A new family of linear maximum rank distance codes

John Sheekey

April 8, 2015

Abstract

In this article we construct a new family of linear maximum rank distance (MRD) codes for all parameters. This family contains the only known family, the Gabidulin codes, and contains codes inequivalent to the Gabidulin codes. We also calculate the automorphism group of these codes, including the automorphism group of the Gabidulin codes.

1 Preliminaries

1.1 Rank metric codes

Delsarte introduced rank metric codes in [8]. A rank metric code $C$ is a subset of a matrix space $M = M_{m \times n}(\mathbb{F})$, $\mathbb{F}$ a field, equipped with the distance function $d(X, Y) := \text{rank}(X - Y)$. A rank metric code is called $\mathbb{F}_0$-linear if it forms an $\mathbb{F}_0$-subspace of $M$ for some subfield $\mathbb{F}_0 \leq \mathbb{F}$. A maximum rank distance code (MRD-code) is a rank metric code over a finite field $\mathbb{F}_q$ meeting the Singleton-like bound $|C| \leq q^{n(m-d+1)}$, where $d$ is the minimum distance of $C$. If $C$ is an $\mathbb{F}_q$-linear MRD code in $M_{m \times n}(\mathbb{F}_q)$ with $d = m - k + 1$ for a subfield $\mathbb{F}_q$, we say that $C$ has parameters $[nm, nk, m - k + 1]$, with the subscript omitted when there is no ambiguity.

Delsarte [8] and Gabidulin [11] constructed linear MRD-codes over the finite field $\mathbb{F}_q$ for every $k, m$ and $n$. In the literature these are usually called (generalised) Gabidulin codes, although the first construction was by Delsarte. When $n = m$ and $k = 1$, MRD-codes correspond to algebraic structures called quasifields, see Subsection 1.2. Cossidente-Marino-Pavese [6] recently constructed non-linear MRD-codes for $n = m = 3$, $k = 2$. When $n = m$ and $1 < k < n - 1$, no other linear MRD-codes were known. In this paper we will construct a new family of linear MRD-codes for each $k$, and we will show that they contain codes inequivalent to the generalised Gabidulin codes.

A good overview of MRD-codes can be found in [28]. Similar problems for symmetric, alternating and hermitian matrices have been studied in for example [12], [29], [16], [14].

1.2 (Pre)semifields and quasifields

A finite presemifield is a division algebra in which multiplication is not necessarily associative; if a multiplicative identity element exists, it is called a semifield. We refer to [20] for background, definitions, and terminology. Presemifield are studied in equivalence classes known as isotopy classes. Presemifields of order $q^n$ with centre containing $\mathbb{F}_q$, $\mathbb{F}_0$ and left nucleus containing $\mathbb{F}_q$ are in one-to-one correspondence with $[n^2, n, n]_{\mathbb{F}_0}$ MRD-codes in $M_n(\mathbb{F}_q)$ (i.e. $\mathbb{F}_q$-linear MRD-codes with $k = 1$). In the theory of semifields, such spaces are called semifield spread sets. Many constructions for finite semifields are known, see for example [18] and [20]. There are two important operations defined on presemifields; the dual, which is the opposite algebra, and the transpose. These together form a chain of six (isotopy classes of) semifields, known as the Knuth orbit.
A quasifield is an algebraic structure satisfying the axioms of a division algebra, except perhaps left distributivity. Quasifields are in one-to-one correspondence with MRD-codes with \( k = 1 \) which are not necessarily linear (see [9]). Explicit statements of the correspondence between semifields, quasifields and MRD-codes can be found in [7].

1.3 Equivalence

There are different concepts of equivalence for rank metric codes, see for example [26]. In this paper, two rank metric codes \( C, C' \subset M_n(F_q) \) will be said to be equivalent if there exist invertible \( F_q \)-linear transformations \( A, B \) and a field automorphism \( \rho \in \text{Aut}(F_q) \) such that \( C' = AC\rho B := \{ AX\rho B : X \in C \} \) where \( X\rho \) is the matrix obtained from \( X \) by applying \( \rho \) to each entry. Note that each of these operations preserve the rank distance, and they form a group. The subgroup fixing \( C \) is called the automorphism group of \( C \), and is denoted by \( \text{Aut}(C) \).

We call the set \( \hat{C} := \{ \hat{X} : X \in C \} \) the adjoint of \( C \), where \( \hat{X} \) denotes the adjoint of \( X \) with respect to some non-degenerate symmetric bilinear form. This form is often chosen so that the adjoint is precisely matrix transposition, though we will not assume this. Note that taking the adjoint also preserves rank distance, and is often included in the definition of equivalence. However we find it more convenient to omit it, and if \( C \) is equivalent to \( \hat{C} \), we say that \( C \) and \( C' \) are adjoint-equivalent.

When \( k = 1 \) and \( C_1, C_2 \) are linear, equivalence corresponds precisely to the presemifields associated to each code \( C_i \) being isotopic, while adjoint-equivalence corresponds to one presemifield being isotopic to the transpose of the other.

