
a) The left, middle and right nucleus of $\mathcal{S}$ are defined as follows:

$$\begin{aligned}
\mathcal{N}_l = \mathcal{N}_l(\mathcal{S}) &= \{x \in \mathcal{S} \mid x \circ (a \circ b) = (x \circ a) \circ b \text{ for all } a, b \in \mathcal{S}\} \\
\mathcal{N}_m = \mathcal{N}_m(\mathcal{S}) &= \{x \in \mathcal{S} \mid a \circ (x \circ b) = (a \circ x) \circ b \text{ for all } a, b \in \mathcal{S}\} \\
\mathcal{N}_r = \mathcal{N}_r(\mathcal{S}) &= \{x \in \mathcal{S} \mid a \circ (b \circ x) = (a \circ b) \circ x \text{ for all } a, b \in \mathcal{S}\}.
\end{aligned}$$

Note that the left nucleus of $\mathcal{S}$ is just the kernel of $\mathcal{S}$ considered as a quasifield.
b) The center $Z(\mathcal{S})$ of $\mathcal{S}$ is the set

$$Z(\mathcal{S}) = \{a \in \mathcal{N}_l \cap \mathcal{N}_m \cap \mathcal{N}_r \mid x \circ a = a \circ x \text{ for all } x \in \mathcal{S}\}.$$

For applications in coding theory we may assume and will do so for the rest of this paper that the quasifields, semifields resp. nearfields are always finite.

**Remark 1.** Quasifields are strongly related to translation planes in finite geometry, i.e., translation planes are precisely those affine planes which can be coordinatized by quasifields [5]. Unfortunately, there is no satisfactory classification of finite quasifields. In contrast, for finite semifields there is a vast literature [12, 10, 3, 13, 9]. Proper finite semifields exist exactly for all orders $p^n \geq 16$ where $p$ is a prime and $n \geq 3$ [12]. Furthermore, finite nearfields have been classified by Zassenhaus in [18].

To continue we recall the following well-known facts which are easy to see.

**Lemma 1.** *a) If $\mathcal{Q}$ is a finite quasifield, then* $\operatorname{Ker} \mathcal{Q}$ *is a finite field.*
*b) $\mathcal{Q}$ is a finite dimensional left vector space over* $\operatorname{Ker} \mathcal{Q}$.
*c) If $\mathcal{S}$ is a finite semifield, then $\mathcal{S}$ is a division algebra over its center $Z(\mathcal{S})$.*

Now let $\mathcal{Q}$ be a finite quasifield and let $K$ be a subfield of $\operatorname{Ker} \mathcal{Q}$. According to Lemma 1 we have $\dim_K \mathcal{Q} = n$ for some $n \in \mathbb{N}$. For $a \in \mathcal{Q}$ we consider the map $x \mapsto x \circ a$ on $\mathcal{Q}$. Since

$$(x + y) \circ a = x \circ a + y \circ a \text{ and } (k \circ x) \circ a = k \circ (x \circ a)$$

for all $x, y \in \mathcal{Q}$ and all $k \in K$ there exists a unique $R(a) = R_K(a) \in \mathrm{GL}(n, K)$ for $a \neq 0$ and $R(0) = 0 \in (K)_{n,n}$ such that

$$xR(a) = x \circ a$$

for all $x \in \mathcal{Q}$. With this notation the set

$$\mathcal{C} = \{R(a) \mid a \in \mathcal{Q}\}$$

is an MRD code in $(K)_{n,n}$ with minimum distance $n$. Note that $\mathcal{C}$ is uniquely determined by $\mathcal{Q}$ and the chosen subfield $K$ of $\mathrm{Ker}\,\mathcal{Q}$ up to conjugation in $\mathrm{GL}(n, K)$. We will always choose the identity $e \in \mathcal{Q}$ as the first basis vector in a basis of $\mathcal{Q}$ over $K$, hence $e = e_1 = (1, 0, \ldots, 0)$. Therefore, the first row in $R(a)$ is equal to $a$ as a vector.

Conversely, let $\mathcal{C} = \{A(w) \mid w \in W\}$ be an MRD code in $(K)_{n,n}$ with minimum distance $n$ as in (1) and let $W = \mathcal{W}$ carry the structure of a quasifield defined as in (2). We shall prove that $K \cong Ke_1$ is contained in $\mathrm{Ker}\,\mathcal{W}$. To see that note that

$$(ke_1)A(w) + (ke_1)A(w') = (ke_1)(A(w) + A(w')) = (ke_1)A(w + w')$$

for $w, w' \in W$ and $k \in K$. Thus

$$ke_1 \circ w + ke_1 \circ w' = ke_1 \circ (w + w').$$

Furthermore,

$$(ke_1 \circ w) \circ w' = (ke_1 A(w))A(w') = k((e_1 A(w))A(w')) = k(w \circ w') = ke_1 \circ (w \circ w'),$$

which proves the claim. Thus we have proved the following which is essentially already stated in [2].

