# On the Sparsity of MRD Codes

Eimear Byrne and Alberto Ravagnani

School of Mathematics and Statistics, University College Dublin, Ireland
{ebyrne,alberto.ravagnani}@ucd.ie

**Abstract.** It is classically known that MDS codes in $\mathbb{F}_q^n$ are dense within the family of $\mathbb{F}_q$-linear block codes with the same dimension as $q \to +\infty$. In the rank-metric, MRD codes are the analogue of MDS codes, and it has been proven recently that they are dense within the family of $\mathbb{F}_{q^m}$-linear codes having the same dimension for $m \to +\infty$. In this paper, we show that $\mathbb{F}_q$-linear matrix MRD codes exhibit a completely different behaviour. More precisely, we prove that MRD matrix codes in $\mathbb{F}_q^{n\times m}$ are not dense within the family of $\mathbb{F}_q$-linear codes with the same dimension, both as $q \to +\infty$ and as $m \to +\infty$. More precisely, we show that their density is asymptotically upper bounded by $1/2$. This is in sharp contrast with the behaviour of MDS and $\mathbb{F}_{q^m}$-linear vector MRD codes.

**Keywords:** rank metric code · MRD code · density problems

## 1 Introduction

The results presented in this extended abstract summarize some sections of the preprint [3], in which the notion of a *partition-balanced family* of codes is applied to determine the density or sparsity of codes that are extremal with respect to properties such as minimum distance and maximality. Here, we focus the discussion on the first of these properties.

Rank metric codes [4,5,14] have seen a recent resurgence of interest both for their potential use in code based cryptography and as error-correcting codes in network communications. See [6,16] among many others. The rank metric analogue of the Singleton bound yields the class of *maximum rank distance* (MRD) codes, which exist for all choices of $m, n$ and minimum distance $d$, both for $\mathbb{F}_{q^m}$-linear subspaces of $\mathbb{F}_{q^m}^n$ (vector rank metric codes) and the larger class of $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^{n\times m}$ (matrix rank metric codes).

While vector rank metric codes exhibit a behaviour similar to block codes for the Hamming metric, there is considerable divergence between these families and the class of matrix rank metric codes. Perhaps the most profound difference is to be seen in the behaviour of the density functions of codes that are extremal with respect to the minimum distance. We will show that, while both MDS and vector rank metric MRD codes are dense among codes having the same dimension, the matrix MRD codes are *never* dense in this sense, neither as $q \to +\infty$ and nor as $m \to +\infty$. This behaviour was also observed independently in [1] for $q \to +\infty$.

We give a brief outline of this paper. Section 2 contains some preliminaries on linear codes. In Section 3 we define density functions and define what we mean

by the terms *sparse* and *dense*. We also give an exposition on how to establish the density of both the MDS linear block codes and the MRD vector linear codes using the Schwartz-Zippel Lemma and explain why this approach does not apply in the case of matrix rank metric codes.

The main results can be read in Sections 4 and 5. In Section 4 we give a lower bound on the number of non-MRD matrix codes of a fixed dimension, and we use this for the results of Section 5. We first show that for any $\varepsilon > 0$, and for sufficiently large $q$, the proportion of non-MRD matrix codes within the family of all codes of the same dimension is at least $1/2-\varepsilon$. We also show for any fixed $q$ and $\varepsilon > 0$, this proportion is at least $1/2(q/(q-1) - 1/(q-1)^2) - \varepsilon \geq 1/2 - \varepsilon$ for sufficiently large $m$.

## 2 Codes for the Hamming and the Rank Metric

In this paper, $q$ denotes a prime power and $k, n, m$ are non-negative integers with $m \geq n \geq 1$ and $k \leq n$.

Recall that an $[n,k]_q$ code is a $k$-dimensional subspace $C \leq \mathbb{F}_q^n$. If $k \geq 1$, then the **minimum** (**Hamming**) **distance** of $\mathcal{C}$ is

$$d_{\mathrm{H}}(C) := \min\{\omega_{\mathrm{H}}(x) \mid x \in C,\ x \neq 0\},$$

where $\omega_{\mathrm{H}}$ is the Hamming weight on $\mathbb{F}_q^n$. The dimension of a non-zero $[n,k]_q$ code satisfies $k \leq n - d_{\mathrm{H}}(C) + 1$. This is the well-known Singleton bound [17]. Codes that meet this bound are called **MDS**. A standard reference on codes endowed with the Hamming metric is [9].

