New Criteria for MRD and Gabidulin Codes and some Rank-Metric Code Constructions

Anna-Lena Horlemann-Trautmann[*]

Algorithmics Laboratory, EPF Lausanne, Switzerland

Kyle Marshall[*]

Institute of Mathematics, University of Zurich, Switzerland

1 Introduction

Codes in the rank metric have been studied for the last four decades. For linear codes a Singleton-type bound can be derived for these codes. In analogy to MDS codes in the Hamming metric, we call rank-metric codes that achieve the Singleton-type bound MRD (maximum rank distance) codes. Since the works of Delsarte [4] and Gabidulin [5] we know that linear MRD codes exist for any set of parameters. The codes they describe are called Gabidulin codes.

Moreover, Berger in [1] and Morrison in [12] showed what the linear and semi-linear isometries of rank-metric codes are. It is an open question if there are other general constructions of MRD codes that are not equivalent (under the isometries) to Gabidulin codes. Recently several results have been established in this direction, e.g. in [2, 3, 13], where many of the derived codes are not linear over the underlying field but only linear over some subfield of it. Hence it is still an open question to find other constructions of non-Gabidulin MRD codes.

In this paper we want to derive criteria for MRD and Gabidulin codes and use these to come up with new non-Gabidulin MRD codes that are linear over the original field, not only a subfield. Moreover, we want to give a classification of these codes and investigate how many different equivalence classes of MRD codes we get for small parameters.

This paper is structured as follows. In Section 2 we give some preliminaries on finite fields, rank-metric codes and Gabidulin codes. In Section 3

1

we present a new criterion for MRD codes, in Section 4 we derive a criterion for Gabidulin codes. In Section 5 we use the results of Sections 3 and 4 to find new non-Gabidulin MRD codes for small parameters. We conclude in Section 6.

2   Preliminaries

Let q be a prime power and let $\mathbb{F}_q$ denote the finite field with q elements. It is well-known that there always exists a primitive element α of the extension field $\mathbb{F}_{q^m}$, such that $\mathbb{F}_{q^m} \cong \mathbb{F}_q[\alpha]$. Moreover, $\mathbb{F}_{q^m}$ is isomorphic (as a vector space over $\mathbb{F}_q$) to the vector space $\mathbb{F}_q^m$. One then easily obtains the isomorphic description of matrices over the base field $\mathbb{F}_q$ as vectors over the extension field, i.e. $\mathbb{F}_q^{m \times n} \cong \mathbb{F}_{q^m}^n$. Since we will work with matrices over different underlying fields, we denote the rank of a matrix X over $\mathbb{F}_q$ by $\mathrm{rank}_q(X)$.

Definition 2.1. *The* rank distance d_R *on* $\mathbb{F}_q^{m \times n}$ *is defined by*

$$d_R(X, Y) := \mathrm{rank}_q(X - Y), \quad X, Y \in \mathbb{F}_q^{m \times n}.$$

Analogously, we define the rank distance between two elements $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$ *as the rank of the difference of the respective matrix representations in* $\mathbb{F}_q^{m \times n}$.

In this paper we will focus on $\mathbb{F}_{q^m}$-linear rank-metric codes in $\mathbb{F}_{q^m}^n$, i.e. those codes that form a vector space over $\mathbb{F}_{q^m}$. Whenever we talk about linear codes in this work, we will mean linearity over the extension field $\mathbb{F}_{q^m}$. The well-known Singleton bound for codes in the Hamming metric implies also an upper bound for codes in the rank metric:

Theorem 2.2. *[5, Section 2] Let* $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ *be a linear matrix code with minimum rank distance* d *of dimension* k *(over* $\mathbb{F}_{q^m}$*). Then*

$$k \leq n - d + 1.$$

Definition 2.3. *A code attaining the Singleton bound is called a* maximum rank distance (MRD) *code.*

For some vector $(v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$ we denote the $k \times n$ *Moore matrix* by

$$M_k(v_1, \ldots, v_n) := \begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ v_1^{[1]} & v_2^{[1]} & \ldots & v_n^{[1]} \\ & & \vdots & \\ v_1^{[k-1]} & v_2^{[k-1]} & \ldots & v_n^{[k-1]} \end{pmatrix},$$

where $[i] := q^i$.

Definition 2.4. *Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. We define a Gabidulin code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k as the linear block code with generator matrix $M_k(g_1, \ldots, g_n)$. Using the isomorphic matrix representation we can interpret $\mathcal{C}$ as a matrix code in $\mathbb{F}_q^{m \times n}$.*

Theorem 2.5. *[5, Section4] A Gabidulin code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k over $\mathbb{F}_{q^m}$ has minimum rank distance $n - k + 1$. Thus Gabidulin codes are MRD codes.*

The dual code of a code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is defined in the usual way as

$$\mathcal{C}^\perp := \{ u \in \mathbb{F}_{q^m}^n \mid \boldsymbol{u}\boldsymbol{c}^T = 0 \quad \forall \boldsymbol{c} \in \mathcal{C} \}.$$

In his seminal paper Gabidulin showed the following two results on dual codes of MRD codes:

Proposition 2.6. *[5, Sections 2 and 4]*

1. *Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an MRD code of dimension k. Then the dual code $\mathcal{C}^\perp \subseteq \mathbb{F}_{q^m}^n$ is an MRD code of dimension $n - k$.*

2. *Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a Gabidulin code of dimension k. Then the dual code $\mathcal{C}^\perp \subseteq \mathbb{F}_{q^m}^n$ is a Gabidulin code of dimension $n - k$.*

Note that the second result in Proposition 2.6 was not stated like this in [5]; Gabidulin showed however that the parity check matrix of a Gabidulin code is of the form described in Definition 2.4, which implies the statement. For more information on bounds and constructions of rank-metric codes the interested reader is referred to [5].

The results of Gabidulin (and Delsarte) were later on generalized by Kshevetskiy and Gabidulin in [9] as follows.

Definition 2.7. *Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$ and $s \in \mathbb{N}$ such that $\gcd(s, m) = 1$. We define a generalized Gabidulin code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ as the linear block code with generator matrix*

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[s]} & g_2^{[s]} & \cdots & g_n^{[s]} \\ & & \vdots & \\ g_1^{[s(k-1)]} & g_2^{[s(k-1)]} & \cdots & g_n^{[s(k-1)]} \end{pmatrix}.$$

Theorem 2.8. *[9, Subsection IV.C] A generalized Gabidulin code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k over $\mathbb{F}_{q^m}$ has minimum rank distance $n - k + 1$. Thus generalized Gabidulin codes are MRD codes.*

Similarly to the non-generalized case, Kshevetskiy and Gabidulin also showed the following.