**Theorem 2.** MRD *codes in $(K)_{n,n}$ (containing the zero and identity matrix) with minimum distance $n$ correspond (in the above sense) to finite quasifields $\mathcal{Q}$ with $K \leq \mathrm{Ker}\,\mathcal{Q}$ and* $\dim_K \mathcal{Q} = n$.

If we require that the codes are closed under addition, hence form abelian groups (since they are finite), we get the following.

**Theorem 3.** *Additively closed* MRD *codes in $(K)_{n,n}$ (containing the identity matrix) with minimum distance $n$ correspond (in the above sense) to finite semifields $\mathcal{S}$ with $K \leq \mathrm{Ker}\,\mathcal{S}$ and* $\dim_K \mathcal{S} = n$.

*Proof.* Suppose that $\mathcal{S}$ is a finite semifield with $K \leq \mathrm{Ker}\,\mathcal{S}$ and $\dim_K \mathcal{S} = n$. Let $\mathcal{C} = \{R(a) = R_K(a) \mid a \in \mathcal{S}\}$. Since $\mathcal{S}$ satisfies the left distributive law we have

$$xR(a + b) = x \circ (a + b) = x \circ a + x \circ b = xR(a) + xR(b) = x(R(a) + R(b))$$

for $x, a, b \in \mathcal{S}$, hence $R(a) + R(b) = R(a + b)$.

Conversely, suppose that $\mathcal{Q}$ is a finite quasifield and $\mathcal{C} = \{R(a) \mid a \in \mathcal{Q}\}$ is additively closed. Thus, for $a, b \in \mathcal{Q}$ there exists a unique $c \in \mathcal{Q}$ such that

$$R(a) + R(b) = R(c).$$

If $e$ is the identity in $\mathcal{Q}$ then

$$c = e \circ c = eR(c) = e(R(a) + R(b)) = eR(a) + eR(b) = e \circ a + e \circ b = a + b.$$

So

$$R(a) + R(b) = R(a + b)$$

or in other words, $R$ is additive. Thus

$$x \circ a + x \circ b = xR(a) + xR(b) = x(R(a) + R(b)) = xR(a + b) = x \circ (a + b)$$

for all $x, a, b \in \mathcal{Q}$. This shows that $\mathcal{Q}$ is left distributive, hence $\mathcal{Q}$ is a semifield $\mathcal{S}$. The fact that $K \leq \operatorname{Ker} \mathcal{S}$ and $\dim_K \mathcal{S} = n$ follows from Theorem 2. □

In order to understand linearity of MRD codes over some field $\mathbb{F}_q$ we need the following result.

**Proposition 1.** *Let $\mathcal{S}$ be a finite semifield and $K$ a subfield of $\mathcal{S}$. The following two conditions are equivalent:*

1. *$\mathcal{S}$ is a division algebra over $K$.*
2. *$K$ is a subfield of $Z(\mathcal{S})$.*

*Proof.* b) $\Longrightarrow$ a): This follows from Lemma 1.
a) $\Longrightarrow$ b): Since $\mathcal{S}$ is a division algebral over $K$, we have

$$(k \circ a) \circ b = k \circ (a \circ b) = a \circ (k \circ b) \tag{3}$$

for all $k \in K$ and all $a, b \in \mathcal{S}$.

The first equality implies $K \leq \mathcal{N}_l(\mathcal{S})$. Plugging $b = e$ into the equality $(k \circ a) \circ b = a \circ (k \circ b)$ we get

$$k \circ a = a \circ k \tag{4}$$

for all $k \in K$ and $a \in \mathcal{S}$. Hence $K \subseteq \{x \in \mathcal{S} \mid x \circ a = a \circ x \text{ for all } a \in \mathcal{S}\}$. It remains to show that $K \subseteq \mathcal{N}_m \cap \mathcal{N}_r$. In order to see that note that

$$\begin{array}{rcll} a \circ (k \circ b) & = & (k \circ a) \circ b & \quad \text{(by (3))} \\ & = & (a \circ k) \circ b & \quad \text{(by (4))} \end{array}$$

for all $k \in K$ and all $a, b \in \mathcal{S}$, hence $K \subseteq \mathcal{N}_m$. Furthermore,

$$\begin{array}{rcll} a \circ (b \circ k) & = & a \circ (k \circ b) & \quad \text{(by (4))} \\ & = & k \circ (a \circ b) & \quad \text{(by (3))} \\ & = & (a \circ b) \circ k & \quad \text{(by (4))} \end{array}$$

for all $k \in K$ and all $a, b \in \mathcal{S}$, hence $K \subseteq \mathcal{N}_r$. □

