On the genericity of maximum rank distance and Gabidulin codes

Alessandro Neri\textsuperscript{1} · Anna-Lena Horlemann-Trautmann\textsuperscript{2} · Tovohery Randrianarisoa\textsuperscript{1} · Joachim Rosenthal\textsuperscript{1}

Received: 18 May 2016 / Revised: 17 November 2016 / Accepted: 14 March 2017 / Published online: 8 April 2017
© Springer Science+Business Media New York 2017

Abstract We consider linear rank-metric codes in $\mathbb{F}_{q^m}^n$. We show that the properties of being maximum rank distance (MRD) and non-Gabidulin are generic over the algebraic closure of the underlying field, which implies that over a large extension field a randomly chosen generator matrix generates an MRD and a non-Gabidulin code with high probability. Moreover, we give upper bounds on the respective probabilities in dependence on the extension degree $m$.

Keywords Rank-metric codes · Finite fields · MRD codes · Gabidulin codes

Mathematics Subject Classification 11T71

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 maximum...
rank distance (MRD) 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 often called Gabidulin codes.

The question, if there are other general constructions of MRD codes that are not equivalent to Gabidulin codes, has been of large interest recently. Some constructions of non-Gabidulin MRD codes can be found e.g. in [2,3,14], where many of the derived codes, when seen as block codes in $\mathbb{F}_{q^m}$, are not linear over $\mathbb{F}_{q^m}$ but only linear over some subfield of it. For some small parameter sets, constructions of linear non-Gabidulin MRD codes were presented in [7]. On the other hand, in the same paper it was shown that all MRD codes in $\mathbb{F}_{2^4}$ are Gabidulin codes. In general, it remains an open question for which parameters non-Gabidulin MRD codes exist, and if so, how many such codes there are.

In this paper we show that the properties of being MRD and non-Gabidulin are generic. Our results imply that over a large field extension degree a randomly chosen generator matrix generates an MRD and a non-Gabidulin code with high probability. Moreover, we give an upper, respectively lower, bound on the respective probabilities in dependence on the extension degree. Finally we show that for any length and dimension there exists a linear non-Gabidulin MRD code, if the extension degree is large enough.

The paper is structured as follows. In Sect. 2 we give some preliminary definitions and results, first for rank-metric codes and then for the notion of genericity. Section 3 contains topological results, showing that the properties of being MRD and non-Gabidulin are generic. In Sect. 4 we derive some upper bounds on the probability of these two code properties in dependence on the extension degree of the underlying finite field. We conclude in Sect. 5.

## 2 Preliminaries

### 2.1 Finite fields and their vector spaces

The following definitions and results can be found in any textbook on finite fields, e.g. [11]. We denote the finite field of cardinality $q$ by $\mathbb{F}_q$. It exists if and only if $q$ is a prime power. Moreover, if it exists, $\mathbb{F}_q$ is unique up to isomorphism. An extension field of extension degree $m$ is denoted by $\mathbb{F}_{q^m}$. We now recall some basic theory on the trace function over finite fields.

**Definition 1** Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_{q^m}$ be an extension field. For $\alpha \in \mathbb{F}_{q^m}$, the *trace* of $\alpha$ over $\mathbb{F}_q$ is defined by

$$\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) := \sum_{i=0}^{m-1} \alpha^{q^i}.$$ 

For every integer $0 < s < m$ with $\gcd(m, s) = 1$, we denote by $\varphi_s$ the map given by

$$\varphi_s : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$$

$$\alpha \mapsto \alpha^{q^s} - \alpha.$$ 

The following result relates the trace with the maps $\varphi_s$.

**Lemma 2** The trace function satisfies the following properties:

1. $\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$ for all $\alpha \in \mathbb{F}_{q^m}$.
2. \( \text{Tr}_{\mathbb{F}_q^m / \mathbb{F}_q} \) is a linear surjective transformation from \( \mathbb{F}_q^m \) to \( \mathbb{F}_q \), where \( \mathbb{F}_q^m \) and \( \mathbb{F}_q \) are considered as \( \mathbb{F}_q \)-vector spaces.

3. For every \( \alpha \in \mathbb{F}_q^m \), the map \( T_\alpha \) defined by

\[
\beta \mapsto \text{Tr}_{\mathbb{F}_q^m / \mathbb{F}_q}(\alpha \beta)
\]

is a linear surjective transformation from \( \mathbb{F}_q^m \) to \( \mathbb{F}_q \), where \( \mathbb{F}_q^m \) and \( \mathbb{F}_q \) are considered as \( \mathbb{F}_q \)-vector spaces.

4. \( \varphi_s \) is a linear transformation from \( \mathbb{F}_q^m \) to itself, considered as \( \mathbb{F}_q \)-vector space.

5. For every \( s \) coprime to \( m \), \( \varphi_s(\alpha) = 0 \) if and only if \( \alpha \in \mathbb{F}_q \).

6. \( \ker(\text{Tr}_{\mathbb{F}_q^m / \mathbb{F}_q}) = \text{Im}(\varphi_s) \) for every \( s \) coprime to \( m \) and has cardinality \( q^{m-1} \).

**Proof** The statements of 1., 2. and 3. can be found e.g. in [11, Theorems 2.23 and 2.24].

4. For \( \alpha, \beta \in \mathbb{F}_q^m \), \( \varphi_s(\alpha + \beta) = (\alpha + \beta)^{q^s} - (\alpha + \beta) = \alpha^{q^s} - \alpha + \beta^{q^s} - \beta = \varphi_s(\alpha) + \varphi_s(\beta) \).
   
   Moreover, for every \( \alpha \in \mathbb{F}_q^m \), \( c \in \mathbb{F}_q \), \( \varphi_s(c \alpha) = c^{q^s} \alpha^{q^s} - c \alpha = c (\alpha^{q^s} - \alpha) = c \varphi_s(\alpha) \).

5. We have \( \varphi_s(\alpha) = \alpha^{q^s} - \alpha \) if and only if \( \alpha \in \mathbb{F}_q \). Since \( \alpha \in \mathbb{F}_q^m \), this is true if and only if \( \alpha \in \mathbb{F}_q^m \cap \mathbb{F}_q = \mathbb{F}_q \).

6. First we show that \( \text{Im}(\varphi_s) \subseteq \ker(\text{Tr}_{\mathbb{F}_q^m / \mathbb{F}_q}) \). Consider an element \( \alpha \in \text{Im}(\varphi_s) \). Then there exists \( \beta \in \mathbb{F}_q^m \) such that \( \alpha = \beta^{q^s} - \beta \). Now

\[
\text{Tr}_{\mathbb{F}_q^m / \mathbb{F}_q}(\alpha) = \text{Tr}_{\mathbb{F}_q^m / \mathbb{F}_q}(\beta^{q^s} - \beta) = \sum_{i=0}^{m-1} (\beta^{q^s} - \beta)^{q^i} = \sum_{i=0}^{m-1} \beta^{q^{s+i}} - \sum_{i=0}^{m-1} \beta^{q^i}.
\]

We observe now that if \( i \equiv j \mod m \), then \( \beta^{q^i} = \beta^{q^j} \). Hence the sum \( \sum_{i=0}^{m-1} \beta^{q^{s+i}} \) is a rearrangement of \( \sum_{i=0}^{m-1} \beta^{q^i} \) and \( \text{Tr}_{\mathbb{F}_q^m / \mathbb{F}_q}(\alpha) = 0 \). At this point observe that the trace function is a polynomial of degree \( q^{m-1} \) and so it has at most \( q^{m-1} \) roots. This means that \( |\ker(\text{Tr}_{\mathbb{F}_q^m / \mathbb{F}_q})| \leq q^{m-1} \). By part 4 and 5 of this lemma we get

\[
|\text{Im}(\varphi_s)| = \frac{|\mathbb{F}_q^m|}{|\ker(\varphi_s)|} = q^{m-1}
\]

and therefore \( \text{Im}(\varphi_s) \) and \( \ker(\text{Tr}_{\mathbb{F}_q^m / \mathbb{F}_q}) \) must be equal.