**Definition 1.** *An $[n \times m, k]_q$ **matrix rank-metric** code is an $\mathbb{F}_q$-linear subspace $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$. If $k \geq 1$, then the **minimum rank distance** of $\mathcal{C}$ is*

$$d_{\mathrm{rk}}(\mathcal{C}) := \min\{\mathrm{rk}(X) \mid X \in \mathcal{C},\ X \neq 0\}.$$

In [4], Delsarte shows the rank-metric analogue of the Singleton bound.

**Theorem 1 (**[4, Theorem 5.4]**).** *Let $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ be a non-zero $[n \times m, k]_q$ rank-metric code. We have $k \leq m(n - d_{\mathrm{rk}}(\mathcal{C}) + 1)$.*

Codes meeting the bound of Theorem 1 are called **MRD**. They enjoy a series of properties that are analogous to those of MDS codes. For example, their weight distribution is determined by their dimension [4, Theorem 5.5]. See [12, Remark 50] for a generalization.

In [5] and [14], Gabidulin and Roth introduce independently a special class of rank-metric codes, that are linear over $\mathbb{F}_{q^m}$. They are defined as follows.

**Definition 2.** *An $[n,k]_{q^m}$ **vector rank-metric** code is an $\mathbb{F}_{q^m}$-linear subspace $C \leq \mathbb{F}_{q^m}^n$. If $k \geq 1$, then the **minimum (rank) distance** of $C$ is*

$$d_{\mathrm{rk}}(C) := \min\{\mathrm{rk}(x) \mid x \in C,\ x \neq 0\},$$

*where $\mathrm{rk}(x)$ denotes the $\mathbb{F}_q$-dimension of the space generated by the entries of $x$.*

There is a simple relation between vector and matrix rank-metric codes, which we briefly describe. Given an $\mathbb{F}_q$-basis $\Gamma = \{\gamma_1, ..., \gamma_m\}$ of $\mathbb{F}_{q^m}$ and a vector $x \in \mathbb{F}_{q^m}^n$, denote by $\Gamma(x)$ the $n \times m$ matrix over $\mathbb{F}_q$ defined by

$$x_i = \sum_{j=1}^{m} \Gamma_{ij}(x)\gamma_j \quad \text{for all } 1 \leq i \leq n.$$

Then the following hold (see e.g. [7, Section 1]).

**Proposition 1.** *For every $\mathbb{F}_q$-basis $\Gamma$ of $\mathbb{F}_{q^m}$, the map $x \mapsto \Gamma(x)$ is $\mathbb{F}_q$-linear and bijective. Moreover, it preserves the (respective) rank weights. In particular, if $C \leq \mathbb{F}_{q^m}^n$ is an $[n,k]_{q^m}$ vector rank metric code, then $\Gamma(C)$ is matrix rank metric code of dimension $mk$ over $\mathbb{F}_q$ with the same minimum distance as $\mathcal{C}$.*

An $[n,k]_{q^m}$ vector rank-metric code $C$ is **MRD** if $\Gamma(C)$ is MRD for some (and therefore for all) basis $\Gamma$ of $\mathbb{F}_{q^m}/\mathbb{F}_q$. Equivalently, $C$ is MRD if $k = n - d_{\mathrm{rk}}(C) + 1$.

While MDS codes, vector MRD codes, and matrix MRD codes often exhibit a similar behaviour, in this paper we show that they behave very differently with respect to density properties.

## 3 Density Questions in Coding Theory

It is natural to ask what the proportion of MDS and MRD code is within the family of codes having the same dimension. This is the question that we address in the remainder of the paper.

We start by defining *density functions* and what it means for a family to be *sparse* or *dense* within a larger family. Such notions have been used for decades in number theory; see e.g. [11].

**Definition 3.** *Let $S \subseteq \mathbb{N}$ be an infinite subset. Let $(\mathcal{F}_s \mid s \in S)$ be a sequence of finite non-empty sets indexed by $S$, and let $(\mathcal{F}'_s \mid s \in S)$ be a sequence of sets with $\mathcal{F}'_s \subseteq \mathcal{F}_s$ for all $s \in S$. The **density function** $S \to \mathbb{Q}$ of $\mathcal{F}'_s$ in $\mathcal{F}_s$ is*

$$s \mapsto |\mathcal{F}'_s|/|\mathcal{F}_s|.$$

*When $\lim_{s\to+\infty} |\mathcal{F}'_s|/|\mathcal{F}_s|$ exists and equals $\delta$, then we say that $\mathcal{F}'_s$ has **density** $\delta$ in $\mathcal{F}_s$. If $\mathcal{F}'_s$ has density $0$ in $\mathcal{F}_s$, then $\mathcal{F}'_s$ is **sparse** in $\mathcal{F}_s$. If $\mathcal{F}'_s$ has density $1$ in $\mathcal{F}_s$, then $\mathcal{F}'_s$ is **dense** in $\mathcal{F}_s$.*

A typical problem is to study the asymptotics of the density functions of sequences of sets (see e.g. [8]). We illustrate this with a very simple example.