**Theorem 4.** *$K$-linear* MRD *codes in $(K)_{n,n}$ (containing the identity matrix) with minimum distance $n$ correspond to finite division algebras $\mathcal{D}$ over $K$ where $K \leq Z(\mathcal{D})$ and* $\dim_K \mathcal{D} = n$.

*Proof.* Let $\mathcal{S}$ be a finite semifield with $K \leq \operatorname{Ker} \mathcal{S}$ and $\dim_K \mathcal{S} = n$. Let $R : \mathcal{S} \to (K)_{n,n}$ be defined as above; i.e. $xR(a) = x \circ a$ for $x, a \in \mathcal{S}$ and let $\mathcal{C} = \{R(a) \mid a \in \mathcal{S}\}$ be the MRD code corresponding to $\mathcal{S}$. Clearly, if $R$ is $K$-linear, i.e. $R(k \circ a) = kR(a)$ for $k \in K$ and $a \in \mathcal{S}$, then $\mathcal{C} = \{R(a) \mid a \in \mathcal{S}\}$ is a $K$-vector space. Conversely, if $\mathcal{C}$ is a $K$-vector space, then $R(k \circ a) = kR(a)$ for $k \in K$ and $a \in \mathcal{S}$ since the first row of $R(k \circ a)$ and $kR(a)$ coincide.

The condition

$$kR(a) = R(k \circ a)$$

for all $k \in K$ and all $a \in \mathcal{S}$ is equivalent to

$$(kx)R(a) = k(xR(a)) = x(kR(a)) = xR(k \circ a)$$

for all $k \in K$ and all $x, a \in \mathcal{S}$, hence to

$$(k \circ x) \circ a = k \circ (x \circ a) = x \circ (k \circ a).$$

for all $k \in K$ and all $x, a \in \mathcal{S}$. The latter means exactly that $\mathcal{S}$ is a division algebra over $K$ and the condition $K \leq Z(\mathcal{S})$ follows by Lemma 1. □

According to the above theorems, division algebras, semifields, nearfields or even quasifields deliver new methods to construct MRD codes which are different from Gabidulin codes. Remember that for a Gabidulin code in $(\mathbb{F}_q)_{n,n}$ with minimum distance $n$ the corresponding quasifield is a field.

## 3. Isotopy and equivalence

As stated in Theorem 4, $K$-linear MRD codes in $(K)_{n,n}$ with minimum distance $n$ correspond to finite division algebras $\mathcal{D}$ over $K \leq Z(\mathcal{D})$ with $\dim_K \mathcal{D} = n$. Since non-isomorphic division algebras may lead to equivalent codes we need the following definition.

**Definition 4.** Let $\mathcal{Q}$ and $\mathcal{Q}'$ be finite quasifields which are left vector spaces over the same field $K \leq \operatorname{Ker} \mathcal{Q} \cap \operatorname{Ker} \mathcal{Q}'$. We say that $\mathcal{Q}'$ is isotopic to $\mathcal{Q}$ over $K$ if there are $K$-linear isomorphisms $F, G, H : \mathcal{Q} \longrightarrow \mathcal{Q}'$ such that

$$aF \circ' bG = (a \circ b)H$$

for all $a, b \in \mathcal{Q}$.

**Example 1.**
a) There exist exactly 23 non-isomorphic proper semifields of order 16 which crumble away into two isotopy classes over $\mathbb{F}_2$ (see [12], section 6.2).
b) Using MAGMA [1] we computed exactly three equivalence classes of MRD codes in $(\mathbb{F}_2)_{4,4}$ with minimum distance 4. One of these classes represents a Gabidulin code which is associated to the finite field $\mathbb{F}_{16}$. The other two classes are represented as follows (without the zero matrix):