We denote by \( \text{GL}_n(q) := \{ A \in \mathbb{F}_q^{n \times n} | \text{rk}(A) = n \} \) the general linear group of degree \( n \) over \( \mathbb{F}_q \). Furthermore we need the Gaussian binomial \( \binom{n}{k}_q \), which is defined as the number of \( k \)-dimensional vector subspaces of \( \mathbb{F}_q^n \). It is well-known that

\[
\binom{n}{k}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i} = \frac{\prod_{i=0}^{k-1} (q^n - q^i)}{|\text{GL}_k(q)|}.
\]

Moreover, the following fact is well-known and easy to see.

**Lemma 3** Let \( k, n \) be two integers such that \( 0 < k \leq n/2 \), and let \( \mathcal{U} \) be a \( k \)-dimensional vector subspace of \( \mathbb{F}_q^n \). Then, for every \( r = 0, \ldots, k \), the number of \( k \)-dimensional subspaces that intersect \( \mathcal{U} \) in a \( (k-r) \)-dimensional subspace is

\[
\binom{k}{k-r}_q \binom{n-k}{r}_q q^{r^2}.
\]
Proof There are \( \binom{k}{k-r} \) many subspaces \( \mathcal{U}' \) of \( \mathcal{U} \) of dimension \((k-r)\) that can be the intersection space. Now, in order to complete \( \mathcal{U}' \) to a \( k \)-dimensional vector space, intersecting \( \mathcal{U} \) only in \( \mathcal{U}' \), we have \( \prod_{i=0}^{r-1} (q^n - q^{k+i}) \) choices for the remaining basis vectors. For a fixed basis of \( \mathcal{U}' \), the number of bases spanning the same subspace is given by the number of \( k \times k \) matrices of the form

\[
\begin{bmatrix}
1 & 0 \\
A & B
\end{bmatrix},
\]

where \( A \in \mathbb{F}_q^{r \times (k-r)} \) and \( B \in \text{GL}_r(q) \). This number is equal to \( q^{r(k-r)} | \text{GL}_r(q) | = \prod_{i=0}^{r-1} (q^k - q^{k-r+i}) \). Hence, the final count is given by

\[
\binom{k}{k-r} \prod_{i=0}^{r-1} (q^n - q^{k+i}) = \binom{k}{k-r} q^{n-k} r_{q^2}.
\]

\( \square \)

2.2 Rank-metric codes

Recall that \( \mathbb{F}_{q^m} \) is isomorphic (as a vector space over \( \mathbb{F}_q \)) to the vector space \( \mathbb{F}_{q^n} \). One then easily obtains the isomorphic description of matrices over the base field \( \mathbb{F}_q \) as vectors over the extension field, i.e. \( \mathbb{F}_q^{m \times n} \cong \mathbb{F}_{q^n} \).

**Definition 4** The rank distance \( d_R \) on \( \mathbb{F}_q^{m \times n} \) is defined by

\[
d_R(X, Y) := \text{rk}(X - Y), \quad X, Y \in \mathbb{F}_q^{m \times n}.
\]

Analogously, we define the rank distance between two elements \( x, y \in \mathbb{F}_{q^n} \) 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 \( \mathbb{F}_{q^n} \), i.e. those codes that form a subspace of \( \mathbb{F}_{q^m} \).

**Definition 5** An \( \mathbb{F}_{q^m} \)-linear rank-metric code \( C \) of length \( n \) and dimension \( k \) is a \( k \)-dimensional subspace of \( \mathbb{F}_{q^n} \) equipped with the rank distance. A matrix \( G \in \mathbb{F}_{q^m}^{k \times n} \) is called a generator matrix for the code \( C \) if

\[
C = \text{rs}(G),
\]

where \( \text{rs}(G) \) is the subspace generated by the rows of the matrix \( G \), called the row space of \( G \).

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 6** [5, Sect. 2] Let \( C \subseteq \mathbb{F}_{q^n} \) be a linear code with minimum rank distance \( d \) of dimension \( k \). Then

\[
k \leq n - d + 1.
\]

**Definition 7** A code attaining the Singleton bound is called a maximum rank distance (MRD) code.
Throughout the paper we denote by $I_k$ the $k \times k$ identity matrix.

**Lemma 8** [7, Lemma 5.3] Any linear MRD code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension $k$ has a generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ in systematic form (also called standard form), i.e.,

$$G = [I_k \mid X].$$

Moreover, all entries in $X$ are from $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$.

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

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

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

**Definition 9** Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$ and let $s$ be coprime to $m$. We define a generalized Gabidulin code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension $k$ as the linear block code with generator matrix $M_{s,k}(g_1, \ldots, g_n)$.

Note that for $s = 1$, this definition coincides with the classical Gabidulin code construction. The following theorem was shown for $s = 1$ in [5, Sect. 4], and for general $s$ in [8].

**Theorem 10** A generalized Gabidulin code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension $k$ over $\mathbb{F}_{q^m}$ has minimum rank distance $n - k + 1$. Thus, generalized Gabidulin codes are MRD codes.

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

$$C^\perp := \{ u \in \mathbb{F}_{q^m}^n \mid uc^T = 0, \quad \forall c \in C \}.$$
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, 16]:

**Lemma 12** [12, Proposition 2] The semilinear $\mathbb{F}_q$-rank isometries on $\mathbb{F}_{q^m}^n$ are of the form $(\lambda, A, \sigma) \in \left(\mathbb{F}_{q^m}^* \times \text{GL}_n(q)\right) \rtimes \text{Aut}(\mathbb{F}_{q^m})$, 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 $C \subseteq \mathbb{F}_{q^m}^n$ is a linear code with minimum rank distance $d$, then $C' = \sigma(\lambda C)A$ is a linear code with minimum rank distance $d$.

As semilinear isometries on $\mathbb{F}_{q^m}^n$ preserve the rank, we get that $\mathbb{F}_q$-linearly independent elements in $\mathbb{F}_{q^m}^n$ remain $\mathbb{F}_q$-linearly independent under the actions of $\left(\mathbb{F}_{q^m}^* \times \text{GL}_n(q)\right) \rtimes \text{Aut}(\mathbb{F}_{q^m})$. Moreover, the $s$-Moore matrix structure is preserved under these actions, which implies that the class of generalized Gabidulin codes is closed under the semilinear isometries. Thus, a code is semilinearly isometric to a generalized Gabidulin code if and only if it is itself a generalized Gabidulin code.

In this work we need the following criteria for both the MRD and the Gabidulin property. The following criterion for MRD codes was given in [7, Corollary 2.12], which in turn is based on a well-known result given in [5]:

**Proposition 13** (MRD criterion) Let $G \in \mathbb{F}_{q^m}^{k \times n}$ be a generator matrix of a rank-metric code $C \subseteq \mathbb{F}_{q^m}^n$. Then $C$ is an MRD code if and only if 

$$\text{rk}(VG^T) = k$$

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

Furthermore, we need the following criterion for the generalized Gabidulin property:

**Theorem 14** (gen. Gabidulin criterion) [7, Theorem 4.8] Let $C \subseteq \mathbb{F}_{q^m}^n$ be an MRD code of dimension $k$. $C$ is a generalized Gabidulin code if and only if there exists $s$ with $\gcd(s, m) = 1$ such that 

$$\dim(C \cap C^{(1^s)}) = k - 1.$$ 

### 2.3 The Zariski topology over finite fields

Consider the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_r]$ over the base field $\mathbb{F}_q$ and denote by $\overline{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$, necessarily an infinite field. For a subset $S \subseteq \mathbb{F}_q[x_1, \ldots, x_r]$ one defines the algebraic set 

$$V(S) := \{x \in \overline{\mathbb{F}}_q^r | f(x) = 0, \ \forall f \in S\}.$$ 

It is well-known that the algebraic sets inside $\overline{\mathbb{F}}_q^r$ form the closed sets of a topology, called the Zariski topology [6, Chap. I, Sect. 1]. The complements of the Zariski-closed sets are the Zariski-open sets.
Definition 15 A subset \( G \subset \overline{\mathbb{F}}_q \) is called a generic set if \( G \) contains a non-empty Zariski-open set.

If the base field are the real number (\( \mathbb{R} \)) or complex numbers (\( \mathbb{C} \)), then a generic set inside \( \mathbb{R}^r \) (respectively inside \( \mathbb{C}^r \)) is necessarily dense and its complement is contained in an algebraic set of dimension at most \( r - 1 \).