1.4 Subspace codes

A subspace code is a set of subspaces of a vector space, with the distance function \( d_s(U, V) = \dim(U) + \dim(V) - 2\dim(U \cap V) \). If all elements of the code have the same dimension, it is called a constant dimension code. These codes were introduced by Kotter and Kschischang [19], and have applications in random network coding. Rank metric codes define constant dimension subspace codes in the following way (see for example [13]). Given a matrix \( X \) we define the subspace \( S_X = \{ (u, Xu) : u \in F_q^n \} \) of \( F_q^{2n} \). Clearly, each \( S_X \) is \( n \)-dimensional, and \( d_s(S_X, S_Y) = 2\text{rank}(X - Y) \). Hence an MRD-code with minimum distance \( d \) defines a subspace code with minimum distance \( 2d \). This is known as a lifted MRD-code [30]. However, not every subspace code defines an MRD-code when \( d < n \), see for example [17]. Many of the best known constructions are constructed by perturbing a lifted Gabidulin code. In the case \( d = n \), we have the well-known correspondence between spreads and quasifields, and in the linear case between semifield spreads and semifields.

1.5 Delsarte’s duality theorem

Define the symmetric bilinear form \( b \) on \( M_{m,n}(F) \) by

\[
b(X, Y) := \text{tr}(\text{Tr}(XY^T)),
\]

where \( \text{Tr} \) denotes the matrix trace, and \( \text{tr} \) denotes the absolute trace from \( F_q \) to \( F_p \), where \( p \) is prime and \( q = p^e \). Define the Delsarte dual \( C^\perp \) of an \( F_p \)-linear code \( C \) by

\[
C^\perp := \{ Y : Y \in M_{m,n}, b(X, Y) = 0 \ \forall X \in C \}.
\]

We choose the name Delsarte dual to distinguish from the notion of dual in semifield theory. Delsarte [8, Theorem 5.5] proved the following theorem, using the theory of association schemes. An elementary proof can be found in [28].
Theorem 1. [8, Theorem 5.5] Suppose $C$ is an $[nm, nk, m - k + 1]_p$ MRD code in $M_{m \times n}(\mathbb{F}_q)$. Then the Delsarte dual $C^\perp$ is an $[nm, n(m - k), k + 1]_p$ MRD code in $M_{m \times n}(\mathbb{F}_q)$.

Note that when $n = m = 2$, $k = 1$, both $C$ and $C^\perp$ are semifield spread sets (and correspond to rank two semifields, see [21]). In the context of semifields, this operation is known as the translation dual, see [22], and is a special case of the switching operation defined in [9].

It is clear that two codes $C$ and $C'$ are equivalent if and only if $C^\perp$ and $C'^\perp$ are equivalent; this was shown in [22] for semifield spread sets, the same proof works for this more general statement. Hence the classification of $[n^2, n^2 - n, 2]_q$-codes is equivalent to the classification of semifields of order $q^n$ with nucleus containing $\mathbb{F}_q$ and centre containing $\mathbb{F}_{q^r}$ up to isotopy.

Furthermore, as semifields of order $q^3$ with centre containing $\mathbb{F}_q$ have been fully classified by Menichetti [24], we have a full classification of all $\mathbb{F}_q$-linear MRD codes in $M_3(\mathbb{F}_q)$: they are either the spread sets corresponding to a field or a generalised twisted field, or the Delsarte dual of one of these. Precise conditions for the equivalence of spread sets arising from generalised twisted fields can be found in [4].

2 Linearized polynomials, and properties of the Gabidulin code

Let us identify the vector space $V(n, q)$ with the elements of $\mathbb{F}_{q^n}$. It is well known that every $\mathbb{F}_q$-linear transformation from $\mathbb{F}_{q^n}$ to itself may be represented by a unique linearized polynomial of $q$-degree at most $n - 1$: that is,

$$M_n(\mathbb{F}_q) \cong L_n := \{ f_0x + f_1x^q + \ldots + f_{n-1}x^{q^{n-1}} : f_i \in \mathbb{F}_{q^n} \}.$$ 

Recall that the $q$-degree is the maximum $i$ such that $f_i \neq 0$. These linearized polynomials form a ring isomorphic to $M_n(\mathbb{F}_q)$, with the multiplication being composition modulo $x^{q^n} - x$ (which we will denote by $\circ$, or simply by juxtaposition when the meaning is clear).

It is obvious that a linearized polynomial of $q$-degree $k$ has rank at least $n - k$. In fact, a linearized polynomial of the form

$$f_0x + f_1x^{q^1} + \ldots + f_{k-1}x^{q^{k-1}}$$

has rank at least $n - k$, for any $s$ relatively prime to $n$. Let $\mathcal{G}_{k,s}$ denote the set of linearized polynomials of this form, for a fixed $s$ and $k$. These are the generalised Gabidulin codes [11], and are MRD-codes with dimension $nk$ and minimum rank-distance $n - k + 1$.

Define $\mathcal{G}_k = \mathcal{G}_{k,1}$, which is then the set of linearized polynomials of degree at most $k - 1$, i.e.

$$\mathcal{G}_k := \{ f_0x + f_1x^{q^1} + \ldots + f_{k-1}x^{q^{k-1}} : a_i \in \mathbb{F}_{q^n} \}.$$ 

These were first constructed by Delsarte [3]. Each code $\mathcal{G}_{1,s}$ is a semifield spread set corresponding to the field $\mathbb{F}_{q^n}$.