Proposition 2.9. *[9, Subsection IV.C] Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a generalized Gabidulin code of dimension k. Then the dual code $\mathcal{C}^\perp \subseteq \mathbb{F}_{q^m}^n$ is a generalized Gabidulin code of dimension $n - k$.*

Denote by $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ the *Galois group* of $\mathbb{F}_{q^m}$, i.e. the automorphisms of $\mathbb{F}_{q^m}$ that fix the base field $\mathbb{F}_q$. It is well-known that $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is generated by the *Frobenius map*, which takes an element to its q-th power. Hence the automorphisms are of the form $x \mapsto x^{[i]}$ for some $0 \leq i \leq m$. We will denote the respective inverse map, i.e. the $[i]$-th root, by $x \mapsto x^{[-i]}$.

The (semi-)linear rank isometries on $\mathbb{F}_{q^m}^n$ are induced by the isometries on $\mathbb{F}_q^{m \times n}$ and are hence well-known, see e.g. [1, 12, 14]:

Lemma 2.10. *[12, Proposition 2] The semilinear $\mathbb{F}_q$-rank isometries on $\mathbb{F}_{q^m}^n$ are of the form*

$$(\lambda, A, \sigma) \in \left(\mathbb{F}_{q^m}^* \times \mathrm{GL}_n(q)\right) \rtimes \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q),$$

acting on $\mathbb{F}_{q^m}^n \ni (v_1, \ldots, v_n)$ via

$$(v_1, \ldots, v_n)(\lambda, A, \sigma) = (\sigma(\lambda v_1), \ldots, \sigma(\lambda v_n))A.$$

In particular, if $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is a linear code with minimum rank distance d, then

$$\mathcal{C}' = \sigma(\lambda \mathcal{C})A$$

is a linear code with minimum rank distance d.

We denote by $\mathrm{GL}_n(q) := \{A \in \mathbb{F}_q^{n \times n} \mid \mathrm{rank}(A) = n\}$ the general linear group of degree n over $\mathbb{F}_q$. One can easily check that $\mathbb{F}_q$-linearly independent elements in $\mathbb{F}_{q^m}$ remain $\mathbb{F}_q$-linearly independent under the actions of $\mathbb{F}_{q^m}^*, \mathrm{GL}_n(q)$ and $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Moreover, the Moore matrix structure is preserved under these actions, which implies that the class of Gabidulin codes is closed under the semilinear isometries.

In this work we want to classify MRD codes and which of them are generalized Gabidulin codes. For this we will derive some criteria for both the MRD and the Gabidulin property. The following criterion for MRD codes was already given in [5]:

Proposition 2.11. *Let $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$ be a parity check matrix of a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. Then $\mathcal{C}$ is an MRD code if and only if*

$$\mathrm{rank}_{q^m}(VH^T) = n - k$$

for all $V \in \mathbb{F}_q^{(n-k) \times n}$ with $\mathrm{rank}_q(V) = n - k$.

This criterion is formulated with respect to the parity check matrix of a linear code. We can easily derive a criterion for the generator matrix of MRD codes from this:

Corollary 2.12. *Let $G \in \mathbb{F}_{q^m}^{k \times n}$ be a generator matrix of a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. Then $\mathcal{C}$ is an MRD code if and only if*

$$\text{rank}_{q^m}(VG^T) = k$$

for all $V \in \mathbb{F}_q^{k \times n}$ with $\text{rank}_q(V) = k$.

Proof. The generator matrix G of $\mathcal{C}$ is a parity check matrix of the dual code $\mathcal{C}^\perp \subseteq \mathbb{F}_{q^m}^n$ of dimension $n - k$. It follows from Proposition 2.11 that $\mathcal{C}^\perp$ is an MRD code if and only if $\text{rank}_{q^m}(VG^T) = k$ for all $V \in \mathbb{F}_q^{k \times n}$ with $\text{rank}_q(V) = k$. Since $\mathcal{C}$ is MRD if and only if $\mathcal{C}^\perp$ is MRD (see Proposition 2.6), the statement follows. $\square$

Throughout the paper I_k denotes the identity matrix of size k. Furthermore, $\langle v_1, \ldots, v_n \rangle_q$ denotes the $\mathbb{F}_q$-vector space generated by $v_1, \ldots, v_n$.

3 New Criterion for MRD Codes

In this section we give a new criterion to check if a given generator matrix G generates an MRD code. The criterion is stated in Theorem 3.2. Before we can state the main theorem we need the following lemma.

Lemma 3.1. *Any generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ of an MRD code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k has only non-zero maximal minors.*

Proof. Let $V = [\, I_k \mid 0_{k \times (n-k)} \,] \in \mathbb{F}_q^{k \times n}$. Then $\det(VG^T)$ is the maximal minor of G involving the first k columns. By Corollary 2.12 this minor is non-zero. Similarly we can create all other maximal minors of G by multiplication with some $V \in \mathbb{F}_q^{k \times n}$ on the left, which implies, by Corollary 2.12, the statement. $\square$

We can now state the new MRD criterion:

Theorem 3.2. *Let $G \in \mathbb{F}_{q^m}^{k \times n}$ be a generator matrix of a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. Then $\mathcal{C}$ is an MRD code if an only if for any $A \in \text{GL}_n(q)$, every maximal minor of GA is non-zero.*

Proof. We first prove the *only if* direction. For this let $\mathcal{C}$ be MRD. Then we know from Lemma 2.10 that all elements on the orbit of $\mathcal{C}$ under $\text{GL}_n(q)$ are MRD. Since $\text{GL}_n(q)$ acts on the columns of any generator matrix of $\mathcal{C}$, together with Lemma 3.1, we get that all maximal minors of any orbit element must be non-zero.

For the other direction, let $\mathcal{C}$ be non-MRD, i.e. there exists a non-zero codeword $\boldsymbol{c} \in \mathcal{C}$ of rank at most $n - k$. Then there exists $A \in \text{GL}_n(q)$ s.t.

$$cA = (\underbrace{0 \ldots 0}_{k} \mid \underbrace{* \cdots *}_{n-k}).$$

This in turn implies that there exists a generator matrix of $\mathcal{C}A$ with cA as a row. Thus the first maximal minor of this generator matrix will be zero. $\square$

We can slightly simplify this criterion as follows. For this denote by $\mathrm{UT}_n^*(q)$ the subgroup of $\mathrm{GL}_n(q)$ of upper triangular matrices with an all-1 diagonal.

Corollary 3.3. *Let $G \in \mathbb{F}_{q^m}^{k \times n}$ be a generator matrix of a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. Then $\mathcal{C}$ is an MRD code if and only if for any $A \in \mathrm{UT}_n^*(q)$ every maximal minor of GA is non-zero.*

Proof. Note that $\mathrm{UT}_n^*(q)$, together with the diagonal matrices and the permutation matrices in $\mathrm{GL}_n(q)$ generate the whole general linear group $\mathrm{GL}_n(q)$. The action of the diagonal matrices multiplies the maximal minors of the generator matrix by a non-zero scalar, the action of the permutation matrices at most changes the sign of the maximal minors. Hence, these two subgroups do not change the *non-zero-ness* of the maximal minors. $\square$

4 New Criterion for Gabidulin Codes

In this section we derive a new criterion to establish if a given MRD code is a generalized Gabidulin code or not. The main result is stated in Theorem 4.8.