Over a finite field \( \mathbb{F}_q \) one has to be a little bit more careful. Indeed for every subset \( T \subset \mathbb{F}_q^r \) one finds a set of polynomials \( S \subseteq \mathbb{F}_q[x_1, \ldots, x_r] \) such that

\[
\{ x \in \mathbb{F}_q^r \mid f(x) = 0, \forall f \in S \} = T.
\]

This follows simply from the fact that a single point inside \( \mathbb{F}_q^r \) forms a Zariski-closed set and any subset \( T \subset \mathbb{F}_q^r \) is a finite union of points. However if one has an algebraic set \( V(S) \), as defined at the beginning of this subsection, then the number of \( \mathbb{F}_q^m \)-rational points defined through

\[
V(S; \mathbb{F}_q^m) := \{ x \in \mathbb{F}_q^r \mid f(x) = 0, \forall f \in S \}
\]

becomes in proportion to the cardinality of the whole vector space \( \mathbb{F}_q^r \) smaller, as the extension degree \( m \) increases. This is a consequence of the Schwartz–Zippel Lemma [13, Corollary 1] which we will formulate, for our purposes, over a finite field. The lemma itself will be crucial for our probability estimations in Sect. 4. We use the following version of the Schwartz–Zippel Lemma.

Lemma 16 (Schwartz–Zippel) [10, Lemma 1.1] Let \( f \in \mathbb{F}_q[x_1, x_2, \ldots, x_r] \) be a non-zero polynomial of total degree \( d \geq 0 \). Let \( \mathbb{F}_q^m \) be an extension field and let \( F \subseteq \mathbb{F}_q^m \) be a finite set. Let \( v_1, v_2, \ldots, v_r \) be selected at random independently and uniformly from \( F \). Then

\[
\Pr\left( f(v_1, v_2, \ldots, v_r) = 0 \right) \leq \frac{d}{|F|}.
\]

3 Topological results

The idea of this section is to show that the properties of being MRD and non-Gabidulin are generic properties.

Recall that, by Lemma 8, every linear MRD code in \( \mathbb{F}_q^n \) of dimension \( k \) has a unique representation by its generator matrix \( G \in \mathbb{F}_q^{k \times n} \) in systematic form

\[
G = [ I_k \mid X ].
\]

Thus, we have a one-to-one correspondence between the set of linear MRD codes in \( \mathbb{F}_q^n \) and a subset of the set of matrices \( \mathbb{F}_q^{k \times (n-k)} \). Therefore we want to investigate how many matrices \( X \in \mathbb{F}_q^{k \times (n-k)} \) give rise to an MRD or a generalized Gabidulin code, when plugged into the above form of a systematic generator matrix.

However, to make sense of the definition of genericity, we need to do this investigation over the algebraic closure of \( \mathbb{F}_q^m \). In particular, we will show that the set of matrices fulfilling the MRD criterion of Proposition 13, and the subset of these matrices not fulfilling the generalized Gabidulin criterion of Theorem 14, are generic sets over the algebraic closure.

We first show that the set of generator matrices fulfilling the MRD criterion of Proposition 13 is generic.
Theorem 17 Let $1 \leq k \leq n - 1$. The set

$$S_{\text{MRD}} := \{ X \in \overline{F}_{q^m}^{k \times (n-k)} \mid \forall A \in F_q^{n \times k} \text{ of rank } k : \det([I_k \mid X]A) \neq 0 \}$$

is a generic subset of $\overline{F}_{q^m}^{k \times (n-k)}$.

Proof We need to show that $S_{\text{MRD}}$ contains a non-empty Zariski-open set. In fact we will show that $S_{\text{MRD}}$ is a non-empty Zariski-open set. The non-emptiness follows from the existence of Gabidulin codes for every set of parameters. Hence it remains to show that it is Zariski-open.

In the following we denote by $S^C$ the complement of the set $S$. If we denote the entries of $X \in \overline{F}_{q^m}^{k \times (n-k)}$ as the variables $x_1, \ldots, x_{k(n-k)}$, then, for a given $A \in F_q^{n \times k}$, we have

$$\det([I_k \mid X]A) \in F_q[x_1, \ldots, x_{k(n-k)}].$$

Hence we can write

$$S_{\text{MRD}} = \bigcap_{A \in F_q^{n \times k}, \text{rk}(A) = k} \{ X \in \overline{F}_{q^m}^{k \times (n-k)} \mid \det([I_k \mid X]A) \neq 0 \},$$

i.e., it is a finite intersection of Zariski-open sets. Therefore, $S_{\text{MRD}}$ is a Zariski-open set. ☐

Remark 18 In Theorem 17 we chose the MRD criterion of Proposition 13 to show that the set of matrices $X \in \overline{F}_{q^m}^{k \times (n-k)}$ satisfying that criterion is generic. One can do the same by using the MRD criterion of Horlemann–Trautmann–Marshall from [7, Corollary 3.3].

We now turn to generalized Gabidulin codes. Firstly, we rewrite the criterion from Theorem 14 in a more suitable way.

Lemma 19 Let $C \subseteq F_{q^m}^n$ be an MRD code of dimension $k$ with generator matrix $[I_k \mid X]$, and let $0 < s < m$ with $\gcd(s, m) = 1$. $C$ is a generalized Gabidulin code with parameter $s$ if and only if

$$\text{rk}(X^{(s)} - X) = 1.$$

Proof We know from Theorem 14 that an MRD code $C = \text{rs}[I_k \mid X] \subseteq F_{q^m}^n$ is a generalized Gabidulin code if and only if $\dim(C \cap C^{(s)}) = k - 1$. We get

$$\dim(C \cap C^{(s)}) = k - 1 \iff \text{rk} \begin{bmatrix} I_k & X \\ I_k & X^{(s)} \end{bmatrix} = k + 1 \iff \text{rk} \begin{bmatrix} I_k & X \\ 0 & X^{(s)} - X \end{bmatrix} = k + 1 \iff \text{rk}(X^{(s)} - X) = 1.$$

The following theorem shows that the set of generator matrices not fulfilling the generalized Gabidulin criterion of Lemma 19 is generic over the algebraic closure.
Theorem 20 Let $1 \leq k \leq n - 1$ and $0 < s < m$ with $\gcd(s, m) = 1$. Moreover, let $S_{\text{MRD}} \subseteq \mathbb{F}_{q^m}^{k \times (n-k)}$ be as defined in Theorem 17. The set
\[ S_{\text{Gab}, s} := \{ X \in \mathbb{F}_{q^m}^{k \times (n-k)} \mid \rk(X^{(s)}) - X) = 1 \} \cap S_{\text{MRD}} \]
is a Zariski-closed subset of the Zariski-open set $S_{\text{MRD}}$.

Proof Let $X \in S_{\text{Gab}, s}$. Since $X \in S_{\text{MRD}}$, it follows from Lemma 8 that $X_{ij} \notin \mathbb{F}_q$ for $i = 1, \ldots, k$ and $j = 1, \ldots, n - k$. Then the condition $\rk(X^{(s)} - X) = 1$ is equivalent to $\rk(X^{(s)} - X) < 2$, which in turn is equivalent to the condition that all $2 \times 2$-minors of $(X^{(s)} - X)$ are zero.

If we denote the entries of $X \in \mathbb{F}_{q^m}^{k \times (n-k)}$ as the variables $x_1, \ldots, x_{k(n-k)}$, then these $2 \times 2$-minors of $(X^{(s)} - X)$ are elements of $\mathbb{F}_q[x_1, \ldots, x_{k(n-k)}]$. Let us call the set of all these minors $S'$. Then
\[ S_{\text{Gab}, s} = \left\{ X \in \mathbb{F}_{q^m}^{k \times (n-k)} \mid f(x_1, \ldots, x_{k(n-k)}) = 0, \quad \forall f \in S' \right\} \cap S_{\text{MRD}} = V(S') \cap S_{\text{MRD}}. \]

Hence it is a Zariski-closed subset of $S_{\text{MRD}} \subseteq \mathbb{F}_{q^m}^{k \times (n-k)}$. \qed

Theorem 20 implies that the complement in $S_{\text{MRD}}$ of $S_{\text{Gab}, s}$, i.e., the set of $k \times (n-k)$ matrices over $\mathbb{F}_{q^m}$ that fulfill the MRD criterion but do not fulfill the generalized Gabidulin criterion, is a Zariski-open subset of $S_{\text{MRD}}$. Thus, if it is non-empty, then the complement of $S_{\text{Gab}, s}$ is a generic set. The non-emptiness of this set will be shown in the following section, in Theorem 32.