Remark 1. Rank metric codes are sometimes viewed as codes in $(\mathbb{F}_{q^n})^n$. The theories are basically identical (see e.g. [23]), with the main difference being that codes in this context are called linear if the corresponding set of linearized polynomials form an $\mathbb{F}_{q^n}$-subspace of $L_n$. Clearly the generalised Gabidulin codes are all $\mathbb{F}_{q^n}$-linear. Note however that $\mathbb{F}_{q^n}$-linearity is not preserved by the equivalence as defined in this paper.

The action of $\text{Aut}(\mathbb{F}_q)$ on $M_n(\mathbb{F}_q)$ can be translated to an action on $L_n$ as follows. Given a linearized polynomial $f$ and an automorphism $\rho$ of $\mathbb{F}_q$, we define $f^\rho(x) = f(x^\rho)$. If $q = p^s$ for $p$ a prime, and $x^\rho = x^{p^s}$, then $f^\rho = x^\rho \circ f \circ x^{p^{n-1}}$. Hence any automorphism of a code $C$ can be written as $(f \circ x^{p^s}, x^{p^{n-1}} \circ g)$ for some linearized polynomials $f, g$. 

3
The set $S := \{ ax : a \in \mathbb{F}_q^* \}$ is a subgroup of $\text{GL}(n, q)$ isomorphic to $\mathbb{F}_q^*$, and is what is known as a Singer cycle. Then $G_k$, is fixed under the actions of $S$ defined by $f \mapsto (ax) \circ f$ and $f \mapsto f \circ (ax)$, for $a \in \mathbb{F}_q^*$. It is also fixed by $f \mapsto x^p \circ f \circ x^{p^{n-1}}$, and hence by the group

$$\{(ax^i, bx^{n-1-i}) : \alpha, \beta \in \mathbb{F}_q^*, i \in \{0, \ldots, n-1\}\}.$$

We will show later that this is in fact the full stabiliser of $G_k$ for each $k$.

The adjoint of a linearized polynomial $a = \sum_{i=0}^{n-1} a_ix^i$ with respect to the symmetric bilinear form $(a, b) \mapsto \text{Tr}(ab)$ is given by $\hat{a} = \sum_{i=0}^{n-1} a_iq^{-i}x^{i}$. It is easy to check that $x^k \circ \hat{G}_k = G_k$, and hence we have the following.

**Lemma 1.** Each Gabidulin code $G_k$ is equivalent to its adjoint $\hat{G}_k$.

We define the bilinear form $b$ on linearized polynomials by

$$b\left(\sum_{i=0}^{n-1} f_i x^i, \sum_{i=0}^{n-1} g_i x^i\right) = \text{tr}\left(\sum_{i=0}^{n-1} f_i g_i\right).$$

Note that $\sum_{i=0}^{n-1} f_i g_i$ is the coefficient of $x$ in $f \hat{g}$. The following Lemma is immediate.

**Lemma 2.** The Delsarte dual $G_k^\perp$ of a Gabidulin code $G_k$ is equivalent to $G_{n-k-1}$.

Note also that the Gabidulin codes form a chain:

$$G_1 \leq G_2 \leq \cdots \leq G_{n-1} \simeq M_n(\mathbb{F}_q).$$

We now consider which subspaces of a Gabidulin code $G_k$ are equivalent to another Gabidulin code $G_r$.

**Theorem 2.** A subspace $U$ of $G_k$, $k \leq n-1$, is isotopic to $G_r$ if and only if there exist invertible linearized polynomials $f, g$ such that $U = fG_r g = \{ f \circ a \circ g : a \in G_r \}$, where $f_0 = 1$, and $\deg_q(f) + \deg_q(g) \leq k - r$.

**Proof.** Clearly if $f$ and $g$ are invertible linearized polynomials satisfying the condition on degrees, then $U$ is contained in $G_k$, and isotopic to $G_r$.

Note that for any $0 \neq \beta \in \mathbb{F}_q^*$ and any $j \in \{0, \ldots, n-1\}$, we have that $\{ f \circ a \circ g : a \in G_r \} = \{ f \circ (\beta x^j) \circ a \circ (\beta^{-1} x^{q^m-j}) \circ g : a \in G_r \}$, and hence we may assume without loss of generality that $f_0 = 1$.