Code 2:

$$\begin{pmatrix} 1&1&1&0\\0&1&0&1\\1&1&0&1\\0&1&0&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&1&0\\1&0&0&1\\1&1&0&0\\0&1&1&1 \end{pmatrix}, \begin{pmatrix} 0&1&1&0\\0&0&0&1\\1&1&1&1\\0&1&0&1 \end{pmatrix}, \begin{pmatrix} 1&1&0&1\\1&1&1&1\\0&1&1&0\\1&0&0&0 \end{pmatrix},$$
$$\begin{pmatrix} 1&0&0&1\\0&0&1&1\\0&1&1&1\\1&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&1\\1&0&1&0\\1&0&1&1\\1&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&0\\1&1&0&1\\1&1&1&0\\0&1&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&1\\1&0&1&1\\0&1&0&0\\1&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&1&1&1\\0&0&1&0\\1&0&0&0\\1&1&1&0 \end{pmatrix},$$
$$\begin{pmatrix} 1&1&0&0\\1&0&0&0\\0&0&1&1\\0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0\\1&1&0&0\\0&0&0&1\\0&0&1&1 \end{pmatrix}, \begin{pmatrix} 1&0&1&1\\1&1&1&0\\1&0&0&1\\1&1&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&0&1\\0&1&1&1\\0&1&0&1\\1&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&1&1\\0&1&1&0\\1&0&1&0\\1&1&1&1 \end{pmatrix}.$$

Code 3:

$$\begin{pmatrix} 0&1&1&1\\1&1&0&0\\0&1&1&0\\0&1&0&0 \end{pmatrix}, \begin{pmatrix} 1&1&1&0\\1&1&0&1\\1&1&0&0\\1&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&1\\0&0&0&1\\1&0&1&0\\1&1&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0\\0&0&1&0\\0&0&0&1\\1&1&0&0 \end{pmatrix},$$
$$\begin{pmatrix} 1&1&0&1\\0&0&1&1\\1&0&1&1\\0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&1&0\\1&0&0&1\\1&1&1&0\\1&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&0\\1&0&1&1\\1&1&1&1\\0&1&1&1 \end{pmatrix}, \begin{pmatrix} 1&0&1&0\\1&1&1&1\\1&1&0&1\\0&1&1&0 \end{pmatrix}, \begin{pmatrix} 1&1&0&0\\0&1&1&0\\0&0&1&1\\1&1&0&1 \end{pmatrix},$$
$$\begin{pmatrix} 1&0&1&1\\1&0&1&0\\0&1&0&1\\1&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&0&1\\0&1&0&1\\1&0&0&0\\1&1&1&1 \end{pmatrix}, \begin{pmatrix} 0&1&0&1\\0&1&1&1\\1&0&0&1\\0&0&1&1 \end{pmatrix}, \begin{pmatrix} 1&1&1&1\\1&0&0&0\\0&1&0&0\\0&1&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&0\\1&1&1&0\\0&1&1&1\\1&0&0&0 \end{pmatrix}.$$

The Codes 2 and 3 correspond naturally to the two non-isotopic semifields of order 16 as the next result shows.

**Theorem 5.** *Let $\mathcal{C}, \mathcal{C}' \subseteq (K)_{n,n}$ be $K$-linear* MRD *codes with minimum distance $n$ and corresponding division algebras $\mathcal{D}$ and $\mathcal{D}'$. In particular $K \leq Z(\mathcal{D})$ and $K \leq Z(\mathcal{D}')$. Then $\mathcal{C}$ and $\mathcal{C}'$ are linearly equivalent if and only if $\mathcal{D}'$ is isotopic to $\mathcal{D}$ or its transpose $\mathcal{D}^t$ over $K$.*

*Proof.* If $W = K^n$ then $\mathcal{C} = \{A(w) \mid w \in W\}$ where $e_1 A(w) = w$ for $w \in W$. Furthermore, if $\mathcal{D}$ is the corresponding division algebra where $\mathcal{D} = W$ as a $K$-vector space, then the multiplication on $\mathcal{D}$ is given by

$$w_1 \circ w_2 = w_1 A(w_2) \quad \text{for } w_i \in W.$$

The transpose $\mathcal{D}^t$ of $\mathcal{D}$ is defined by $\mathcal{D}^t = W$ as a $K$-vector space but with multiplication $w_1 \circ w_2 = w_1 A(w_2)^t$. We use the same notation for the second code but with a $'$ everywhere.