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear MRD code of dimension k (i.e. rank distance $d = n - k + 1$) with generator matrix G. Recall the notation $[i] := q^i$. We apply the Frobenius on vectors and matrices coordinate-wise, i.e., for $G \in \mathbb{F}_{q^m}^{k \times n}$ we have $G^{[i]} = (g_{jk}^{[i]})_{j,k}$ and for $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ we have $\mathcal{C}^{[i]} = \{c^{[i]} \mid c \in \mathcal{C}\}$. In this section we let $s \in \mathbb{N}$, $s < m$ be such that $\gcd(s, m) = 1$.

The following three Lemmas are needed to prove Proposition 4.6 and then Theorem 4.8.

Lemma 4.1. *Let $A \in \mathrm{GL}_k(q^m)$. Then $(A^{-1})^{[1]} = (A^{[1]})^{-1}$.*

Proof. We have that

$$
\begin{aligned}
A^{-1}A = I_k &\iff (A^{-1}A)^{[1]} = I_k \\
&\iff (A^{-1})^{[1]}A^{[1]} = I_k \\
&\iff (A^{-1})^{[1]} = (A^{[1]})^{-1}.
\end{aligned}
$$

$\square$

It is well-known that the roots of $x^q - x$ are exactly the elements of $\mathbb{F}_q$ (see e.g. [10, Theorem 2.5]). For our main results we need a generalization of this result:

Lemma 4.2. *If $\gcd(s, m) = 1$, then the roots in $\mathbb{F}_{q^m}$ of $x^{[s]} - x$ are exactly the elements of $\mathbb{F}_q$.*

Proof. Consider the field $F_{q^{ms}}$, then both $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^s}$ are subfields of it [10, Theorem 2.6]. Since m and s are coprime these two subfields only intersect in the base field $\mathbb{F}_q$. Moreover, the roots of $x^{[s]} - x$ in $\mathbb{F}_{q^{ms}}$ are exactly the elements of $\mathbb{F}_{q^s}$, hence the roots of it in $\mathbb{F}_{q^m}$ are the elements of $\mathbb{F}_q$. $\qquad\square$

Lemma 4.3. *Let* $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$ *be of rank* r *over* $\mathbb{F}_q$. *Then* $\boldsymbol{v}, \boldsymbol{v}^{[s]}, \ldots, \boldsymbol{v}^{[s(r-1)]}$ *are linearly independent over* $\mathbb{F}_{q^m}$.

Proof. Assume that $\boldsymbol{v}, \boldsymbol{v}^{[s]}, \ldots, \boldsymbol{v}^{[s(r-1)]}$ are not linearly independent over $\mathbb{F}_{q^m}$, i.e. there exist $\lambda_0, \ldots, \lambda_{r-1} \in \mathbb{F}_{q^m}$, at least one $\lambda_i \neq 0$, such that

$$\sum_{i=0}^{r-1} \lambda_i \boldsymbol{v}^{[is]} = \boldsymbol{0}.$$

Then the q^s-linearized polynomial $p(x) := \sum_{i=0}^{r-1} \lambda_i x^{[si]} = \sum_{i=0}^{r-1} \lambda_i x^{(q^s)^i} \in \mathbb{F}_{q^{ms}}[x]$ has roots $v_1, \ldots, v_n$. Since $p(x)$ is linearized, all elements of the vector space $\langle v_1, \ldots, v_n \rangle_{q^s}$ are roots of it. Since $\langle v_1, \ldots, v_n \rangle_q$ has dimension r, by [9, Lemma 4.3], also $\langle v_1, \ldots, v_n \rangle_{q^s}$ has dimension r. Hence, there are q^{rs} roots of $p(x)$ in $\mathbb{F}_{q^{ms}}$. Hence $p(x)$ must have degree at least q^{rs}, which is a contradiction. $\qquad\square$

The following straight-forward lemma is needed to prove Lemma 4.5.

Lemma 4.4. *Let* $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k \in \mathbb{F}_{q^m}^n$ *be linearly independent over* $\mathbb{F}_{q^m}$. *Then* $\boldsymbol{w}_1^{[s]}, \ldots, \boldsymbol{w}_k^{[s]} \in \mathbb{F}_{q^m}^n$ *are also linearly independent over* $\mathbb{F}_{q^m}$

Proof. Assume that $\boldsymbol{w}_1^{[s]}, \ldots, \boldsymbol{w}_k^{[s]}$ are not linearly independent, i.e. there exist $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_{q^m}$ with

$$\sum_{i=1}^{k} \lambda_i \boldsymbol{w}_i^{[s]} = \boldsymbol{0} \iff \left(\sum_{i=1}^{k} \lambda_i^{[-s]} \boldsymbol{w}_i \right)^{[s]} = \boldsymbol{0} \iff \sum_{i=1}^{k} \lambda_i^{[-s]} \boldsymbol{w}_i = \boldsymbol{0}.$$

Thus the vectors $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k$ are not linearly independent over $\mathbb{F}_{q^m}$, which is a contradiction. $\qquad\square$

The following result is a generalization of [7, Theorem 1].

Lemma 4.5. *Let* $\mathcal{W} \subset \mathbb{F}_{q^m}^n$ *be a subspace of dimension* $k \leq n$ *satisfying* $\mathcal{W}^{[s]} = \mathcal{W}$. *Then* $\mathcal{W}$ *has a generator matrix in* $\mathbb{F}_q^{k \times n}$. *In particular* $\mathcal{W}$ *contains elements of rank* 1 *over* $\mathbb{F}_q$.

Proof. If $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k\} \subset \mathbb{F}_{q^m}^n$ is a basis for $\mathcal{W}$, then by Lemma 4.4 $\{\boldsymbol{w}_1^{[s]}, \ldots, \boldsymbol{w}_k^{[s]}\}$ is also a basis of $\mathcal{W}$. Then there exists $A \in \mathrm{GL}_k(q^m)$ such that

$$\begin{pmatrix} w_{1,1}^{[s]} & w_{1,2}^{[s]} & \cdots & w_{1,n}^{[s]} \\ w_{2,1}^{[s]} & w_{2,2}^{[s]} & \cdots & w_{2,n}^{[s]} \\ & & \vdots & \\ w_{k,1}^{[s]} & w_{k,2}^{[s]} & \cdots & w_{k,n}^{[s]} \end{pmatrix} = A \begin{pmatrix} w_{1,1} & w_{1,2} & \cdots & w_{1,n} \\ w_{2,1} & w_{2,2} & \cdots & w_{2,n} \\ & & \vdots & \\ w_{k,1} & w_{k,2} & \cdots & w_{k,n} \end{pmatrix}.$$