In other words, over the algebraic closure, a randomly chosen generator matrix fulfills the MRD criterion and does not fulfill the generalized Gabidulin criterion with probability 1.

4 Probability estimations

In the previous section we have used the Zariski topology to show that a randomly chosen linear code over $\mathbb{F}_{q^m}$ fulfills most likely the MRD criterion but not the generalized Gabidulin criterion. Intuitively this tells us that over a finite, but large, extension field of $\mathbb{F}_q$ a randomly chosen linear code is most likely an MRD code but not a generalized Gabidulin code. In this section we derive some bounds on the probability that this statement is true, in dependence of the field extension degree $m$.

4.1 Probability for MRD codes

Here we give a lower bound on the probability that a random linear rank-metric code in $\mathbb{F}_{q^m}^n$ is MRD. A straight-forward approach gives the following result.

Theorem 21 Let $X \in \mathbb{F}_{q^m}^{k \times (n-k)}$ be randomly chosen. Then
\[ \Pr(\{ X \mid X \text{ is an MRD code} \}) \geq 1 - k \prod_{i=0}^{k-1} \left( \frac{q^n - q^i}{q^m} \right) \geq 1 - k q^{kn-m}. \]
Proof It follows from Proposition 13 that \( rs[I_k \mid X] \) is a non-MRD code if and only if
\[
p^* := \prod_{A \in \mathbb{F}_q^{n \times k} \atop \text{rk}(A) = k} \det((I_k \mid X)A) = 0.
\]
If we see the entries of \( X \) as the variables \( x_1, \ldots, x_{k(n-k)} \), then every variable \( x_i \) is contained in at most one row of the matrix
\[
[I_k \mid X]A = (A_{ij} + \sum_{\ell = k+1}^n X_{i(\ell-k)} A_{ij})_{i,j}.
\]
Thus, \( \det((I_k \mid X)A) \in \mathbb{F}_q[x_1, \ldots, x_{k(n-k)}] \) has degree at most \( k \). The number of matrices in \( \mathbb{F}_q^{n \times k} \) of rank \( k \) is
\[
\prod_{i=0}^{k-1} (q^n - q^i) \leq q^{kn},
\]
and hence the degree of \( p^* \) is at most \( k \prod_{i=0}^{k-1} (q^n - q^i) \).

It follows from Lemma 16 that
\[
\Pr( \text{rs}[I_k \mid X] \text{ is not an MRD code } ) \leq \frac{\deg p^*}{q^m}
\]
and hence
\[
\Pr( \text{rs}[I_k \mid X] \text{ is an MRD code } ) \geq 1 - \frac{\deg p^*}{q^m}
\geq 1 - k \prod_{i=0}^{k-1} (q^n - q^i) \geq 1 - k q^{kn-m}.
\]

In the remainder of this subsection we want to improve the bound obtained in Theorem 21. To do so we introduce the set
\[
T(k, n) = \left\{ E \in \mathbb{F}_q^{k \times n} \mid E \text{ is in reduced row echelon form and } \text{rk}(E) = k \right\}.
\]
With this notation we can formulate a variation of Proposition 13:

**Proposition 22** Let \( G \in \mathbb{F}_q^{k \times n} \) be a generator matrix of a rank-metric code \( C \subseteq \mathbb{F}_q^n \). Then \( C \) is an MRD code if and only if
\[
\text{rk}(EG^T) = k
\]
for all \( E \in T(k, n) \).

Proof For every matrix \( V \in \mathbb{F}_q^{k \times n} \) consider its reduced row echelon form \( E_V \). I.e., there exists a matrix \( R \in \text{GL}_k(q) \) such that \( V = RE_V \). Then
\[
\det(VE^T) = \det(RE_VE^T) = \det(R) \det(E_VE^T),
\]
and, since \( \det(R) \neq 0 \), we obtain that \( \text{rk}(VE^T) = k \) if and only if \( \text{rk}(E_VE^T) = k \). By Proposition 13 the statement follows.

For \( E \in T(k, n) \) we define the polynomial
\[
f_E(x_1, \ldots, x_{k(n-k)}) := \det((I_k \mid X)E^T) \in \mathbb{F}_q[x_1, \ldots, x_{k(n-k)}],
\]
and we furthermore define
\[
f^*(x_1, \ldots, x_{k(n-k)}) := \text{lcm} \left\{ f_E(x_1, \ldots, x_{k(n-k)}) \mid E \in T(k, n) \right\},
\]
\[
\square\text{ Springer}
\]
where, as before, the entries of $X$ are the variables $x_1, \ldots, x_{k(n-k)}$. We can easily observe the following.

**Proposition 23** The set of linear non-MRD codes of dimension $k$ in $\mathbb{F}_{q^m}^n$ is in one-to-one correspondence with the algebraic set

$$V(\{f^*\}) = \left\{ (v_1, \ldots, v_{k(n-k)}) \in \mathbb{F}_{q^m}^{k(n-k)} \mid f^*(v_1, \ldots, v_{k(n-k)}) = 0 \right\}.$$  

*Proof* It follows from Proposition 22 that the set of linear non-MRD codes of dimension $k$ in $\mathbb{F}_{q^m}^n$ is in one-to-one correspondence with the algebraic set

$$V = \bigcup_{E \in \mathcal{T}(k,n)} \left\{ (v_1, \ldots, v_{k(n-k)}) \in \mathbb{F}_{q^m}^{k(n-k)} \mid f_E(v_1, \ldots, v_{k(n-k)}) = 0 \right\}$$

$$= \left\{ (v_1, \ldots, v_{k(n-k)}) \in \mathbb{F}_{q^m}^{k(n-k)} \mid \prod_{E \in \mathcal{T}(k,n)} f_E(v_1, \ldots, v_{k(n-k)}) = 0 \right\}$$

$$= \left\{ (v_1, \ldots, v_{k(n-k)}) \in \mathbb{F}_{q^m}^{k(n-k)} \mid f^*(v_1, \ldots, v_{k(n-k)}) = 0 \right\},$$

where the last two equalities follow from the well-known fact that

$$V(\{f\}) \cup V(\{g\}) = V(\{fg\}) = V(\{\text{lcm}(f, g)\})$$

for any $f, g \in \mathbb{F}_q[x_1, \ldots, x_{k(n-k)}]$.

Note that in the definition of an algebraic set, it suffices to use the square-free part of the defining polynomial(s). In the above definition of $V$ however, $f^*(x_1, \ldots, x_{k(n-k)})$ is already square-free, as we show in the following.

**Lemma 24** For every $E \in \mathcal{T}(k,n)$ the polynomial $f_E(x_1, \ldots, x_{k(n-k)})$ is square-free. In particular, the polynomial $f^*(x_1, \ldots, x_{k(n-k)})$ is square-free.

*Proof* As in the proof of Theorem 21, every variable $x_i$ is contained in at most one row of the matrix $[I_k \mid X]E^T$. Hence, in the polynomial $f_E(x_1, \ldots, x_{k(n-k)})$ the degree with respect to every variable is at most 1. Thus, $f_E(x_1, \ldots, x_{k(n-k)})$ cannot have multiple factors.  

We now determine an upper bound on the degree of the defining polynomial $f^*$.