We first suppose that $\mathcal{C}$ and $\mathcal{C}'$ are equivalent and prove that the corresponding semifields are isotopic over $K$. Thus by assumption there exist $X, Y \in \mathrm{GL}(n, K)$ such that

$$\{XA(w)Y \mid w \in W\} = \{A'(w) \mid w \in W\} \qquad (*)$$

or

$$\{XA(w)Y \mid w \in W\} = \{A'(w)^t \mid w \in W\}. \qquad (**)$$

Suppose that $(*)$ holds true. This means that for each $w \in W$ there exists exactly one $\tilde{w} \in W$ such that

$$XA(w)Y = A'(\tilde{w}).$$

Let $F : W \longrightarrow W$ denote the map $wF = \tilde{w}$. For $w_1, w_2 \in W$ we obtain

$$(w_1 \circ w_2)Y = w_1 A(w_2)Y = w_1 X^{-1} A'(\tilde{w_2}) = w_1 X^{-1} A'(w_2 F) = w_1 X^{-1} \circ' w_2 F.$$

Since $Y^{-1}$ and $X$ are $K$-linear it remains to show that $F$ is $K$-linear as well.

First note that $A(k_1 w_1 + k_2 w_2) = k_1 A(w_1) + k_2 A(w_2)$ for $k_i \in \mathbb{F}_q$ and $w_i \in W$ since the first row of $A(w)$ is equal to $w$ and $\mathcal{C}$ is a $K$-vector space. The same holds for $A'$. From this we obtain

$$\begin{aligned} A'((k_1 w_1 + k_2 w_2)F) &= XA(k_1 w_1 + k_2 w_2)Y \\ &= k_1 XA(w_1)Y + k_2 XA(w_2)Y \\ &= k_1 A'(w_1 F) + k_2 A'(w_2 F) \\ &= A'(k_1(w_1 F) + k_2(w_2 F)). \end{aligned}$$

Applying the inverse of $A'$ we get

$$(k_1 w_1 + k_2 w_2)F = k_1(w_1 F) + k_2(w_2 F)$$

which proves that $F$ is $K$-linear. Thus the division algebras $\mathcal{D}$ and $\mathcal{D}'$ are isotopic over $K$. In case $(**)$ the proof runs similar.

Now suppose that the corresponding division algebras are isotopic over $K$. Thus there are $K$-linear isomorphisms $F, G, H : W \longrightarrow W$ such that

$$(w_1 \circ w_2)H = w_1 F \circ' w_2 G$$

for $v, w \in W$. If follows

$$w_1 A(w_2)H = w_1 F A'(w_2 G)$$

for all $w_i \in W$. This implies $A(w)H = FA'(wG)$ for $w \in W$ or

$$F^{-1} A(w)H = A'(wG)$$

for all $w \in W$. Thus

$$\begin{aligned} F^{-1}\mathcal{C}H &= \{F^{-1}A(w)H \mid w \in W\} \\ &= \{A'(wG) \mid w \in W\} \\ &= \{A'(w) \mid w \in W\} = \mathcal{C}'. \end{aligned}$$

This shows that $\mathcal{C}$ and $\mathcal{C}'$ are equivalent. The case that $\mathcal{D}$ is isotopic to the transpose of $\mathcal{D}'$ is done similarly. □

**Remark 2.** a) The second part of the proof of Theorem 5 shows that an isotopy between two quasifields always leads to equivalent codes.
b) We do not know what an equivalence between two additively closed MRD codes in $(K)_{n,n}$ with minimum distance $n$ means for the corresponding semifields. Note that such an equivalence is not necessarily linear.

## 4. Symmetric MRD codes

Let $E = \mathbb{F}_{q^n}$ and let $K = \mathbb{F}_q \leq E$. On $E$ the standard non-degenerate symmetric $K$-bilinear form $\langle \cdot \,, \cdot \rangle$ is defined by

$$\langle x, y \rangle \;=\; \mathrm{tr}_{E/K}(xy)$$

for $x, y \in E$ where tr denotes the trace of $E$ over $K$. If $a$ is running over all non-trivial elements of $E$ we get non-degenerate symmetric $K$-bilinear forms of $E$ by

$$\langle x, y \rangle_a \;=\; \langle ax, y \rangle.$$

Taking the corresponding Gram matrices together with the zero matrix we obtain a linear MRD code in $(\mathbb{F}_q)_{n,n}$ with minimum distance $n$ consisting of symmetric matrices. This code is equivalent to a Gabidulin code which can be seen as follows. We fix a basis $x_1, \ldots, x_n$ of $E$ over $K$. Let $y_i = Bx_i$ for $i = 1, \ldots, n$ be the dual basis. Then the Gram matrices with respect to the basis $x_1, \ldots, x_n$ are of the form $A^tB^{-1}$ where $A$ runs through a Singer subgroup of $\mathrm{GL}(n, q)$.

According to [7], the symmetry can be used to correct (symmetric) errors beyond the bound $\lfloor \frac{d-1}{2} \rfloor$.