Since the rightmost matrix has rank k, there exists a set of k linearly independent (over $\mathbb{F}_{q^m}$) columns. Without loss of generality, we can assume that the first k columns are linearly independent. Thus the submatrix $W_1 := (w_{i,j})_{i,j=1}^{k}$ is invertible (and therefore $W_1^{[s]}$ is also invertible by Lemma 4.4), and so we can solve

$$A = W_1^{[s]} W_1^{-1}.$$

Define $W_2 := (w_{i,j})_{i=1 \ j=k+1}^{k \quad n}$. Then we have

$$W_2^{[s]} = W_1^{[s]} W_1^{-1} W_2.$$

If we apply the Frobenius map s times on both sides and use Lemma 4.1, we obtain

$$
\begin{aligned}
W_2^{[2s]} &= W_1^{[2s]} (W_1^{-1})^{[s]} W_2^{[s]} \\
&= W_1^{[2s]} (W_1^{[s]})^{-1} W_1^{[s]} W_1^{-1} W_2 \\
&= W_1^{[2s]} W_1^{-1} W_2.
\end{aligned}
$$

Then, we have

$$W_1^{[2s]} (W_1^{-1})^{[s]} W_2^{[s]} = W_1^{[2s]} W_1^{-1} W_2.$$

Since $W_1^{[2s]}$ is invertible, we obtain

$$(W_1^{-1} W_2)^{[s]} = W_1^{-1} W_2,$$

and therefore we must have that $W_1^{-1} W_2$ has only entries in $\mathbb{F}_q$, by Lemma 4.2. Therefore, a generator matrix for $\mathcal{W}$ can be expressed as $W_1^{-1}[W_1 \mid W_2] = [I_k \mid W_1^{-1} W_2] \in \mathbb{F}_q^{k \times n}$, whose rows have rank weight 1 over $\mathbb{F}_q$. $\qquad\square$

We can now state and prove the central ingredient for the main result in Theorem 4.8:

Proposition 4.6. *Suppose that $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ is a linear code of dimension $k \geq 2$ and minimum rank distance at least k. If $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = k - 1$ (this automatically implies that $k < n$), then there exists a generator matrix for $\mathcal{C}$ of the form*

$$
G^* = \begin{pmatrix}
g_1 & g_2 & \cdots & g_n \\
g_1^{[s]} & g_2^{[s]} & \cdots & g_n^{[s]} \\
& & \vdots & \\
g_1^{[s(k-1)]} & g_2^{[s(k-1)]} & \cdots & g_n^{[s(k-1)]}
\end{pmatrix}
$$

with $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$.

Proof. We prove this inductively on k. First assume that $k = 2$. Then $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = 1$, i.e. there exists $\boldsymbol{g}' \in \mathcal{C}$ such that $\mathcal{C} \cap \mathcal{C}^{[s]} = \langle \boldsymbol{g}' \rangle_{q^m}$. Since $\boldsymbol{g}' \in \mathcal{C}^{[s]}$, we get that $\boldsymbol{g}'^{[-s]} \in \mathcal{C}$. The minimum rank distance of $\mathcal{C}$ is at least $k = 2$, i.e. the rank of $\boldsymbol{g}'^{[-s]}$ over $\mathbb{F}_q$ is at least 2. Then, by Lemma 4.3, $\boldsymbol{g}'^{[-s]}$ and $\boldsymbol{g}'$ are linearly independent. Hence they form a basis of $\mathcal{C}$ and we can rename $\boldsymbol{g} := \boldsymbol{g}'^{[-s]}$ to write a generator matrix

$$G^* = \begin{pmatrix} \boldsymbol{g} \\ \boldsymbol{g}^{[s]} \end{pmatrix}.$$

We now explain the induction step $(k-1) \to k$. Let $\mathcal{W} = \mathcal{C} \cap \mathcal{C}^{[s]}$, then we know from Lemma 4.5 that $\mathcal{W}^{[s]} \neq \mathcal{W}$, because the minimum rank distance of $\mathcal{C}$ is at least k. Since $\mathcal{W}, \mathcal{W}^{[s]} \subset \mathcal{C}^{[s]}$, both with codimension 1, we get $\langle \mathcal{W}, \mathcal{W}^{[s]} \rangle_{q^m} = \mathcal{C}^{[s]}$. Then

$$\dim(\mathcal{W} \cap \mathcal{W}^{[s]}) = \dim(\mathcal{W}) + \dim(\mathcal{W}^{[s]}) - \dim(\mathcal{W} + \mathcal{W}^{[s]}) = 2(k-1) - k = k - 2.$$

Furthermore, since $\mathcal{W} \subset \mathcal{C}$, the minimum rank distance of $\mathcal{W}$ is at least k. Therefore, $\mathcal{W}$ satisfies the conditions of the induction hypothesis, and so we can express $\mathcal{W}$ in terms of some basis of the form

$$\{\boldsymbol{w}, \boldsymbol{w}^{[s]}, \ldots, \boldsymbol{w}^{[s(k-2)]}\}.$$

Hence, $\{\boldsymbol{w}, \boldsymbol{w}^{[s]}, \ldots, \boldsymbol{w}^{[s(k-2)]}\} \in \mathcal{C}$ and thus $\{\boldsymbol{w}^{[s]}, \boldsymbol{w}^{[2s]}, \ldots, \boldsymbol{w}^{[s(k-1)]}\} \in \mathcal{C}^{[s]}$. On the other hand, $\boldsymbol{w} \in \mathcal{W} \subset \mathcal{C}^{[s]}$, i.e. $\{\boldsymbol{w}, \boldsymbol{w}^{[s]}, \ldots, \boldsymbol{w}^{[s(k-1)]}\} \in \mathcal{C}^{[s]}$. By Lemma 4.3 this set is linearly independent, i.e. it is a basis of $\mathcal{C}^{[s]}$. This in turn implies that $\{\boldsymbol{w}^{[-s]}, \boldsymbol{w}, \boldsymbol{w}^{[s]}, \ldots, \boldsymbol{w}^{[s(k-2)]}\}$ is a basis of $\mathcal{C}$. Define $\boldsymbol{g} = \boldsymbol{w}^{[-s]}$, then $\{\boldsymbol{g}, \boldsymbol{g}^{[s]}, \ldots, \boldsymbol{g}^{[s(k-1)]}\}$ is a basis of $\mathcal{C}$. $\qquad \square$

Lemma 4.7. *Let $\mathcal{C}$ be a linear MRD code of dimension $k < n$ with generator matrix*

$$G^* = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[s]} & g_2^{[s]} & \cdots & g_n^{[s]} \\ & & \vdots & \\ g_1^{[s(k-1)]} & g_2^{[s(k-1)]} & \cdots & g_n^{[s(k-1)]} \end{pmatrix}.$$

Then $g_1, \ldots, g_n$ are linearly independent over $\mathbb{F}_q$.