**Lemma 25** Let $E \in \mathcal{T}(k,n)$ and let $\mathcal{U}_0$ be the subspace of $\mathbb{F}_q^n$ defined by

$$\mathcal{U}_0 := \text{rs}[ I_k \mid 0 ] = \left\{ (u_1, \ldots, u_n) \in \mathbb{F}_q^n \mid u_{k+1} = u_{k+2} = \ldots = u_n = 0 \right\}.$$  

Then

$$\deg f_E = k - \dim (\text{rs}(E) \cap \mathcal{U}_0).$$

*Proof* Let $r := k - \dim (\text{rs}(E) \cap \mathcal{U}_0)$ with $0 \leq r \leq k$. We can write

$$E^T = \begin{bmatrix} E_1 \\ E_2 \end{bmatrix},$$

where $E_1 \in \mathbb{F}_q^{k \times k}, E_2 \in \mathbb{F}_q^{(n-k) \times k}$. Since $\dim (\text{rs}(E) \cap \mathcal{U}_0) = k - r$, we have $\text{rk}(E_2) = r$. Thus, there exists a matrix $R \in \text{GL}_k(q)$ such that the first $r$ columns of $E_2R$ are linearly independent and the last $k-r$ columns are zero. Then

$$f_E(x_1, \ldots, x_{k(n-k)}) = \text{det}(\begin{bmatrix} I_k & X \end{bmatrix}E^T) = \text{det}(R)^{-1} \text{det}(E_1R + XE_2R).$$
The last \( k - r \) columns of the matrix \( X E_2 R \) are zero, i.e., the last \( k - r \) columns of \( E_1 R + X E_2 R \) do not contain any of the variables \( x_i \). On the other hand, the entries of the first \( r \) columns are polynomials in \( \mathbb{F}_q[x_1, \ldots, x_{(n-k)}] \) of degree 1, since

\[
E_1 R + X E_2 R = \left( \sum_{\ell=1}^{n} (E_1)_{i\ell} R_{ij} + \sum_{\ell=1}^{k} \sum_{\ell'=1}^{n} X_{i\ell'} (E_2)_{\ell'j} R_{ij} \right)_{i,j}.
\]

Hence we have \( \deg f_E \leq r \).

Now consider the matrix \( E_2 R \). We can write

\[
E_2 R = \begin{bmatrix} \tilde{E}_2 & 0 \end{bmatrix}
\]

where \( \tilde{E}_2 \) is an \( (n-k) \times r \) matrix of rank \( r \). Hence

\[
XE_2 R = \begin{bmatrix} X \tilde{E}_2 & 0 \end{bmatrix}.
\]

First we prove that the entries of the matrix \( X \tilde{E}_2 \) are algebraically independent over \( \mathbb{F}_q \). Fix \( 1 \leq i \leq k \) and denote by \( (X \tilde{E}_2)_i \) the \( i \)-th row of the matrix \( X \tilde{E}_2 \). Then consider the polynomials \( (X \tilde{E}_2)_{ij} \), for \( j = 1, \ldots, r \), that only involve the variables \( x_{(i-1)(n-k)+1}, \ldots, x_{(n-k)} \). The Jacobian of these polynomials is \( \tilde{E}_2^T \), whose rows are linearly independent over \( \mathbb{F}_q \). Therefore the elements in every row are algebraically independent over \( \mathbb{F}_q \).\(^1\) Moreover, different rows involve different variables, hence we can conclude that the entries of the matrix \( X \tilde{E}_2 \) are algebraically independent over \( \mathbb{F}_q \).

At this point consider the set of all \( r \times r \) minors of \( X \tilde{E}_2 \). These minors are all different and hence linearly independent over \( \mathbb{F}_q \), otherwise a non-trivial linear combination of them that gives 0 would produce a non-trivial polynomial relation between the entries of \( X \tilde{E}_2 \). Now observe that the degree \( r \) term of \( f_E \) is a linear combination of these minors. If we write

\[
E_1 R = \begin{bmatrix} \ast & \tilde{E}_1 \end{bmatrix},
\]

where \( \tilde{E}_1 \in \mathbb{F}_q^{k \times (k-r)} \), then the coefficients of this linear combination are given by the \( (k-r) \times (k-r) \) minors of \( \tilde{E}_1 \), multiplied by \( \det(R)^{-1} \). Since \( E^T R \) has rank \( k \) and the last \( k-r \) columns of \( E_2 R \) are 0, it follows that the columns of \( \tilde{E}_1 \) are linearly independent, and hence at least one of the coefficients of the linear combination is non-zero. This proves that the degree \( r \) term of \( f_E \) is non-zero, and hence \( \deg f_E = r \).

We can now give the main result of this subsection, an upper bound on the probability that a random generator matrix generates an MRD code:

**Theorem 26** Let \( X \in \mathbb{F}_q^{k \times (n-k)} \) be randomly chosen. Then

\[
\Pr\left( \text{rs}[I_k | X] \text{ is an MRD code} \right) \geq 1 - \sum_{r=0}^{k} \binom{k}{k-r} \binom{n-k}{r} q^{r^2} q^{-m}.
\]

**Proof** For every \( r = 0, 1, \ldots, k \) we define the set

\[
T_r = \{ E \in T(k, n) \mid \dim(U_0 \cap \text{rs}(E)) = k-r \},
\]

\(^1\) The Jacobian criterion for algebraic independence of polynomials over \( \mathbb{C} \) can be found in [9, Chap. I, Sect. 5]. In positive characteristic, it remains true that the linear independence of the rows of the Jacobian matrix of a set of polynomials implies the algebraic independence of them.
where
\[ U_0 := \text{rs}[ I_k \mid 0 ] = \left\{ (u_1, \ldots, u_n) \in F_q^n \mid u_{k+1} = u_{k+2} = \cdots = u_n = 0 \right\} . \]

By Lemma 3 we have
\[ |T_r| = \binom{k}{k-r} q \binom{n-k}{r} q^r . \]

Moreover, by Lemma 25, if \( E \in T_r \), then \( \text{deg } f_E = r \). Hence, by the definition of \( f^*(x_1, \ldots, x_{k(n-k)}) \), we have
\[ \text{deg } f^* \leq \sum_{E \in T(k,n)} \text{deg } f_E = \sum_{r=0}^k \sum_{E \in T_r} r \binom{k}{k-r} q \binom{n-k}{r} q^r . \]

With Lemma 16, the statement follows.

Remember that we know how to construct MRD codes, namely as Gabidulin codes, for any set of parameters. Hence the probability that a randomly chosen generator matrix generates an MRD code is always greater than zero. However, the lower bound of Theorem 26 is not always positive. In particular, for
\[ m < k(n-k) + \log_q k \]
we get
\[
1 - \sum_{r=0}^k r \binom{k}{k-r} q \binom{n-k}{r} q^r q^m = 1 - q^{-m} \left( k \binom{n-k}{k} q^{k^2} + \sum_{r=1}^{k-1} r \binom{k}{k-r} q \binom{n-k}{r} q^r \right) \leq 1 - q^{-m} \left( kq^{k(n-k)} \right) < 0 ,
\]
i.e., the bound is not tight (and not sensible) in these cases.

Figure 1 depicts the lower bounds of Theorems 21 and 26 for some small parameters. One can see that the bound of Theorem 26 really is an improvement over the bounds of Theorem 21.

4.2 Probability for Gabidulin codes

We have seen in Lemma 19 that the set of matrices in \( \text{rs}[ I_k \mid X ] \) in systematic form, that generate a generalized Gabidulin code with parameter \( s \) (such that \( 0 < s < m \) with \( \text{gcd}(s, m) = 1 \)), is in one-to-one correspondence with a subset of the set
\[ \left\{ X \in \text{rs}[ I_{k \times (n-k)} ] \mid \text{rk}(X^{(s)}) - X = 1 \right\} , \]
namely with the elements that represent an MRD code. By Lemma 8 we furthermore know that, if \( X \) has entries from \( F_q \), then \( \text{rs}[ I_k \mid X ] \) is not MRD. Hence the set of matrices in systematic form that generate a generalized Gabidulin code is in one-to-one correspondence with a subset of the set
\[ \mathcal{G}(s) := \left\{ X \in (F_q^m \setminus F_q) \times (n-k) \mid \text{rk}(X^{(s)}) - X = 1 \right\} . \]
For simplicity we make the following estimation of the probability that a randomly chosen generator matrix generates a generalized Gabidulin code.

**Lemma 27** Let $X \in \mathbb{F}_q^{k \times (n-k)}$ be randomly chosen. Then

$$
\Pr \left( \text{rs}[I_k \mid X] \text{ is a gen. Gabidulin code} \right) \leq \sum_{0 < s < m} \Pr \left( X \in \mathcal{G}(s) \right)
$$
\[
\sum_{0 < s < m \atop \gcd(s, m) = 1} \frac{|G(s)|}{q^{mk(n-k)}}.
\]

**Proof** The inequality follows from the fact that the set of generalized Gabidulin codes is in one-to-one correspondence with a subset of the set

\[
\bigcup_{0 < s < m \atop \gcd(s, m) = 1} G(s).
\]

Since \( |\mathbb{F}_q^k \times (n-k) | = q^{mk(n-k)} \), the statement follows. \( \square \)

For every integer \( 0 < s < m \) with \( \gcd(m, s) = 1 \), we now define the map \( \Phi_s \) given by

\[
\Phi_s : \mathbb{F}_q^k \times (n-k) \rightarrow \mathbb{F}_q^k \times (n-k)
\]

\[
X \mapsto X^{[s]} - X.
\]

Observe that \( \Phi_s \) is exactly the function that maps every entry \( X_{ij} \) of the matrix \( X \) to \( \varphi_s(X_{ij}) \).