**Definition 5.** Let $K$ be a finite field. We call a code $\mathcal{C} \subseteq (K)_{n,n}$ symmetric if all matrices $A$ in $\mathcal{C}$ are symmetric, i.e., $A = A^t$ for all $A \in \mathcal{C}$.

**Definition 6.** Let $\mathcal{Q}$ be a finite quasifield over $K \leq \mathrm{Ker}\ \mathcal{Q}$. A $K$-bilinear form $\langle \cdot \,, \cdot \rangle$ on $\mathcal{Q}$ is called invariant if

$$\langle x \circ a, y \rangle \;=\; \langle x, y \circ a \rangle$$

for all $a, x, y \in \mathcal{Q}$.

**Lemma 2.** *Let $\mathcal{Q}$ be a finite quasifield over $K \leq \mathrm{Ker}\ \mathcal{Q}$ and let $\langle \cdot \,, \cdot \rangle$ be an invariant non-degenerate symmetric $K$-bilinear form on $\mathcal{Q}$. For $a \in \mathcal{Q}$ we define the form $\langle \cdot \,, \cdot \rangle_a$ by*

$$\langle x \,, y \rangle_a = \langle x \circ a \,, y \rangle$$

*for $x, y \in \mathcal{Q}$. Then, for all $0 \neq a \in \mathcal{Q}$, the form $\langle \cdot \,, \cdot \rangle_a$ is $K$-bilinear, non-degenerate and symmetric.*

*Proof.* One easily checks that $\langle \cdot\,,\cdot\rangle_a$ is $K$-bilinear since $(x_1+x_2)\circ a = x_1\circ a + x_2\circ a$ and $(k\circ x)\circ a = k\circ(x\circ a)$ for all $x, x_1, x_2, a \in \mathcal{Q}$ and all $k \in K$.

Let $G$ denote the Gram matrix of $\langle \cdot\,,\cdot\rangle$ with respect to the basis as $R(a)$ is taken where $x\circ a = xR(a)$. Then $\langle \cdot\,,\cdot\rangle_a$ has the Gram matrix $R(a)^tG$ which is regular for $a \neq 0$. Thus $\langle \cdot\,,\cdot\rangle_a$ is non-degenerate for all $0 \neq a \in \mathcal{Q}$.

Finally, the symmetry follows by

$$\begin{array}{rcll} \langle x\,,y\rangle_a & = & \langle x\circ a\,,y\rangle & \\ & = & \langle x\,,y\circ a\rangle & \text{(since } \langle\cdot\,,\cdot\rangle \text{ is invariant)} \\ & = & \langle y\circ a\,,x\rangle & \text{(since } \langle\cdot\,,\cdot\rangle \text{ is symmetric)} \\ & = & \langle y\,,x\rangle_a & \end{array}$$

for all $x, y, a \in \mathcal{Q}$. □

**Theorem 6.** *Let $\mathcal{Q}$ be a finite quasifield over the field $K \leq \mathrm{Ker}\ \mathcal{Q}$ and let $\mathcal{C} = \{R(a) \mid a \in \mathcal{Q}\}$ be the corresponding* MRD *code in $(K)_{n,n}$. Then $\mathcal{Q}$ admits an invariant non-degenerate symmetric $K$-bilinear form if and only if the equivalence class of $\mathcal{C}$ contains a symmetric code.*

*Proof.* Suppose that $\mathcal{Q}$ admits an invariant non-degenerate symmetric $K$-bilinear form $\langle\cdot\,,\cdot\rangle$. According to Lemma 2 the $K$-bilinear forms $\langle\cdot\,,\cdot\rangle_a$ are non-degenerate and symmetric for $a \neq 0$ with Gram matrices $R(a)^tG$. Furthermore for $a \neq b$ in $\mathcal{Q}$, the difference of the corresponding Gram matrices

$$R(a)^tG - R(b)^tG = (R(a) - R(b))^tG$$

is regular. Thus $\{R(a)^tG \mid a \in \mathcal{Q}\}$ is a symmetric MRD code which is equivalent to $\mathcal{C}$.