*Example 1.* Let $S = \mathbb{N}$. For all $s \in S$ define the sets $\mathcal{F}_s := \{n \in \mathbb{N} \mid n \leq s\}$ and $\mathcal{F}'_s := \{n \in \mathbb{N} \mid n \leq s \text{ and } n \text{ is even}\}$. Then $1/2 \leq |\mathcal{F}'_s|/|\mathcal{F}_s| \leq 1/2 + 1/s$ for all $s \in S$, as it can be easily checked. Thus $\mathcal{F}'_s$ has density $1/2$ in $\mathcal{F}_s$, as one expects.

To simplify the notation, the variable $s$ in $\mathcal{F}_s$ and $\mathcal{F}'_s$ is omitted when it is clear from the context. Notions of lower density (the $\lim_{s\to+\infty}\inf$) and upper density (the $\lim_{s\to+\infty}\sup$) are also used and appear in the literature, but are not required here.

MDS codes are dense for $q \to +\infty$. This result is classically known, although we cannot provide a precise reference. More precisely, the following hold.

**Theorem 2.** *For all $1 \leq k \leq n$, there are at least*

$$q^{k(n-k)}\left(1-\frac{k}{q}\left(\binom{n}{k}-1\right)\right)$$

*$k$-dimensional MDS codes in $\mathbb{F}_q^n$. In particular, MDS codes are dense in the set of $k$-dimensional codes as $q \to +\infty$.*

*Proof.* For a matrix $G$ over $\mathbb{F}_q$, we let $\mathrm{piv}(G)$ denote the pivot indices in the reduced row-echelon form of $G$. Now suppose that $G \in \mathbb{F}_q^{k\times n}$ is a rank $k$ matrix in reduced row-echelon form. Using standard coding theory arguments one shows that the following are equivalent:

1. the rows of $G$ generate a $k$-dimensional MDS code;
2. all the $k \times k$ minors of $G$ are non-zero (in particular, $\mathrm{piv}(G) = \{1, ..., k\}$).

Consider a matrix of the form $G = (I_k \mid Y)$, where $Y$ is a $k \times (n-k)$ matrix of $\mathbb{F}_q$-independent variables $(z_i \mid 1 \leq i \leq N)$ and $N = k(n-k)$. Let $p_1, ..., p_M$ be the maximal minors of $G$, where $M = \binom{n}{k}$. Then each $p_j$ is a polynomial in the variables $z_1, ..., z_N$ whose degree is upper bounded by $k$. Moreover, since $G$ has an identity in the first $k \times k$ block, $p_1 = 1$ without loss of generality. Therefore the polynomial $p = p_1 p_2 \cdots p_M$ has degree upper bounded by $k(M-1)$. By the first part of the proof, the $k$-dimensional MDS codes in $\mathbb{F}_q^n$ are in bijection with the set $\{\alpha \in \mathbb{F}_q^N \mid p(\alpha) \neq 0\}$. Therefore by the Schwartz-Zippel Lemma [15,18] their number is at least

$$q^N\left(1-q^{-1}k(M-1)\right) = q^{k(n-k)}\left(1-\frac{k}{q}\left(\binom{n}{k}-1\right)\right).$$

The second part of the statement follows from the fact that

$$\lim_{q\to+\infty} q^{k(n-k)}\left(1-\frac{k}{q}\left(\binom{n}{k}-1\right)\right)\begin{bmatrix} n \\ k \end{bmatrix}_q^{-1} = 1,$$

as one can easily check using the well-known estimate

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \sim q^{k(n-k)} \quad \text{as } q \to +\infty.$$

The rank-metric analogue of Theorem 2 holds for vector MRD codes that are linear over $\mathbb{F}_{q^m}$, for $m \to +\infty$. This was shown in [10] with the aid of the Schwartz-Zippel Lemma.