Proof. We prove this by contradiction. Assume that WLOG g_1 is in $\langle g_2, \ldots, g_n \rangle_q$, i.e. there exist $\lambda_2, \ldots, \lambda_n \in \mathbb{F}_q$ with $g_1 = \sum_{i=2}^n \lambda_i g_i$. Then

$$g_1^{[j]} = \left(\sum_{i=2}^n \lambda_i g_i \right)^{[j]} = \sum_{i=2}^n \lambda_i^{[j]} g_i^{[j]} = \sum_{i=2}^n \lambda_i g_i^{[j]}$$

i.e. $g_1^{[j]} \in \langle g_2^{[j]}, \ldots, g_n^{[j]} \rangle_q$ for any $j \in \mathbb{N}$. Hence there exists $A \in \mathrm{GL}_n(q)$ such that the first column of $G^* A$ is zero. It follows from Theorem 3.2 that $\mathcal{C}$ is not a MRD code, which is a contradiction. $\qquad \square$

Theorem 4.8. *Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear MRD code of dimension $k < n$. Then $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = k - 1$ if and only if $\mathcal{C}$ is a generalized Gabidulin code.*

Proof. Let $\mathcal{C}$ be a generalized Gabidulin code of dimension k with generalization parameter s. Then it follows from the structure of the generator matrix of $\mathcal{C}$ that $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = k - 1$, which proves the first direction.

For the other direction we distinguish two cases: If $k \leq (n+1)/2$, then the minimum distance of $\mathcal{C}$ is at least k. Then it follows from Proposition 4.6 that $\mathcal{C}$ has a generator matrix of the form

$$G^* = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[s]} & g_2^{[s]} & \cdots & g_n^{[s]} \\ & & \vdots & \\ g_1^{[s(k-1)]} & g_2^{[s(k-1)]} & \cdots & g_n^{[s(k-1)]} \end{pmatrix}.$$

It follows from Lemma 4.7 that the g_i are linearly independent over $\mathbb{F}_q$. This is the definition of a generalized Gabidulin code.

If $k > (n+1)/2$, then it follows from Proposition 2.6 that the dual code $\mathcal{C}^\perp \subseteq \mathbb{F}_{q^m}^n$ has dimension $n - k$ and minimum distance $k + 1 > n - k$, i.e. we can use Proposition 4.6 and Lemma 4.7 as before to show that $\mathcal{C}^\perp$ is a generalized Gabidulin code. Since the dual of a generalized Gabidulin code is again a generalized Gabidulin code (see Proposition 2.9), the statement follows. $\square$

5 Non-Gabidulin MRD Codes

5.1 General results

In this subsection we want to state some general results on the non-existence of non-Gabidulin MRD codes, i.e. for which parameters all MRD codes actually are Gabidulin codes.

Theorem 5.1. *All linear MRD codes in $\mathbb{F}_{q^m}^n$ of dimension $k = 1$ or $k = n - 1$ are Gabidulin codes.*

Proof. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an MRD code of dimension 1. Then the minimum rank distance is n and it can be generated by one vector in $\mathbb{F}_{q^m}^n$. Clearly this vector needs to have only entries that are linearly independent over $\mathbb{F}_q$, thus it is a Gabidulin code.

Since the dual of a Gabidulin code is again a Gabidulin code (see Proposition 2.6), the statement for codes of dimension $n - 1$ follows. $\square$

Then the following statement easily follows.

Corollary 5.2. *All linear MRD codes of length $n \in \{1, 2, 3\}$ are Gabidulin codes.*

The following observation is helpful for further investigations:

Lemma 5.3. *Any MRD code* $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ *of dimension* k *has a generator matrix* $G \in \mathbb{F}_{q^m}^{k \times n}$ *in systematic form, i.e.*

$$G = [\, I_k \mid * \,].$$

Moreover, all entries of $*$ *are from* $\mathbb{F}_{q^m} \backslash \mathbb{F}_q$.

Proof. The first statement is a direct consequence of Lemma 3.1 The second statement follows from the minimum rank distance $n - k + 1$ of the code, because every codeword needs to have at least $n-k$ entries from $\mathbb{F}_{q^m} \backslash \mathbb{F}_q$. $\square$

In the first case not covered by Theorem 5.1, i.e. for length $n = 4$ and dimension $k = 2$, we can get the following statement. The same observation is mentioned as a computational result in [13, Section V].

Proposition 5.4. *All linear MRD codes in* $\mathbb{F}_{2^4}^4$ *are Gabidulin codes.*

Proof. The case for codes of dimension $k = 1$ or $k = 3$ follows from Theorem 5.1. It remains to show the case $k = 2$. Then by Lemma 5.3 there exists a generator matrix of the form

$$G = \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix}$$

with $a, b, c, d \in \mathbb{F}_{2^4} \backslash \mathbb{F}_2$.

By Theorem 3.2 a generator matrix G of an MRD code satisfies

$$G \begin{pmatrix} 1 & u_1 & u_2 & u_3 \\ 0 & 1 & u_4 & u_5 \\ 0 & 0 & 1 & u_6 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & u_1 & u_2 + a & u_3 + au_6 + b \\ 0 & 1 & u_4 + c & u_5 + cu_6 + d \end{pmatrix}$$

needs to have only non-zero maximal minors for $u_1, \dots, u_6 \in \mathbb{F}_2$. Thus we get the following inequations:

$$1 \neq 0$$
$$u_4 + c \neq 0$$
$$u_5 + cu_6 + d \neq 0$$
$$(u_2 + a) + u_1(u_4 + c) \neq 0$$
$$(u_3 + au_6 + b) + u_1(u_5 + cu_6 + d) \neq 0$$
$$(u_2 + a)(u_5 + cu_6 + d) + (u_4 + c)(u_3 + au_6 + b) \neq 0.$$

Clearly the first inequation is always true; the same for the second, since $u_4 \in \mathbb{F}_2$ and $c \notin \mathbb{F}_2$.

If G does not generate a Gabidulin code then, by Theorem 4.8,

$$\operatorname{rank} \begin{bmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \\ 1 & 0 & a^2 & b^2 \\ 0 & 1 & c^2 & d^2 \end{bmatrix} \neq 3.$$

Since $a, b, c, d \notin \mathbb{F}_2$ the rank of the above matrix is at least 3. Thus we need that the rank is equal to 4, which is equivalent to

$$(a^2 + a)(d^2 + d) + (b^2 + b)(c^2 + c) \neq 0.$$

Thus, overall, we need to check that there is no solution to the system of inequations

$$u_5 + cu_6 + d \neq 0$$
$$(u_2 + a) + u_1(u_4 + c) \neq 0$$
$$(u_3 + au_6 + b) + u_1(u_5 + cu_6 + d) \neq 0$$
$$(u_2 + a)(u_5 + cu_6 + d) + (u_4 + c)(u_3 + au_6 + b) \neq 0$$
$$(a^2 + a)(d^2 + d) + (b^2 + b)(c^2 + c) \neq 0$$

for any $u_1, \ldots, u_6 \in \mathbb{F}_2$. With the help of a computer program one can check that there exists no solution for $a, b, c, d \in \mathbb{F}_{2^4} \backslash \mathbb{F}_2$ for the above system of inequations, for any representation of the extension field. $\qquad\square$

The previous results show that the first set of parameters for which we can hope to construct non-Gabidulin MRD codes is $n = 4, k = 2$ and $q \geq 3$. This is what we will do in the following subsection.