Moreover, we define the sets

\[
\mathcal{R}_1 := \{ A \in \mathbb{F}_q^k \times (n-k) \mid \rk(A) = 1 \},
\]

\[
\mathcal{R}_1^* := \{ A \in (\mathbb{F}_q^*)^k \times (n-k) \mid \rk(A) = 1 \},
\]

\[
\mathcal{K} := (\ker(\Tr_{\mathbb{F}_q^m/\mathbb{F}_q}))^{k \times (n-k)}.
\]

We state now the crucial results that will help us to compute an upper bound on the cardinality of the sets \( G(s) \).

**Lemma 28**

1. Given a matrix \( A \in \mathbb{F}_q^k \times (n-k) \), there exists a matrix \( X \in \mathbb{F}_q^k \times (n-k) \) such that \( \Phi_s(X) = A \) if and only if \( A \in \mathcal{K} \).

2. If \( A \in \mathcal{R}_1 \), then

\[
|\Phi_s^{-1}(A)| = \begin{cases} 
0 & \text{if } A \notin \mathcal{K} \\
q^{k(n-k)} & \text{if } A \in \mathcal{K}.
\end{cases}
\]

3. For every integer \( s \) coprime to \( m \)

\[
G(s) = \Phi_s^{-1}(\mathcal{R}_1^* \cap \mathcal{K}),
\]

and

\[
|G(1)| = |G(s)| = q^{k(n-k)} |\mathcal{R}_1^* \cap \mathcal{K}|.
\]

**Proof**

1. Since \( \Phi_s \) is the function that maps every entry \( X_{ij} \) of the matrix \( X \) to \( \varphi_s(X_{ij}) \), we have that \( A \in \text{Im}(\Phi_s) \) if and only if every entry \( A_{ij} \) of \( A \) belongs to \( \text{Im}(\varphi_s) \). By Lemma 2 part 6 this is true if and only if every \( A_{ij} \) belongs to \( \ker(\Tr_{\mathbb{F}_q^m/\mathbb{F}_q}) \).

2. If \( A \notin \mathcal{K} \), then by part 1 this means that \( \Phi_s^{-1}(A) = \emptyset \). Otherwise, again by part 1, \( \Phi_s^{-1}(A) \neq \emptyset \). In this case every entry \( A_{ij} \) belongs to \( \text{Im}(\varphi_s) \), and since \( \varphi_s \) is linear over \( \mathbb{F}_q \), \( |\varphi_s^{-1}(A_{ij})| = |\ker(\varphi_s)| \). Since, by Lemma 2,

\[
|\ker(\varphi_s)| = \frac{|\mathbb{F}_q^m|}{|\text{Im}(\varphi_s)|} = q,
\]

and \( A \) has \( k(n-k) \) entries, we get \( |\Phi_s^{-1}(A)| = q^{k(n-k)} \).
3. Observe that $\mathcal{R}_1^* = \mathcal{R}_1 \cap (\mathbb{F}_{q^n}^{k \times (n-k)})$. Moreover

$$\Phi_s^{-1}(\mathcal{R}_1) = \left\{ X \in \mathbb{F}_{q^n}^{k \times (n-k)} \mid \text{rk}(X^{(s)}) - X = 1 \right\}$$

and, by Lemma 2 part 5,

$$\Phi_s^{-1}\left( (\mathbb{F}_{q^n}^{k \times (n-k)}) \right) = (\mathbb{F}_{q^n} \setminus \mathbb{F}_q)^{k \times (n-k)}.$$ 

Hence

$$\Phi_s^{-1}(\mathcal{R}_1^*) = \Phi_s^{-1}\left( \mathcal{R}_1 \cap (\mathbb{F}_{q^n}^{k \times (n-k)}) \right) = \Phi_s^{-1}(\mathcal{R}_1) \cap \Phi_s^{-1}\left( (\mathbb{F}_{q^n}^{k \times (n-k)}) \right) = \mathcal{G}(s).$$

Now we can write

$$\mathcal{R}_1^* = (\mathcal{R}_1^* \cap \mathcal{K}) \cup (\mathcal{R}_1^* \cap \mathcal{K}^c)$$

and by part 1 we have that $\Phi_s^{-1}(\mathcal{R}_1^* \cap \mathcal{K}^c) = \emptyset$. Then

$$\mathcal{G}(s) = \Phi_s^{-1}(\mathcal{R}_1^*) = \Phi_s^{-1}(\mathcal{R}_1^* \cap \mathcal{K}) \cup \Phi_s^{-1}(\mathcal{R}_1^* \cap \mathcal{K}^c) = \Phi_s^{-1}(\mathcal{R}_1^* \cap \mathcal{K}).$$

By part 2 we have $|\Phi_s^{-1}(\mathcal{R}_1^* \cap \mathcal{K})| = q^{k(n-k)}|\mathcal{R}_1^* \cap \mathcal{K}|$, which proves the statement.

\[\square\]

In analogy to the previous subsection we now first derive a straightforward upper bound on the probability that a random generator matrix gives rise to a generalized Gabidulin code. Afterwards we will improve this bound.

**Theorem 29** Let $X \in \mathbb{F}_{q^n}^{k \times (n-k)}$ be randomly chosen. Denote by $\phi(m)$ the Euler-$\phi$-function. Then

$$\Pr\left( \text{rs}[I_k \mid X] \text{ is a generalized Gabidulin code} \right) \leq \phi(m)(2q^{1-m})\left\lfloor \frac{1}{2} \right\rfloor \left\lfloor \frac{n-k}{2} \right\rfloor$$

**Proof** We want to derive the cardinality of $\mathcal{G}(s)$ for any valid $s$. For this, by Lemma 28 part 3, we note that these cardinalities are all equal to the cardinality of $\mathcal{G}(1)$. Now for any $X \in (\mathbb{F}_{q^n} \setminus \mathbb{F}_q)^{k \times (n-k)}$ the rank of $X^{(q)} - X$ is greater than zero. Therefore we can also write

$$\mathcal{G}(1) = \left\{ X \in (\mathbb{F}_{q^n} \setminus \mathbb{F}_q)^{k \times (n-k)} \mid \text{rk}(X^{(q)} - X) \leq 1 \right\}.$$ 

The condition that $\text{rk}(X^{(q)} - X) \leq 1$ is equivalent to that any $2 \times 2$-minor of $X^{(q)} - X$ is zero. Hence a necessary condition is that any set of non-intersecting minors is zero. We have $\left\lfloor \frac{1}{2} \right\rfloor \left\lfloor \frac{n-k}{2} \right\rfloor$ many such non-intersecting minors, each of which has degree at most $2q$ if we see the entries of $X$ as the variables $x_1, \ldots, x_{k(n-k)}$. With Lemma 16 we get for each minor $M_{ij}$,

$$\Pr(M_{ij} = 0) \leq 2q^{1-m}.$$ 

Since the non-intersecting minors are independent events, the probability that all of these are zero is at most

$$(2q^{1-m})\left\lfloor \frac{1}{2} \right\rfloor \left\lfloor \frac{n-k}{2} \right\rfloor.$$ 

With Lemma 27 and the fact that the number of $s$ with $\text{gcd}(s, m) = 1$ is given by $\phi(m)$, the statement follows.
To improve the above bound we need the following lemma.