Conversely suppose that the equivalence class of $\mathcal{C}$ contains a symmetric code. Thus we may assume that there are regular matrices $X$ and $Y$ such that $\{XR(a)Y \mid a \in \mathcal{Q}\}$ consists of symmetric matrices. (The second type of equivalence in Theorem 1 leads to the same just by taking transpose matrices.) Since $R(e)$ is the identity matrix we have $(XY)^t = XY$, hence $Z = YX^{-t} = X^{-1}Y^t = Z^t$. Let $\langle\cdot\,,\cdot\rangle$ be the standard symmetric non-degenerate bilinear form on the $K$-vector space $\mathcal{Q}$. Thus the non-degenerate bilinear form $\langle\cdot\,,\cdot\rangle_Z$ defined by

$$\langle x, y\rangle_Z \;=\; \langle x, yZ\rangle$$

is symmetric. From $(XR(a)Y)^t = Y^tR(a)^tX^t = XR(a)Y$ we get

$$X^{-1}Y^tR(a)^t = R(a)YX^{-t},$$

hence $ZR(a)^t = R(a)Z$. It follows

$$\langle x\circ a, y\rangle_Z = \langle xR(a), yZ\rangle = \langle x, yZR(a)^t\rangle = \langle x, yR(a)Z\rangle = \langle x, y\circ a\rangle_Z$$

and $\langle\cdot\,,\cdot\rangle_Z$ is invariant.

□

**Remark 3.** a) In finite geometry Theorem 6 can be stated as follows [11]: The translation plane associated to a quasifield $\mathcal{Q}$ is symplectic if and only if $\mathcal{Q}$ admits a non-degenerate invariant symmetric bilinear form.
b) According to ([11], Theorem 4.2), $\mathcal{Q}$ admits a non-degenerate invariant symmetric bilinear form over $\mathrm{Ker}\,\mathcal{Q}$ if and only if the additive group generated by $\{(xy)z - x(zy) \mid x, y, z \in \mathcal{Q}\}$ is a proper subgroup of $(\mathcal{Q}, +)$.

c) Symmetric MRD codes have been explicitly constructed by Kai-Uwe Schmidt in [16].

## 5. Finite nearfields

Finite nearfields have been classified by Zassenhaus (see [18], or section 5.5.2 in [5]). These are the regular quasifields, usually denoted by $N(n,q)$, and seven exceptional cases. The quasifields $N(n,q)$ exist for all $q$ and $n$, provided all prime divisors of $n$ divide $q-1$ and $4 \nmid n$ in case $q \equiv 3 \pmod 4$. Note that $N(n,q)$ is not a field if $n > 1$, and $N(1,q) = \mathbb{F}_q$. Moreover, the center of $N(n,q)$ is $\mathbb{F}_q$. If $\mathcal{C}$ is the MRD code corresponding to $N(n,q)$ for $n > 1$ then $\mathcal{C}^* = \mathcal{C} \setminus \{0\}$ is a nonabelian group of order $q^n - 1$ whereas in the class of Gabidulin codes this group is cyclic of order $q^n - 1$. We demonstrate one of the exceptional cases in the next example.

**Example 2.** Let $Q$ be the subgroup of $GL(2,11)$ generated by $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 2 & 4 \\ 1 & -3 \end{pmatrix}$. One easily checks that $Q \cong \mathrm{SL}(2,5)$. Furthermore $Q$ acts regularly on the non-zero vectors of $V(2,11)$. Thus $\mathcal{C} = Q \cup \{0\}$ is an MRD code in $(\mathbb{F}_{11})_{2,2}$. The orders of elements of $Q$ are $1,2,3,4,5,6$ and $10$. Since $E + A$ has order 40, the rank metric code $\mathcal{C}$ is not additively closed.

## 6. MRD codes with $k > 1$ and $n = m$

**Example 3.** Using Magma we see that $(\mathbb{F}_3)_{3,3}$ contains two equivalence classes of linear MRD codes with minimum distance $d = n - k + 1 = 2$. One of them represents the Gabidulin code $\mathcal{G}$ and has the following matrices as a basis.

$$\begin{pmatrix} 1&0&0 \\ 0&0&0 \\ 0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0 \\ 0&0&0 \\ 1&2&1 \end{pmatrix}, \begin{pmatrix} 0&0&1 \\ 0&0&0 \\ 0&1&2 \end{pmatrix}, \begin{pmatrix} 0&0&0 \\ 1&0&0 \\ 0&0&2 \end{pmatrix}, \begin{pmatrix} 0&0&0 \\ 0&1&0 \\ 0&2&1 \end{pmatrix}, \begin{pmatrix} 0&0&0 \\ 0&0&1 \\ 2&1&0 \end{pmatrix}.$$

The other class contains a code $\mathcal{C}$ which has the following basis.