Consider $f \circ ax^j \circ g$, where $a \in \mathbb{F}_q^*$. Then the coefficient of $x^m$ is

$$a_{m-j}(\alpha) := \sum_{i=0}^{n-1} f_i g_{m-i-j} \alpha^{q^i},$$

where indices are taken modulo $n$. If $U$ is contained in $G_k$, we must have that for each $m \geq k$, $j \leq r-1$, $a_m(\alpha)$ is zero for every $\alpha \in \mathbb{F}_q^*$. Hence for all $m \geq k$, $j \leq r-1$ and $i \in \{0, \ldots, n-1\}$ we have that

$$f_i g_{m-i-j} = 0.$$

As $f_0 \neq 0$, we get that $g_m = 0$ for all $m \geq k$. Let $\deg_q(f) = s$, $\deg_q(g) = t$, and so $f_s g_t \neq 0$. Then $g_{m-s-r+1} = 0$ for all $m \in \{k, \ldots, n-1\} \neq 0$, and hence $t \leq k - s - r$, proving the claim. \hfill \square

In [26, Proposition IV.7] it was shown that the group $\{(ax, \beta x) : \alpha, \beta \in \mathbb{F}_q^* \}$ is a subgroup of the automorphism group of $G_k$. Note that the result in [26, Theorem IV.4] refers to a different definition of equivalence to the definition used in this paper. We now give a complete description of the automorphism group of the Gabidulin codes.
Theorem 3. The automorphism group of the Gabidulin code $G_k$ is given by

\[ \{(\alpha x^i, \beta x^{q^k-i}) : \alpha, \beta \in \mathbb{F}_q^n, i \in \{0, \ldots, n-1\}\} \]

Proof. Clearly the given group is a subgroup of the automorphism group of $G_k$. Suppose $fG_k^0g = G_k$ for some invertible linearized polynomials $f, g$ and some $\rho \in \text{Aut}(\mathbb{F}_q)$. As $G_k^0 = G_k$ for all $\rho \in \text{Aut}(\mathbb{F}_q)$, we may assume that $\rho$ is the identity. Then $f = f' \circ (\alpha x^i)$ for some $\alpha \in \mathbb{F}_q^n$, $i \in \{0, \ldots, n-1\}$, where $f'$ such that $f'_0 = 1$. Let $g' = x^i \circ g$. Then $f'G_kg' = G_k$, and by the proof of Theorem 2 we must have $\text{deg}_q(f') + \text{deg}_q(g') = 0$. Hence $f' = x$ and $g' = \beta x^i x$ for some $\beta \in \mathbb{F}_q^n$, and so $(f, g) = (\alpha x^i, \beta x^{q^k-i})$, proving the claim.

Remark 2. An analogous proof shows that the automorphism group of any generalised Gabidulin code $G_{k,s}$ is equal to the automorphism group of $G_k$.

3 Construction of new linear MRD-codes

The following Lemma is key to our construction. The result also follows from [15, Theorem 10].

Lemma 3. Suppose $f$ is a linearized polynomial of $q$-degree $k$. If $f$ has rank $n - k$, then $N(f_0) = (-1)^{kn}N(f_k)$.

Proof. Any $k$-dimensional $\mathbb{F}_q$-subspace $U$ of $\mathbb{F}_q^n$ is annihilated by a unique monic linearized polynomial of degree $k$, denoted by $m_U$ and called the minimal polynomial of $U$. Every linearized polynomial of degree $k$ annihilating $U$ is an $\mathbb{F}_q^n$-multiple of $m_U$, and hence it suffices to prove the result for any particular linearized polynomial of degree $k$ annihilating $U$.

We proceed by induction on $k$. If $k = 1$ and $U = \langle \alpha \rangle$, then $U$ is annihilated by $\alpha x - \alpha x$, and so the case $k = 1$ holds. Suppose the case $k - 1$ holds. Let $\{\alpha_1, \ldots, \alpha_k\}$ be an $\mathbb{F}_q$-basis for $U$, and let $U' = \langle \alpha_1, \ldots, \alpha_{k-1} \rangle$. Define $g := m_{U'}$, and $f := (g(\alpha_k)x - g(\alpha_k)x) \circ g$. Then $f$ annihilates $U$. Now $f_k = g(\alpha_k)g_{k-1}^0$ and $f_0 = -g(\alpha_k)^qg_0$. By the induction hypothesis, $N(g_{k-1}) = (-1)^{(k-1)n}N(g_0)$, and so the result follows.

Theorem 4. Let $H_k(\eta, h)$ denote the set of linearized polynomials of degree at most $k \leq n - 1$ satisfying $f_k = \eta f_0^h$, with $\eta$ such that $N(\eta) \neq (-1)^{nk}$, i.e.

\[ H_k(\eta, h) := \{f_0 x + f_1 x^q + \ldots + f_{k-1} x^{q^{k-1}} + \eta f_0^h x^q : a_i \in \mathbb{F}_q^n\} \]

Then each $H_k(\eta, h)$ is an MRD-code with the same parameters as $G_k$.

Proof. It is clear that $H_k(\eta, h)$ has dimension $nk$ over $\mathbb{F}_q$. As $\text{deg}(f) \leq q^k$ for all $f \in H_k(\eta, h)$, we have that $\text{rank}(f) \geq n - k$. By Lemma 4, $\text{rank}(f) > n - k$, and hence $\text{rank}(f) \geq n - k + 1$ for all $f \in H_k(\eta, h)$. It follows that $H_k(\eta, h)$ is an MRD-code with parameters $[n^2, nk, n - k + 1]$, as claimed.

Theorem 5. The adjoint of $H_k(\eta, h)$ is equivalent to $H_k(\eta^{-q^{k-h}}, k - h)$, and the Delsarte dual satisfies $H_k(\eta, h)^\perp = H_{n-k}(-\eta^{q^{n-h}}, n - h)$.