**Lemma 30** The set $\mathcal{R}_{1}^{*} \cap \mathcal{K}$ is in one-to-one correspondence with the set

$$V_{R} := \left\{ (\alpha, \beta) \in \mathbb{F}_{q^{m}}^{k} \times \mathbb{F}_{q^{m}}^{n-k-1} \mid \alpha_i, \alpha_i \beta_j \in \ker \left( \text{Tr}_{\mathbb{F}_{q^{m}}/\mathbb{F}_{q}} \right) \setminus \{0\} \right\}$$

$$= \left\{ (\alpha, \beta) \in \mathbb{F}_{q^{m}}^{k} \times \mathbb{F}_{q^{m}}^{n-k-1} \mid \alpha_i \in \ker \left( \text{Tr}_{\mathbb{F}_{q^{m}}/\mathbb{F}_{q}} \right) \setminus \{0\}, \beta_j \in \bigcap_{i=1}^{k} \ker \left( T_{\alpha_i} \right) \setminus \{0\} \right\}$$

via the map $\psi : V_{R} \rightarrow \mathcal{R}_{1}^{*} \cap \mathcal{K}$, given by

$$(\alpha, \beta) \mapsto \begin{bmatrix} \alpha_1 \\ \vdots \\ \beta_1, \ldots, \beta_{n-k-1} \end{bmatrix}.$$ 

and hence

$$|\mathcal{R}_{1}^{*} \cap \mathcal{K}| \leq (q^{m-1} - 1)^{n-1}.$$ 

**Proof** From the definition of the set $V_{R}$ it is clear that the map $\psi$ is well-defined, i.e., it maps every element in $V_{R}$ to an element in $\mathcal{R}_{1}^{*} \cap \mathcal{K}$.

Let $(\alpha, \beta), (\gamma, \delta)$ be two elements that have the same image. Then the first column of $\psi(\alpha, \beta)$ and the first column of $\psi(\gamma, \delta)$ are equal, hence $\alpha = \gamma$. Also the first rows of $\psi(\alpha, \beta)$ and $\psi(\gamma, \delta)$ are equal, thus $\alpha_1 \beta_j = \gamma_1 \delta_j$ for every $j = 1, \ldots, n-k-1$, and since $\alpha_1 = \gamma_1 \neq 0$ we get $\beta = \delta$ and this shows the injectivity of the map $\psi$.

In order to show the surjectivity consider a rank 1 matrix $A \in \mathcal{R}_{1}^{*} \cap \mathcal{K}$ with entries $A_{ij}$. Consider the vectors $\alpha = (A_{11}, \ldots, A_{k1})^{T}$ and $\beta = A_{11}^{-1} (A_{12}, \ldots, A_{1(n-k)})^{T}$.

It is clear that $(\alpha, \beta) \in V_{R}$, and that $\psi(\alpha, \beta) = A$.

At this point for every $\alpha_i$ we have $q^{m-1} - 1$ possible choices, while for every $\beta_i$ we have a number of choices that is less or equal to $| \ker(T_{\alpha_i}) \setminus \{0\} |$, that is again $q^{m-1} - 1$. Therefore we get

$$|\mathcal{R}_{1}^{*} \cap \mathcal{K}| \leq (q^{m-1} - 1)^{n-1}.$$ 

We can now formulate the main result concerning the probability that a random linear rank-metric code is a generalized Gabidulin code.

**Theorem 31** Let $X \in \mathbb{F}_{q^{m}}^{k \times (n-k)}$ be randomly chosen. Then

$$\Pr \left( \text{rs}[I_{k} \mid X] \text{ is a gen. Gabidulin code} \right) \leq \phi(m) q^{-(m-1)(n-k-1)(k-1)},$$

where $\phi$ denotes the Euler-\( \phi \) function.

**Proof** We have already seen in Lemma 27 that

$$\Pr \left( \text{rs}[I_{k} \mid X] \text{ is a gen. Gabidulin code} \right) \leq \sum_{0<s<m \atop (s,m)=1} \frac{|G(s)|}{q^{mk(n-k)}}.$$
By Lemma 28 part 3, the sets \( G(s) \) all have cardinality \( q^{k(n-k) | \mathcal{R}^*_1 \cap \mathcal{K}} \), thus
\[
\sum_{0 < s < m \atop (s,m)=1} \frac{|G(s)|}{q^{mk(n-k)}} = \phi(m) \frac{q^{k(n-k) | \mathcal{R}^*_1 \cap \mathcal{K}}}{q^{mk(n-k)}}.
\]
Moreover, by Lemma 30, we know that \( |\mathcal{R}^*_1 \cap \mathcal{K}| \leq (q^{m-1}-1)^{n-1} \leq q^{(m-1)(n-1)}. \) Combining all the inequalities implies the statement.

\[\square\]

### 4.3 Existence of non-Gabidulin MRD codes

We can now use the probability estimations we got in Theorems 26 and 31 to give implicit and explicit results about the existence of linear MRD codes that are not generalized Gabidulin codes for almost every set of parameters.

**Theorem 32**  
For any prime power \( q \), and for any \( 1 < k < n - 1 \), there exists an integer \( M(q, k, n) \) such that, for every \( m \geq M(q, k, n) \), there exists a \( k \)-dimensional linear MRD code in \( \mathbb{F}_{q^m} \) that is not a generalized Gabidulin code.

An integer \( M(q, k, n) \) with this property can be found as the minimum integer solution of the inequality

\[
1 - \sum_{r=0}^{k} r \binom{k}{k-r} q^{r} q^{-m} > (m - 1)q^{-(m-1)(n-k)(k-1)} \tag{1}
\]
taken over all \( m \in \mathbb{N} \).

**Proof** For fixed \( q, k \) and \( n \) consider the function
\[
F(m) = \sum_{r=0}^{k} r \binom{k}{k-r} q^{r} q^{-m} = aq^{-m} + (m - 1)q^{-c(m-1)},
\]
where
\[
a := \sum_{r=0}^{k} r \binom{k}{k-r} q^{r}, \quad c := (n - k - 1)(k - 1).
\]
Since \( k \neq 1 \) and \( k \neq n - 1 \), we have \( c > 0 \). In this case \( F(m) \) is the sum of two non-increasing functions and hence it is non-increasing. Therefore the function \( 1 - F(m) \) is non-decreasing. Moreover, it is easy to see that
\[
\lim_{m \to +\infty} 1 - F(m) = 1.
\]
This means that the set of the solutions of Inequality (1) is non-empty. Then it has a minimum solution \( M(q, k, n) \). Since the function \( 1 - F(m) \) is non-decreasing, every \( m \geq M(q, k, n) \) is also a solution of (1). Hence, by Theorems 26 and 31, we have the following chain of inequalities for every \( m \geq M(q, k, n) \),
\[
\Pr \left( rs[I_k \mid X] \text{ is MRD} \right) \geq 1 - aq^{-m} > (m - 1)q^{-c(m-1)} \\
\geq \Pr \left( rs[I_k \mid X] \text{ is gen. Gabidulin} \right),
\]
which concludes the proof.

\[\square\]
The theorem above proves the existence of infinitely many integers \( m \) such that there exists a linear non-Gabidulin MRD code over \( \mathbb{F}_{q^m} \) of dimension \( k \) and length \( n \). These integers are given implicitly as the solutions of Inequality 1. In the following we derive such integers explicitly, in order to give an idea of the magnitude of the extension degree needed to have non-Gabidulin MRD codes.

We first need some auxiliary results: For \( b \in \mathbb{N} \) we consider the sequence \( \{ Q(b) \}_{b \in \mathbb{N}} \) defined as

\[
Q(b) := \prod_{i=1}^{b} \left( 1 - \frac{1}{2^i} \right).
\]

**Lemma 33** \( \{ Q(b) \}_{b \in \mathbb{N}} \) is a decreasing positive sequence, such that

\[
\lim_{b \to +\infty} Q(b) = C \simeq 0.2887.
\]

In particular, for every \( b \in \mathbb{N} \), \( Q(b) > \frac{1}{4} \).

**Proof** The sequence \( \{ Q(b) \}_{b \in \mathbb{N}} \) is trivially positive and decreasing. Its decimal expansion, which gives rise to the above approximation, can be found in [15] with ID number A048651. \( \square \)

**Lemma 34** Let \( a, b \) be two positive integers with \( 0 < b \leq a \). Then

\[
\binom{a}{b}_q \leq \frac{1}{Q(b)} q^{b(a-b)}.
\]

**Proof** We have

\[
\binom{a}{b}_q = \prod_{i=0}^{b-1} q^{a-i} - 1 \leq \prod_{i=0}^{b-1} q^{a-i} - \left( \frac{1}{2} \right)^{b-i} = \frac{1}{Q(b)} q^{b(a-b)}.
\]

\( \square \)

We can now state the explicit version of the existence of linear non-Gabidulin MRD codes:

**Theorem 35** Let \( q \) be a prime power, and let \( k, n \) be two integers such that \( 1 < k < n - 1 \). If

\[
m \geq k(n - k) + \lceil \log_q (4k + 1) \rceil,
\]

then there exists a \( k \)-dimensional linear MRD code in \( \mathbb{F}_{q^m}^n \) that is not a generalized Gabidulin code.