$$\begin{pmatrix} 1&0&0 \\ 0&0&0 \\ 1&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0 \\ 0&0&0 \\ 0&0&2 \end{pmatrix}, \begin{pmatrix} 0&0&1 \\ 0&0&0 \\ 2&0&2 \end{pmatrix}, \begin{pmatrix} 0&0&0 \\ 1&0&0 \\ 1&2&1 \end{pmatrix}, \begin{pmatrix} 0&0&0 \\ 0&1&0 \\ 2&2&1 \end{pmatrix}, \begin{pmatrix} 0&0&0 \\ 0&0&1 \\ 1&2&2 \end{pmatrix}.$$

The only semifield of order 27 has the Frobenius map $x \mapsto x^3$ in $\mathbb{F}_{27}$ as a semifield automorphism and we may use the Gabidulin construction over the semifield to get a rank metric code $\mathcal{C}'$. However, up to equivalence we do not get the above code since $\mathcal{C}'$ contains matrices of rank 1. Note that the rank distribution of $\mathcal{C}$ and the corresponding Gabidulin code coincide, consistently with Theorem 5.6 of [4]. There are exactly 338 matrices of rank 2 and 390 of rank 3. Furthermore, if we consider the matrices of $\mathcal{C}$ as vectors in $\mathbb{F}_{27}^3$ we obtain an MDS code which is not linear over $\mathbb{F}_{27}$ in contrast to the corresponding Gabidulin code.

Nevertheless we would like to mention here that both $\mathcal{G}$ and $\mathcal{C}$ are equivalent to their duals (see [15], Proposition 5.9). The duality is defined with respect to the bilinear form

$$\langle A, B \rangle = \mathrm{tr}(AB^t)$$

for $A, B \in (\mathbb{F}_3)_{3,3}$.

## Acknowledgement

We would like to thank Peter Müller who brought the connection of MRD codes in $(K)_{n,n}$ of minimum distance $n$ with spreadsets to our attention. Furthermore, we would like to thank Thomas Honold who told us about the book [17] and Hua's result. Finally, the authors appreciated valuable discussions with John Sheekey at the ALCOMA15 meeting at Banz. Special thanks goes to the anonymous referees which we owe some improvements.

## References

[1] W. Bosma, J. Cannon, and C. Playoust. *The Magma algebra system. I. The user language.* J. Symbolic Comput., **24** 3-4 (1997), 235–265.
[2] R.H. Bruck and R.C. Bose, *The construction of translation planes from projectives spaces.* J. Algebra **1** (1964), 85–102.
[3] M. Cordero and G.P. Wene, *A survey of finite semifields.* Discrete Math. **208/209** (1999), 125–137.
[4] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory.* J. Comb. Theory A **25** (1978), 226–241.
[5] P. Dembowski, *Finite Geometries.* Springer 1968.
[6] E.M. Gabidulin, *Theory of codes with maximal rank distance.* Probl. Inform. Transm. **21** (1985), 1–12.
[7] E.M. Gabidulin and N.I. Pilipchuk, *Symmetric matrices and codes correcting rank errors beyond the* $\lfloor \frac{d-1}{2} \rfloor$ *bound.* Discrete Appl. Math. **154** (2006), 305–312.
[8] `http://www.math.uni-kiel.de/geometrie/klein/math/geometry.html`
[9] *Handbook of finite translation planes.* Eds. M. Johnson, V. Jha and M. Biliotti, Chapman and Hall/CRC 2007.
[10] W.M. Kantor, *Finite semifields.* In: Finite geometries, groups, and computation, Walter de Gruyter, Berlin, 2006, 103–114.
[11] N. Knarr, *Quasifields of symplectic translation planes.* J. of Comb. Theory Serie A **116** (2009), 1080–1086.
[12] D.E. Knuth, *Finite semifields and projectives planes.* Thesis, California Inst.of Technology, Pasadena 1963.
[13] M. Lavrauw and O. Polverino, *Finite semifields.* Chapter in *Current research topocs in Galois geometry* (Eds. J.de Beule and l. Storme), NOVA Academic Publishers, New York 2011.
[14] K. Morrison, *Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes.* `arXiv:1304.0501v1`, 2013.
[15] G. Nebe and W. Willems, *On self-dual MRD codes.* `arXiv:1505.07237`, 2015
[16] K.-U. Schmidt, *Symmetric bilinear forms over finite fields with applications to coding theory.* `arXiv:1410.7184`, 2014.
[17] Z.-X. Wan, *Geometry of matrices.* In memory of Professor L. K. Hua (1910–1985), World Scientific, Singapore 1996.
[18] H. Zassenhaus, *Über endliche Fastkörper.* Abh. Math. Sem. Univ.Hamburg **11** (1936), 187–220.