Proof. This follows from a straightforward calculation.

Note that $H_k(0, h) = G_k$, so this family includes the Gabidulin codes. We now prove that there are new MRD-codes in this family. First we require the following lemma.

Lemma 4. Suppose $\eta \neq 0$. Then there is a unique subspace of $H_k(\eta, h)$ equivalent to $G_{k-1}$, unless $k \in \{1, n - 1\}$, or $k = 2$ and $h \leq 2$.  

5
Proof. Note that \( H_k(\eta, h) \) is contained in \( G_{k+1} \). Suppose \( U \) is a subspace of \( H_k(\eta, h) \) equivalent to \( G_{k-1} \). Then by Theorem 2, \( U = fG_{k-1}g \) for some \( f, g \) with \( f \neq 0 \) and \( \deg(f) + \deg(g) \leq 2 \).

If \( \deg(f) = s \), then \( \deg(g) \leq 2 - s \). Let \( b = \sum_{i=0}^{k-2} b_i x^i \) be a generic element of \( G_{k-1} \). Then the coefficient of \( x^i \) in \( f g \) is \( a_{i, j}^{\ell} b_j \), while the coefficient of \( x^i \) in \( \eta^h \) is \( \alpha_{i, j}^{\ell} b_j \). Hence we must have \( \eta(b_0 f_0 g_0)^i = b_{i, j}^{\ell} f_0 g_0^{\ell} \) for all \( b_0, b_{k-2} \in \mathbb{F}_{q^n} \). As \( \eta \neq 0 \) and \( f_0, f_s \neq 0 \), if \( k = 2 \) this is possible if and only if \( g_0 = g_{2-s} = 0 \). Hence \( s = 0, \) \( g = g_1 x^q \), implying \( U = G_{k-1} / x^q \), proving the claim.

If \( k = 2 \), we get \( \eta(b_0 f_0 g_0)^i = b_{0}^{\ell} f_0 g_0^{\ell} \) for all \( b_0 \in \mathbb{F}_{q^n} \), which is possible only if \( h = s \leq 2 \).

This lemma allows us to calculate the automorphism group, and hence prove that the family \( H_k(\eta, h) \) contains codes equivalent to any generalised Gabidulin code, and therefore contains new MRD codes.

**Theorem 6.** Suppose \( k \notin \{1, n-1 \}, \eta \neq 0 \). Then the automorphism group of \( H_k(\eta, h) \) is

\[
\{ (ax^\nu, bx^{\nu-a}) : \alpha, \beta \in \mathbb{F}_{q^n}, \alpha^{1-q^h} (\beta^{q^h-q^h} p^i \eta^{p^i}) = \eta \}
\]

Hence \( H_k(\eta, h) \) is not equivalent to \( G_{k,s} \) unless \( k \in \{1, n-1 \} \) and \( h \in \{0, 1 \} \). Furthermore, \( H_k(\eta, h) \) is equivalent to \( H_k(\nu, j) \) if and only if \( j = h \) and there exist \( \alpha, \beta \in \mathbb{F}_{q^n} \) such that \( \nu = \alpha^{1-q^h} (\beta^{q^h-q^h}) p^i \eta^{p^i} \).

Proof. Suppose first that \( k \neq 2 \). By Lemma 4 there is a unique subspace of \( H_k(\eta, h) \) equivalent to \( G_{k-1} \).

Hence any isomorphism from \( H_k(\eta, h) \) to \( H_k(\nu, j) \) is also an automorphism of \( G_{k-1} \). By Theorem 3 these are all of the form \( (ax^\nu, bx^{\nu-a}) \) for some \( \alpha, \beta \in \mathbb{F}_{q^n}, i \in \{0, \ldots, n-1 \} \).

Now the coefficient of \( x \) in a generic element of \( (ax^\nu) \circ (\beta x^{\nu-a}) = \alpha \beta^{q^{k-1}} (\eta f_0^q)^i \), while the coefficient of \( x^q \) is \( \alpha \beta^{q^{k+1}} (\eta f_0^{q^i})^i \). Hence for this to lie in \( H_k(\nu, j) \) we must have \( \alpha \beta^{q^{k+1}} (\eta f_0^q)^i = \nu (\alpha \beta^{q^{k+1}} (\eta f_0^{q^i})^i \) for all \( f_0 \in \mathbb{F}_{q^n} \). This occurs if and only if \( j = h \) and \( \alpha \beta^{q^{k+1}} (\eta f_0^q)^i = \nu (\alpha \beta^{q^{k+1}} (\eta f_0^{q^i})^i \), proving the last claim. Setting \( \eta = \nu \) gives the automorphism group of \( H_k(\eta, h) \).

If \( k = 2 < n-1 \), then the result follows by taking into account Theorem 5 and noting that \( \text{Aut}(C^{\perp}) = \{ (f, g) : (f, g) \in \text{Aut}(C) \} \).

It is clear that \( \text{Aut}(H_k(\eta, h)) \) is strictly smaller than \( \text{Aut}(G_{s,k}) \), unless \( \eta = 0 \), proving that \( H_k(\eta, h) \) is not equivalent to \( G_{s,k} \) for \( k \notin \{1, n-1 \} \).