5.2   Constructions of length 4 and dimension 2

In this subsection we use the results of the previous sections to derive some linear MRD codes that are not generalized Gabidulin codes. The codes that we derive in this subsection have length 4 and dimension 2.

Theorem 5.5. *Let $m > 4$, $\alpha \in \mathbb{F}_{q^m}$ primitive such that $\mathbb{F}_{q^m}^* = \langle \alpha \rangle$ and $\gamma \in \mathbb{F}_q$ be a quadratic non-residue in $\mathbb{F}_q$ such that $\gamma \neq (\alpha^{[s]} + \alpha)^2$ for any $0 < s < m$ with $\gcd(s, m) = 1$. Then*

$$G = \begin{pmatrix} 1 & 0 & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & \gamma\alpha \end{pmatrix}$$

is a generator matrix of an MRD code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^4$ of dimension $k = 2$ that is not a generalized Gabidulin code.

Proof. First we prove that $\mathcal{C}$ is MRD. For this we use Corollary 3.3. Note that

$$\mathrm{UT}^*_{4}(q) = \left\{ \begin{pmatrix} 1 & u_1 & u_2 & u_3 \\ 0 & 1 & u_4 & u_5 \\ 0 & 0 & 1 & u_6 \\ 0 & 0 & 0 & 1 \end{pmatrix} \,\middle|\, u_1, \ldots, u_6 \in \mathbb{F}_q \right\}$$

and

$$G \begin{pmatrix} 1 & u_1 & u_2 & u_3 \\ 0 & 1 & u_4 & u_5 \\ 0 & 0 & 1 & u_6 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & u_1 & u_2 + \alpha & u_3 + u_6\alpha + \alpha^2 \\ 0 & 1 & u_4 + \alpha^2 & u_5 + u_6\alpha^2 + \gamma\alpha \end{pmatrix}.$$

We need to show that all maximal minors of this matrix are non-zero for any values of $u_1, \ldots, u_6$:

$$1 \neq 0$$
$$u_4 + \alpha^2 \neq 0$$
$$u_5 + \alpha^2 u_6 + \gamma\alpha \neq 0$$
$$(u_2 + \alpha) - u_1(u_4 + \alpha^2) \neq 0$$
$$(u_3 + \alpha u_6 + \alpha^2) - u_1(u_5 + \alpha^2 u_6 + \gamma\alpha) \neq 0$$
$$(u_2 + \alpha)(u_5 + \alpha^2 u_6 + \gamma\alpha) - (u_4 + \alpha^2)(u_3 + \alpha u_6 + \alpha^2) \neq 0.$$

One can easily see that the first four inequations are always true, since all u_i are in $\mathbb{F}_q$. We can rewrite the fifth inequation as

$$(u_1 u_5 - u_3) + (u_1\gamma - u_6)\alpha + (u_1 u_6 - 1)\alpha^2 \neq 0.$$

If the last term is zero then $u_1 = u_6^{-1}$. But then $u_1\gamma - u_6 = u_6^{-1}(\gamma - u_6^2) \neq 0$ because γ is a quadratic non-residue. Thus, in this case, the middle term of the above sum does not vanish, i.e. the inequation is always true. Lastly we can rewrite the sixth inequation as

$$(u_2 u_5 - u_3 u_4) + (u_2\gamma + u_5 - u_4 u_6)\alpha + (u_2 u_6 + \gamma - u_4 - u_3)\alpha^2 - \alpha^4 \neq 0.$$

This is always true, since the minimal polynomial of α has degree $m > 4$ and $u_1, \ldots, u_6, \gamma \in \mathbb{F}_q$, i.e. nothing can cancel out the α^4-term.

It remains to prove that $\mathcal{C}$ is not a generalized Gabidulin code. For this we use Theorem 4.8 and compute

$$\mathrm{rank} \begin{bmatrix} G \\ G^{[s]} \end{bmatrix} = \mathrm{rank} \begin{bmatrix} 1 & 0 & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & \gamma\alpha \\ 1 & 0 & \alpha^{[s]} & \alpha^{2[s]} \\ 0 & 1 & \alpha^{2[s]} & \gamma\alpha^{[s]} \end{bmatrix} =$$

$$\text{rank} \begin{bmatrix} 1 & 0 & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & \gamma\alpha \\ 0 & 0 & \alpha^{[s]} - \alpha & \alpha^{2[s]} - \alpha^2 \\ 0 & 0 & \alpha^{2[s]} - \alpha^2 & \gamma(\alpha^{[s]} - \alpha) \end{bmatrix},$$

for any s with $\gcd(s, m) = 1$. Since $\alpha \notin \mathbb{F}_q$ this rank cannot be equal to 2, by Lemma 4.2. Hence, $\mathcal{C}$ is Gabidulin if and only if the determinant of the lower right submatrix from above is zero, i.e. if and only if

$$\gamma(\alpha^{[s]} - \alpha)^2 - (\alpha^{2[s]} - \alpha^2)^2 = 0$$

$$\iff \gamma(\alpha^{[s]} - \alpha)^2 = (\alpha^{2[s]} - \alpha^2)^2$$

$$\iff \gamma(\alpha^{[s]} - \alpha)^2 = (\alpha^{[s]} - \alpha)^2(\alpha^{[s]} + \alpha)^2$$

$$\iff \gamma = (\alpha^{[s]} + \alpha)^2.$$

This is a contradiction to the conditions on γ, which implies that $\mathcal{C}$ is non-Gabidulin. $\qquad\square$

Note that in the previous theorem $\gamma \in \mathbb{F}_q$ can in particular be chosen as a quadratic non-residue in the extension field $\mathbb{F}_{q^m}$.

Example 5.6. *Let $q = 3, m = 5$ and α a root of $x^5 + 2x^2 + x + 1$. Then $\gamma = 2$ is a non-quadratic residue in $\mathbb{F}_{3^5}$ and the code with generator matrix*

$$G = \begin{pmatrix} 1 & 0 & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & 2\alpha \end{pmatrix}$$

is an MRD but not a generalized Gabidulin code.

Although we proved Theorem 5.5 for $m > 4$ we can find analog constructions for $m = 4$, as shown in the following examples. The proof that these examples are also non-Gabidulin MRD codes is analogous to the one of Theorem 5.5, but when checking if the maximal minor of $\mathrm{GUT}_n^*(q)$ involving the third and fourth column is non-zero we cannot use the argument that the minimal polynomial $m(x)$ of α has degree at least 4. Instead we need to write α^4 modulo $m(x)$ and show that the minor is non-zero.