**Proof** We will prove the statement for the case \( n \geq 2k \). The other case, \( n < 2k \), then follows by duality, using Proposition 11.

As in the proof of Theorem 32, consider the function

\[
F(m) = \sum_{r=0}^{k} \binom{k}{k-r} \binom{n-k}{r} q^{r^2 q^{-m} + (m-1)q^{-(m-1)(n-k-1)(k-1)}}.
\]

We need to show that \( F(m) < 1 \) for \( m \geq k(n - k) + \lceil \log_q (4k + 1) \rceil \). We divide the proof into two cases.
Hence, we can conclude that for prime power which is fulfilled by the conditions

\[ k \leq m \]

where the last inequality follows from Lemmas 34 and 33. Moreover,

\[ (m - 1)q^{-m} \leq q^{-m} \]

Furthermore, we observe that

\[ n + k^2 + 1 - kn \leq 0 \iff n \geq \frac{k^2 + 1}{k - 1} \iff n \geq k + 1 + \frac{2}{k - 1}, \]

which is fulfilled by the conditions \( k \leq n/2 \) and \( n \geq 5 \). Therefore,

\[
\begin{align*}
(1 - m)(k(n - k) - n + 1) + \log_q (m - 1) - (k(n - k) - m) \\
= m(n + k^2 - kn) + 1 + \log_q (m - 1) - n \\
\leq m(n + k^2 - kn + 1) - n \\
\leq 0.
\end{align*}
\]

Combining this with Inequality (2) and Equality (3) we get

\[ F(m) < 4kq^{k(n-k)-m} + q^{(1-m)(k(n-k)-n+1)+\log_q (m-1)} \leq (4k + 1)q^{k(n-k)-m}. \]

Hence, we can conclude that for \( m \geq k(n - k) + \lceil \log_q (4k + 1) \rceil \), it holds that \( F(m) < 1 \), i.e., there exists a non-Gabidulin MRD code.

Case \( n = 4 \). This implies that \( k = 2 \) and \( m \geq 4 + \lceil \log_q (9) \rceil \). For these fixed values of \( k \) and \( n \) we consider \( F(m) = G(q, m) \) as a function of \( q \) and \( m \). We get

\[ G(q, m) = \frac{2q^4 + q^3 + 2q^2 + q}{q^m} + \frac{m - 1}{q^{m-1}}, \]

which is a decreasing function in both \( q \) and \( m \). Hence, if we fix \( q \), we have that

\[ G(q, 4 + \lceil \log_q (9) \rceil) \geq G(q, m), \]

for every \( m \geq 4 + \lceil \log_q (9) \rceil \). So we need to show that \( G(q, 4 + \lceil \log_q (9) \rceil) < 1 \) for every prime power \( q \). We have

\[
G(q, 4 + \lceil \log_q (9) \rceil) = \frac{2q^4 + q^3 + 2q^2 + q}{q^{4 + \lceil \log_q (9) \rceil}} + \frac{3 + \lceil \log_q (9) \rceil}{q^{3 + \lceil \log_q (9) \rceil}} \leq \frac{2q^4 + q^3 + 2q^2 + q}{9q^4} + \frac{3 + \lceil 2 \log_q (3) \rceil}{9q^3} =: K(q).
\]

We observe that \( K(q) \) is a decreasing function in \( q \). Therefore,

\[ G(q, 4 + \lceil \log_q (9) \rceil) \leq K(q) \leq K(2) = \frac{4}{9} < 1, \]

which concludes the proof. \( \square \)

\( \text{Springer} \)
Remark 36 In the previous theorem, the condition $1 < k < n - 1$ is not a real restriction, since one can easily see that all MRD codes of dimension $k = 1$ or $k = n - 1$ are Gabidulin codes, see e.g. [7, Thm. 5.1].

In Figs. 2 and 3 we compare the bounds derived in this section with experimental results, which we got by randomly generating over 500 rank-metric codes. The continuous lines show the bounds, the dotted lines show the experimental probabilities. In Fig. 2 we see that Gabidulin codes are very few among all MRD codes when the extension degree $m$ is large. The probabilities for generalized Gabidulin codes decrease so quickly for increasing parameters.
that we show them separately, in logarithmic scale, in Fig. 3. Notice that from \( m = 10 \) it is very difficult to generate a generalized Gabidulin code randomly and thus, experimentally we got a probability zero. This is why the experimental result was shown only up to \( m = 9 \).

For comparison, the lower bound for \( m \) (such that there exist non-Gabidulin MRD codes) from Theorem 35 is given in the following table:
5 Conclusion

In this work we have shown that, over the algebraic closure of a given finite field, MRD codes and non-Gabidulin codes are generic sets among all linear rank-metric codes. For this we have used two known criteria for these two properties, which give rise to algebraic descriptions of the respective sets. Afterwards we have used the same two criteria to establish a lower bound on the probability that a randomly chosen systematic generator matrix generates an MRD code, and an upper bound on the probability that a randomly chosen systematic generator matrix generates a generalized Gabidulin code. With these two bounds we were then able to show that non-Gabidulin MRD codes exist for any length $n$ and dimension $1 < k < n - 1$, as long as the underlying field size is large enough.

Acknowledgements This work was partially supported by SNF Grants Nos. 149716 and 169510.

References

1. Berger T.P.: Isometries for rank distance and permutation group of Gabidulin codes. IEEE Trans. Inf. Theory 49(11), 3016–3019 (2003). doi: 10.1109/TIT.2003.819322.
2. Cossidente A., Marino G., Pavese F.: Non-linear maximum rank distance codes. Des. Codes Cryptogr. 79(3), 597–609 (2016). doi: 10.1007/s10623-015-0108-0.
3. de la Cruz J., Kiermaier M., Wassermann A., Willems W.: Algebraic structures of MRD codes. arXiv:1502.02711 [cs.IT] (2015).
4. Delsarte P.: Bilinear forms over a finite field, with applications to coding theory. J. Comb. Theory Ser. A 25(3), 226–241 (1978). doi: 10.1016/0097-3165(78)90015-8.
5. Gabidulin E.M.: Theory of codes with maximum rank distance. Probl. Pereda. Inf. 21(1), 3–16 (1985).
6. Hartshorne R.: Algebraic Geometry, vol. 52. Springer, Berlin (2013).
7. Horlemann-Trautmann A., Marshall K.: New criteria for MRD and Gabidulin codes and some rank-metric code constructions. arXiv:1507.08641 [cs.IT] (2015).
8. Kshevetskiy A., Gabidulin E.: The new construction of rank codes. Proc. Int. Symp. Inf. Theory 2005, 2105–2108 (2005). doi: 10.1109/ISIT.2005.1523717.
9. Lefschetz S.: Algebraic Geometry. Courier Corporation, Boston (2012).
10. Lewin D., Vadhan S.: Checking polynomial identities over any field: towards a derandomization? In: Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, pp. 438–447. ACM (1998).
11. Lidl R., Niederreiter H.: Introduction to Finite Fields and their Applications. Cambridge University Press, Cambridge (1994). (Revised edition).
12. Morrison K.: Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes. IEEE Trans. Inf. Theory 60(11), 7035–7046 (2014). doi: 10.1109/TIT.2014.2359198.
13. Schwartz J.T.: Fast probabilistic algorithms for verification of polynomial identities. J. ACM 27(4), 701–717 (1980).
14. Sheekey J.: A new family of linear maximum rank distance codes. Adv. Math. Commun. 10(3), 475–488 (2016).
15. Sloane N.J.A., et al.: The on-line encyclopedia of integer sequences (2003). https://oeis.org/.
16. Wan Z.X.: Geometry of Matrices. World Scientific, Singapore (1996). In memory of Professor L.K. Hua (1910–1985).