When \( k = 1 \), the code \( H_k(\eta, h) \) is a semifield spread set corresponding to a **generalised twisted field**, as introduced by Albert [1], i.e., a semifield with multiplication \( x \circ y = xy + \eta x^q y^q \), where \( N(-\eta) \neq 1 \). The equivalence and automorphisms of these follow from [4]. By duality, we get the result for \( k = n-1 \), completing the proof.

Remark 3. As noted in the proof above, when \( k = 1 \), the code \( H_k(\eta, h) \) is a semifield spread set corresponding to a **generalised twisted field**, see [1]. For this reason we propose to name this family of codes **twisted Gabidulin codes**.

Remark 4. Note that when we view \( H_k(\eta, h) \) as a code in \( (\mathbb{F}_{q^n})^n \), it is \( \mathbb{F}_{q^n} \)-linear if and only if \( h = 0 \).

Remark 5. The special case \( H_2(\eta, 1) \) was discovered independently in [24].
Remark 7. Suppose $f : K$ space-time coding with multiplication. However it does not necessarily hold that if $M$ MRD-codes exist in $H$ property is of the form $\eta, h$ (1). It is clear that the analogue of Lemma 3 holds in this case; that is, the rank of $n$ is an $\eta, h \in K$ and $\mathcal{H}(\eta, h)$ by definition. Note that for each pair $(\phi_1, \phi_2)$, the code $\mathcal{H}(\phi_1, \phi_2)$ is contained in $G_k$ and contains $G_{k-1} \times \phi_2$, and every MRD-code satisfying this property is of the form $\mathcal{H}(\phi_1, \phi_2)$ for some $\phi_1, \phi_2$. Note also that every such $(\phi_1, \phi_2)$ defines a presemifield, with multiplication $x \phi_1(y) + x^0 \phi_2(y)$.

Remark 6. Let $\phi_1, \phi_2$ be linearized polynomials. Define $\mathcal{H}_k(\phi_1, \phi_2)$ to be the set of linearized polynomials of degree at most $k$ with $f_0 = \phi_1(a)$, $f_k = \phi_2(a)$. Then $\mathcal{H}_k(\phi_1, \phi_2)$ is an MRD-code with parameters $[n^2, nk, n - k + 1]$ if and only if $N(\phi_1(x)) \neq (-1)^k N(\phi_2(x))$ for all $x \in \mathbb{F}_q^n$. This is equivalent to finding an $(n - 1)$-dimensional subspace in $PG(2n - 1, q)$ disjoint from the hypersurface $Q_{n-1,q} := \{(x, y) : x, y \in \mathbb{F}_q^n, N(x) \neq N(y)\}$. This hypersurface was studied in detail in [21]. The only known pairs of functions $(\phi_1, \phi_2)$ satisfying this condition are equivalent to the pair $(x, \eta x^\alpha)$, and $\mathcal{H}(x, \eta x^\alpha) = \mathcal{H}(\eta, h)$ by definition. It is clear that the analogue of Lemma 3 holds in this case; that is, the rank of $n$ is an $\eta, h \in \mathbb{F}_q$ and $\mathcal{H}(\eta, h)$ by definition. Note that every such $(\phi_1, \phi_2)$ defines a presemifield, with multiplication $x \phi_1(y) + x^0 \phi_2(y)$.

It is clear that the analogue of Lemma 3 holds in this case; that is, the rank of $f(\sigma)$ is equal to $n - \deg(f)$ only if $N(f_0) = (-1)^k N(f_0)$. Hence the codes $\mathcal{H}_k(\eta, h; \sigma)$ defined as the set of endomorphisms $f(\sigma)$ where $\deg(f) \leq k$ and $f_k = \eta f_0^\sigma$ is also a MRD-code, and an analogous proof shows that is inequivalent to the Gabidulin codes. When $K = \mathbb{F}_q^n$, $F = \mathbb{F}_q$, $x^\sigma = x^\sigma$, this coincides precisely with the generalised Gabidulin codes. These codes in characteristic zero were studied in [2], and have applications to space-time coding.

Remark 8. Given an MRD-code $C$ in $M_n(\mathbb{F})$, one can define a code $\overline{C}$ in $M_{m \times n}(\mathbb{F})$ by deleting the last $(n - m)$ rows from each element of $C$. This turns out to also be an MRD-code, known as a punctured code. However it does not necessarily hold that if $C$ and $C'$ are inequivalent then $\overline{C}$ and $\overline{C'}$ are inequivalent. It is not clear whether or not the punctured codes obtained from $\mathcal{H}_k(\eta, h)$ are inequivalent to those obtained from generalised Gabidulin codes.