Example 5.7. *Let $q = 3, m = 4$ and α a root of $x^4 - x^3 - 1$. Then $\gamma = 2$ is a quadratic non-residue in $\mathbb{F}_3$ and it fulfills the conditions that $\gamma \neq (\alpha^{[s]} + \alpha)^2$ for any $0 < s < m$ with $\gcd(s, m) = 1$. Now the code with generator matrix*

$$G = \begin{pmatrix} 1 & 0 & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & 2\alpha \end{pmatrix}$$

is an MRD but not a generalized Gabidulin code. To show that it is an MRD code we need to prove that the before mentioned minor is non-zero, i.e. that

$$(u_2 u_5 - u_3 u_4) + (2u_2 + u_5 - u_4 u_6)\alpha + (u_2 u_6 + 2 - u_4 - u_3)\alpha^2 - \alpha^4$$

$$\Longleftrightarrow \quad (u_2 u_5 - u_3 u_4 - 1) + (2u_2 + u_5 - u_4 u_6)\alpha + (u_2 u_6 + 2 - u_4 - u_3)\alpha^2 - \alpha^3$$

is non-zero for any $u_1, \ldots, u_6 \in \mathbb{F}_q$. This is clearly the case since nothing can cancel out the α^3-term.

Note that in the previous example we could have chosen any minimal polynomial of α that involves a non-zero term of order 3 (and a suitable γ). The same proof would then show that the generated code is MRD but not a generalized Gabidulin code.

We want to conclude with a final example over $\mathbb{F}_5$. A generalization for other values of q is then straight-forward.

Example 5.8. *Let $q = 5, m = 4$ and α a root of $x^4 + x^3 + x^2 + x + 3$. Then $\gamma = 2$ is a quadratic non-residue in $\mathbb{F}_5$ and it fulfills the conditions that $\gamma \neq (\alpha^{[s]} + \alpha)^2$ for any $0 < s < m$ with $\gcd(s, m) = 1$. Now the code with generator matrix*

$$G = \begin{pmatrix} 1 & 0 & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & 2\alpha \end{pmatrix}$$

is an MRD but not a generalized Gabidulin code. To show that it is an MRD code we need to prove that the before mentioned minor is non-zero, i.e. that

$$(u_2 u_5 - u_3 u_4) + (u_2 \gamma + u_5 - u_4 u_6)\alpha + (u_2 u_6 + \gamma - u_4 - u_3)\alpha^2 - \alpha^4$$

$$\Longleftrightarrow \quad (u_2 u_5 - u_3 u_4 + 2) + (u_2 \gamma + u_5 - u_4 u_6 + 4)\alpha + (u_2 u_6 + \gamma - u_4 - u_3 + 4)\alpha^2 + 4\alpha^3$$

is non-zero for any $u_1, \ldots, u_6 \in \mathbb{F}_q$. This is clearly the case since nothing can cancel out the $4\alpha^3$-term.

5.3 Construction of length 5 and dimension 2

Analogously to the previous subsection, we present a construction of linear MRD codes of length 5 and dimension 2 that are not generalized Gabidulin codes.

Theorem 5.9. *Let $m > 7$, $\alpha \in \mathbb{F}_{q^m}$ primitive such that $\mathbb{F}_{q^m}^* = \langle \alpha \rangle$ and $\gamma \in \mathbb{F}_q$ be such that $\gamma \neq (\alpha^{[s]} + \alpha)(\alpha^{2[s]} + \alpha^{[s]+1} + \alpha^2)$ for any $0 < s < m$ with $\gcd(s, m) = 1$. Then*

$$G = \begin{pmatrix} 1 & 0 & \alpha & \alpha^2 & \alpha^3 \\ 0 & 1 & \alpha^2 & \alpha^4 & \gamma\alpha \end{pmatrix}$$

is a generator matrix of an MRD code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^5$ of dimension $k = 2$ that is not a generalized Gabidulin code.

Proof. First we prove that $\mathcal{C}$ is MRD. For this we use Corollary 3.3. Note that

$$\mathrm{UT^*}_5(q) = \left\{ \begin{pmatrix} 1 & u_1 & u_2 & u_3 & u_4 \\ 0 & 1 & u_5 & u_6 & u_7 \\ 0 & 0 & 1 & u_8 & u_9 \\ 0 & 0 & 0 & 1 & u_{10} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \Bigg| \; u_1, \ldots, u_{10} \in \mathbb{F}_q \right\}$$

and

$$G \begin{pmatrix} 1 & u_1 & u_2 & u_3 & u_4 \\ 0 & 1 & u_5 & u_6 & u_7 \\ 0 & 0 & 1 & u_8 & u_9 \\ 0 & 0 & 0 & 1 & u_{10} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & u_1 & u_2 + \alpha & u_3 + u_8\alpha + \alpha^2 & u_4 + u_9\alpha + u_{10}\alpha^2 + \alpha^3 \\ 0 & 1 & u_5 + \alpha^2 & u_6 + u_8\alpha^2 + \alpha^4 & u_7 + u_9\alpha^2 + u_{10}\alpha^4 + \gamma\alpha \end{pmatrix}.$$

We need to show that all maximal minors of this matrix are non-zero for any values of $u_1, \ldots, u_{10}$. Analogously to the proof of Theorem 5.5, one can easily see that the minors involving the first column are non-zero. The same holds for the minor involving the second and third column. The following equations remain:

$$(u_3 + \alpha u_8 + \alpha^2) - u_1(u_6 + \alpha^2 u_8 + \alpha^4) \quad \neq 0 \quad (1)$$
$$(u_4 + \alpha u_9 + \alpha^2 u_{10} + \alpha^3) - u_1(u_7 + \alpha^2 u_9 + \alpha^4 u_{10} + \gamma\alpha) \quad \neq 0 \quad (2)$$
$$(u_2 + \alpha)(u_6 + \alpha^2 u_8 + \alpha^4 u_{10} + \alpha^4) - (u_5 + \alpha^2)(u_3 + \alpha u_8 + \alpha^2) \quad \neq 0 \quad (3)$$
$$(u_2 + \alpha)(u_7 + \alpha^2 u_9 + \alpha^4 u_{10} + \gamma\alpha) -$$
$$(u_5 + \alpha^2)(u_4 + \alpha u_9 + \alpha^2 u_{10} + \alpha^3) \quad \neq 0 \quad (4)$$
$$(u_3 + u_8\alpha + \alpha^2)(u_7 + u_9\alpha^2 + u_{10}\alpha^4 + \gamma\alpha) -$$
$$(u_4 + u_9\alpha + u_{10}\alpha^2 + \alpha^3)(u_6 + u_8\alpha^2 + \alpha^4) \quad \neq 0 \quad (5)$$

We can rewrite Inequation (1) as

$$(u_3 - u_1 u_6) + u_8\alpha + (1 - u_1 u_8)\alpha^2 - u_1\alpha^4 \neq 0.$$

The α^2-term only vanishes if $u_1 u_8 = 1$, but then the α-term (and the α^4-term) do not vanish. Hence, this inequation is always true. Inequation (2) has an α^3-term that never vanishes, thus it is also true. Similarly, Inequation (3) has an α^5-term that never vanishes, and Inequation (7) has an α^7-term, that never vanishes. These two inequations are therefore also true. We can rewrite Inequation (4) as

$$(u_2 u_7 - u_4 u_5) + (u_2\gamma + u_7 - u_5 u_9)\alpha + (u_2 u_9 + \gamma - u_5 u_{10} - u_4)\alpha^2 - u_5\alpha^3$$

$$+(u_2 u_{10} - u_{10})\alpha^4 + (u_{10} - 1)\alpha^5 \neq 0.$$

For the α^5-term to vanish we need $u_{10} = 1$, for the α^3-term to vanish we need $u_5 = 0$. If additionaly we want the α^4-term to vanish we need $u_2 = 1$. Then we need $u_7 = 0$ for the first summand to be zero. But then the α-term does not vanish, since $\gamma \neq 0$. Thus this inequation is also true. Therefore we have shown that $\mathcal{C}$ is an MRD code.