4 MRD-codes and scattered linear sets

The projective line $PG(1, q^n)$ is the geometry whose points are 1-dimensional $\mathbb{F}_q^n$-subspaces of $V(2, q^n)$. A linear set of rank $r$ is a set $L(U) := \{u \in \mathbb{F}_q^n : u \in U^\times\} \subset PG(1, q^n)$, where $U$ is an $\mathbb{F}_q$-subspace of $V(2, q^n)$ of dimension $r$. A linear set is said to be scattered if $|L(U)| = \frac{q^n - 1}{q - 1}$. Two linear sets $L(U)$ and $L(U')$ are said to be equivalent if there exists an element of PTL$(2, q^n)$ mapping $L(U)$ to $L(U')$. Given a linearized polynomial $f$, define $U_f := \{(y, f(y)) : y \in \mathbb{F}_q^n\}$. Note that every linear set of rank $n$ is equivalent under PGL$(2, q^n)$ to a set of the form $L(U_f)$. Then $L(U_f)$ is scattered if and only if rank$(f - \beta x) \geq n - 1$ for all $\beta \in \mathbb{F}_q^n$. This occurs if and only if rank$(\alpha f - \beta x) \geq n - 1$ for all $\alpha, \beta \in \mathbb{F}_q^n$. We will call such a polynomial a scattered polynomial. Hence the set $C_f := \{(x, f(x)): x \in \mathbb{F}_q^n\}$ is an MRD-code of dimension $2n$ and minimum distance $n - 1$, i.e. $k = 2$. Furthermore, $C_f$ contains the identity map, and is an $\mathbb{F}_q$-subspace of $L_m$. Indeed, such codes are in one-to-one correspondence with scattered linear sets of rank $n$ on the projective line $PG(1, q^n)$. We show now that the notions of equivalence coincide.

It is straightforward to check that the linear sets $U_f$ and $U_g$ are equivalent if and only if $g = (\alpha f^\rho + \beta x)(\gamma f^\rho + \delta x)^{-1}$ for some $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q^n$, $\rho \in \text{Aut}(\mathbb{F}_q)$, with $\alpha \delta - \beta \gamma \neq 0$ and $(\gamma f^\rho + \delta x)$ invertible. Hence if $L(U_f)$
and $L(U_g)$ are equivalent, then $C_f$ and $C_g$ are equivalent, as
\[
C_g = \langle x, g \rangle_{F_q^n} = \langle x, (\alpha f^\rho + \beta x)(\gamma f^\rho + \delta x)^{-1} \rangle_{F_q^n}
\]
\[
= (\alpha f^\rho + \beta x, \gamma f^\rho + \delta x)_{F_q^n} (\gamma f^\rho + \delta x)^{-1}
\]
\[
= \langle x, f \rangle_{F_q^n} (\gamma f^\rho + \delta x)^{-1} = (C_f)^\rho (\gamma f + \delta x)^{-1}.
\]

For the converse, it can be shown that if $X$ is an invertible linear map, then $XC_f$ is an $F_q^n$-subspace if and only $X(x) = \alpha x^\rho$ for some $\alpha \in F_q^n$ and $\rho \in \Aut(F_q)$, whence $XC_f = C_{f\rho}$. Hence if $C_g = XC_fY$, then $C_g = C_{f\rho}Y$. As the identity is in $C_g$, we get that $Y = C_{f\rho}(\gamma f^\rho + \delta x)^{-1}$ for some $\gamma, \delta \in F_q^n$, and so $C_f$ is equivalent to $C_g$ if and only if $C_g = (C_f)^\rho(\gamma f^\rho + \delta x)^{-1}$. Then the argument from the preceding paragraph can be reversed to show that $U_f$ is equivalent to $U_g$. Hence we have shown the following.

**Theorem 7.** Let $f$ and $g$ be scattered linearized polynomials. Then $L(U_f)$ and $L(U_g)$ are equivalent as linear sets if and only if $C_f$ and $C_g$ are equivalent as MRD-codes.

As far as the author is aware, there are only two known constructions for scattered linear sets of rank $n$ in PG(1, $q^n$). They are $f(x) = x^{q^s}$, $(n, s) = 1$ (Blokhuis-Lavrauw [5]), and $f(x) = x^q + \eta x^{q^n-1}$, with $N(\eta) \neq 1$ (Lunardon-Polverino [23]). The first family leads to generalised Gabidulin codes $G_{2, \eta}$, while the second lead to codes equivalent to $H_2(\eta, 1)$. These are the only $F_q$-linear codes in the family $H_2$, and so we do not obtain any new scattered linear sets from this construction.

### 5 Assorted computational results

In [10] it was shown that the set of elements of minimum rank in an MRD-code is partitioned into constant rank subspaces of dimension $n$, each lying in the annihilator of a subspace of dimension $k - 1$. Hence an MRD-code with $k = 2$ must contain an $n$-dimensional constant rank $n - 1$ subspace of Ann($u$) for each $u$.

Hence we can quickly classify linear MRD-codes with $q = 2, 3, n = 3$, and $k = 2$. First we calculate all constant rank 2 subspaces of Ann($u$) up to equivalence for some chosen $u$, then extend them to MRD-codes and calculate the equivalence classes again. When $q = 2$, there is only the Gabidulin code $G_2$. When $q = 3$, there are precisely two such codes, namely $G_2$ and $H_2$. This in fact follows from Section 1.5.