It remains to prove that $\mathcal{C}$ is not a generalized Gabidulin code. For this we use Theorem 4.8 and compute

$$\text{rank}\begin{bmatrix} G \\ G^{[s]} \end{bmatrix} = \text{rank}\begin{bmatrix} 1 & 0 & \alpha & \alpha^2 & \alpha^3 \\ 0 & 1 & \alpha^2 & \alpha^4 & \gamma\alpha \\ 1 & 0 & \alpha^{[s]} & \alpha^{2[s]} & \alpha^{3[s]} \\ 0 & 1 & \alpha^{2[s]} & \alpha^{4[s]} & \gamma\alpha^{[s]} \end{bmatrix} =$$

$$\text{rank}\begin{bmatrix} 1 & 0 & \alpha & \alpha^2 & \alpha^3 \\ 0 & 1 & \alpha^2 & \alpha^4 & \gamma\alpha \\ 0 & 0 & \alpha^{[s]} - \alpha & \alpha^{2[s]} - \alpha^2 & \alpha^{3[s]} - \alpha^3 \\ 0 & 0 & \alpha^{2[s]} - \alpha^2 & \alpha^{4[s]} - \alpha^4 & \gamma(\alpha^{[s]} - \alpha) \end{bmatrix}, \tag{6}$$

for any s with $\gcd(s,m) = 1$. Since $\alpha \notin \mathbb{F}_q$ this rank cannot be equal to 2, by Lemma 4.2. Hence, $\mathcal{C}$ is Gabidulin if and only if the rank of the matrix in (6) is equal to 3. We compute the determinant of the lower submatrix involving columns 3 and 5,

$$\gamma(\alpha^{[s]} - \alpha)^2 - (\alpha^{2[s]} - \alpha^2)(\alpha^{3[s]} - \alpha^3) =$$

$$(\alpha^{[s]} - \alpha)^2(\gamma - (\alpha^{[s]} + \alpha)(\alpha^{2[s]} - \alpha^{[s]+1} + \alpha^2)),$$

which is non-zero by the conditions on γ. Hence the rank of the matrix from (6) is 4, which implies that $\mathcal{C}$ is non-Gabidulin. $\square$

Example 5.10. *Let $q = 2, m = 8$ and α a root of $x^8 + x^4 + x^3 + x^2 + 1$. Then $\gamma = 1$ fulfills the conditions that $\gamma \neq (\alpha^{[s]} + \alpha)(\alpha^{2[s]} + \alpha^{[s]+1} + \alpha^2)$ for any $0 < s < m$ with $\gcd(s,m) = 1$. Now the code with generator matrix*

$$G = \begin{pmatrix} 1 & 0 & \alpha & \alpha^2 & \alpha^3 \\ 0 & 1 & \alpha^2 & \alpha^4 & \alpha \end{pmatrix}$$

is an MRD but not a generalized Gabidulin code.

Note that, analogously to the constructions of length 4 from the previous subsection, one can use the construction from Theorem 5.9 to construct non-Gabidulin MRD codes, also if $5 \leq m \leq 7$. One simply needs to check that the minimal polynomial of α is such that all the inequations arising from $G\ \text{UT}^*{}_5(q)$ hold.

6　Conclusion

In this work we give a new criterion to check if a given matrix generates a linear MRD code. Moreover, we derive a criterion to check if a given generator matrix belongs to a linear generalized Gabidulin code or not. Although the criterion itself is quite simple, the proof of it involves several, to our knowledge new, technical lemmas on the Frobenius map, as well as the $\mathbb{F}_q$-rank and linear independence of elements in $\mathbb{F}_{q^m}$.

We then use these results to construct linear MRD codes that are not generalized Gabidulin codes. Since the class of Gabidulin codes is closed under the semilinear isometries (also called equivalencies by some authors) this means that these codes are also not semilinearly isometric (or equivalent) to generalized Gabidulin codes.

In future work we want to use these criteria to find more general constructions for non-Gabidulin MRD codes. Moreover, we would like to classify all linear MRD codes and see how many different classes of codes there are, for given parameter sets.

We also believe that the results of this paper are interesting from a cryptographic point of view. Especially for the cryptanalysis of McEliece-type cryptosystems based on Gabidulin codes [6, 11] our criteria for MRD and Gabidulin codes might lead to new and more efficient attacks. First results in this direction can be found in [8], and we would like to pursue this line of research further in the future.

Acknowledgement

References

[1] T. P. Berger. Isometries for rank distance and permutation group of Gabidulin codes. *IEEE Transactions on Information Theory*, 49(11):3016 – 3019, nov. 2003.

[2] A. Cossidente, G. Marino, and F. Pavese. Non-linear maximum rank distance codes. *preprint*, 2015.

[3] J. de la Cruz, M. Kiermaier, A. Wassermann, and W. Willems. Algebraic structures of MRD codes. *arXiv:1502.02711*, [cs.IT], 2015.

[4] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25(3):226–241, 1978.

[5] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[6] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In *Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'91, pages 482–489, Berlin, Heidelberg, 1991. Springer-Verlag.

[7] M. Giorgetti and A. Previtali. Galois invariance, trace codes and subfield subcodes. *Finite Fields Appl.*, 16(2):96–99, 2010.

[8] A.-L. Horlemann-Trautmann, K. Marshall, and J. Rosenthal. Extension of Overbeck's attack for Gabidulin based cryptosystems. *arXiv:1511.01549*, [cs.CR], 2015.

[9] A. Kshevetskiy and E. Gabidulin. The new construction of rank codes. In *Proceedings of the International Symposium on Information Theory (ISIT) 2005*, pages 2105–2108, Sept 2005.

[10] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications.* Cambridge University Press, Cambridge, London, 1994. Revised edition.

[11] P. Loidreau. Designing a rank metric based McEliece cryptosystem. In *Proceedings of the Third International Conference on Post-Quantum Cryptography*, PQCrypto'10, pages 142–152, Berlin, Heidelberg, 2010. Springer-Verlag.

[12] K. Morrison. Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes. *IEEE Transactions on Information Theory*, 60(11):7035–7046, Nov 2014.

[13] J. Sheekey. A new family of linear maximum rank distance codes. *arXiv:1504.01581 [cs.IT]*, 2015.

[14] Z.-X. Wan. *Geometry of matrices.* World Scientific, Singapore, 1996. In memory of Professor L.K. Hua (1910 – 1985).