When $n = 4, q = 2$, there is only one MRD-code with $k = 2$ containing a semifield spread set; the Gabidulin code, an 8-dimensional code of minimum distance 3. The only semifield spread sets it contains are all isotopic to $F_{16}$. There are three isotopy classes of semifields of order 16, i.e. MRD-codes in $M_4(F_q)$ with minimum distance 4. One is maximal as a rank metric code of minimum distance 3. One is contained in a 5-dimensional code of minimum distance 3, but not a 6-dimensional code of minimum distance 3.

All calculations were carried out using the computer algebra package MAGMA.

### References

[1] A.A. Albert. Generalized twisted fields, Pacific J. Math, 11 (1961) 1-8.

[2] D. Augot, P. Loidreau, G. Robert. Rank metric and Gabidulin codes in characteristic zero, Proceedings ISIT 2013, 509-513.

[3] S. Ball, G. Ebert, M. Lavrauw. A geometric construction of finite semifields, J. Algebra 311 (2007), 117-129.

[4] M. Biliotti, V. Jha, N.L. Johnson. The collineation groups of generalized twisted field planes, Geom. Dedicata 76 (1999), 97-126.
[5] A. Blokhuis, M. Lavrauw. Scattered spaces with respect to a spread in $\text{PG}(n, q)$, *Geom. Dedicata* 81 (2000), 231-243.

[6] A. Cossidente, G. Marino, F. Pavese. Non-linear maximum rank distance codes, *preprint*.

[7] J. de la Cruz, M. Kiermaier, A. Wassermann, W. Willems. Algebraic structures of MRD Codes, arXiv:1502.02711.

[8] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory Ser. A* 25 (1978) 226-241.

[9] P. Dembowski. *Finite Geometries*, Springer, 1968.

[10] J.-G. Dumas, R. Gow, G. McGuire, J. Sheekey. Subspaces of matrices with special rank properties, *Linear Algebra Appl.* 433 (2010), 191-202.

[11] E. M. Gabidulin. Theory of codes with maximum rank distance, *Probl. Inf. Transm.* 21 (1985), 1-12.

[12] E. M. Gabidulin, N. I. Pilipchuk. Symmetric rank codes, *Probl. Inf. Transm.* 40 (2004), 103-117.

[13] M. Gadouleau, Z. Yan. Constant-rank codes and their connection to constant-dimension codes, *IEEE Transactions on Information Theory* 56 (2010), 3207-3216.

[14] R. Gow, M. Lavrauw, J. Sheekey, F. Vanhove. Constant rank-distance sets of hermitian matrices and partial spreads in hermitian polar spaces, *Elect. J. Comb.* 21 (2014), P1.26.

[15] R. Gow, R. Quinlan. Galois theory and linear algebra. *Linear Algebra Appl.* 430 (2009), 1778-1789.

[16] R. Gow, R. Quinlan. Galois extensions and subspaces of alternating bilinear forms with special rank properties. *Linear Algebra Appl.* 430 (2009), 2212-2224.

[17] T. Honold, M. Kiermaier, S. Kurz. Optimal binary subspace codes of length 6, constant dimension 3 and minimum subspace distance 4, *Contemporary Mathematics* 632.

[18] W.M. Kantor. *Finite semifields*, Finite geometries, groups, and computation, 103-114, Walter de Gruyter GmbH & Co. KG, Berlin, 2006.

[19] R. Kotter, F.R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. on Inf. Theory*, 54 (2008), 3579-3591.

[20] M. Lavrauw, O. Polverino. *Finite semifields*. Chapter in *Current research topics in Galois Geometry* (Editors J. De Beule and L. Storme), NOVA Academic Publishers, New York, 2011.

[21] M. Lavrauw, J. Sheekey, C. Zanella. On embeddings of minimum dimension of $\text{PG}(n, q) \times \text{PG}(n, q)$, *Des. Codes Cryptogr.*, 74 (2015) 427-440.

[22] G. Lunardon, G. Marino, O. Polverino, R. Trombetti. *Translation dual of a semifield*, J. Combin. Theory Ser. A 115 (2008), 1321-1332.

[23] G. Lunardon, O. Polverino. Blocking sets and derivable partial spreads, *J. Algebr. Comb.* 14 (2001), 49-56.

[24] K. Marshall, A-L. Trautmann. Characterizations of MRD and Gabidulin codes. Conference presentation, ALCOMA15, [http://user.math.uzh.ch/trautmann/ALCOMA_presentation.pdf](http://user.math.uzh.ch/trautmann/ALCOMA_presentation.pdf)

[25] G. Menichetti. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field, *J. Algebra* 47 (1977), 400-410.
[26] K. Morrison. Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes, arXiv:1304.0501v1.

[27] K. Otal, F. Özbudak. Some non-Gabidulin MRD Codes, Conference presentation, ALCOMA15.

[28] A. Ravagnani. Rank-metric codes and their MacWilliams identities, arXiv:1410.1333v2.

[29] K-U. Schmidt. Symmetric bilinear forms over finite fields with applications to coding theory, arXiv:1410.7184v1

[30] D. Silva, F. R. Kschischang, R. Koetter. A rank-metric approach to error control in random network coding, *IEEE Trans. Inform. Theory*, 54 (2008), 3951-3967.