**Theorem 3.** *For all $1 \leq k \leq n \leq m$, there are at least*

$$q^{mk(n-k)}\left(1-\frac{k}{q^m}\prod_{i=0}^{k-1}(q^n-q^i)\right)$$

*$\mathbb{F}_{q^m}$-linear MRD codes in $\mathbb{F}_{q^m}^n$ of dimension $k$ over $\mathbb{F}_{q^m}$. In particular, MRD codes are dense in the set of $k$-dimensional $\mathbb{F}_{q^m}$-linear vector rank-metric codes codes as $m \to +\infty$.*

*Remark 1.* The proof of Theorem 3 uses the fact that $\mathbb{F}_{q^m}$-linear MRD codes correspond to the non-zeroes of a polynomial $p$ in $k(n-k)$ variables with coefficients in $\mathbb{F}_{q^m}$. In the argument of [10], it is crucial that the degree of $p$ satisfies

$$\lim_{m\to+\infty} \deg(p)/q^m = 0, \tag{1}$$

from which the density of $\mathbb{F}_{q^m}$-linear MRD codes as $m \to +\infty$ can be deduced using the Schwartz-Zippel Lemma.

We notice that this proof technique cannot be applied to deduce that $\mathbb{F}_q$-linear matrix MRD codes are dense as $q \to +\infty$. These optimal codes of dimension $m(k-d+1)$ over $\mathbb{F}_q$, where $d$ denotes the minimum distance, can easily be described as the non-zeroes of a multivariate polynomial in $m^2(n-d+1)(d-1)$ variables and coefficients in $\mathbb{F}_q$. However, the degree of any such polynomial, say $p$, does *not* satisfy

$$\lim_{q\to+\infty} \deg(p)/q = 0 \quad \text{or} \quad \lim_{m\to+\infty} \deg(p)/q = 0$$

in general, thereby preventing the application of the Schwartz-Zippel Lemma. In fact, $\mathbb{F}_q$-linear MRD codes are *not* dense in the set of codes with the same $\mathbb{F}_q$-dimension, as we will shortly see. In particular, the behaviour of matrix MRD codes is in sharp contrast with that of vector MRD codes.

## 4 The Density Function of Matrix MRD Codes

In this section we obtain a lower bound for the number of $\mathbb{F}_q$-linear non-MRD codes in $\mathbb{F}_q^{n\times m}$ of a given dimension $k$. This result will be applied in Section 5 to deduce that matrix MRD codes are not dense within the set of codes having the same dimension over $\mathbb{F}_q$.

**Theorem 4.** *Let $k$ be a multiple of $m$ with $m \leq k \leq m(n-1)$. The number of $\mathbb{F}_q$-linear $k$-dimensional non-MRD codes in $\mathbb{F}_q^{n\times m}$ is at least*

$$q \cdot \Lambda_q(mn, mn-k, k) \cdot \left(1-\frac{\left(q^k-1\right)\left(q^{mn-k}-1\right)}{2\left(q^{mn}-q^{mn-k}\right)}\right),$$

*where*

$$\Lambda_q(N,t,r) = \sum_{h=1}^{t} \begin{bmatrix} t \\ h \end{bmatrix}_q \sum_{s=h}^{t} \begin{bmatrix} t-h \\ s-h \end{bmatrix}_q \begin{bmatrix} N-s \\ N-r \end{bmatrix}_q (-1)^{s-h} q^{\binom{s-h}{2}}$$

*for all non-negative integers $N, t, r$ and any prime power $q$.*

The proof of Theorem 4 is long and quite technical. We therefore only give the idea of how it works and organize it in eight steps. We refer to [3, Section 6] for a full proof.

*Proof (sketch).* Define $d = n - k/m + 1$. The main idea behind the proof is to construct $q$ vector spaces of matrices $\mathcal{D}_1, ..., \mathcal{D}_q \leq \mathbb{F}_q^{n\times m}$ that only contain matrices of rank upper bounded by $d-1$, and then derive a lower bound for the number of $k$-dimensional codes $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ that intersect non-trivially at least one of these spaces. Clearly, this gives a lower bound on the number of $k$-dimensional codes $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ that are not MRD.

1. The first step is to show that one can assume $n \geq 2(d-1)$ without loss of generality. To see this, observe that trace-duality in $\mathbb{F}_q^{n\times m}$ gives a bijection between the MRD codes of distance $d$ and dimension $k$ and the MRD codes of distance $n-d+2$ and dimension $mn-k$. See e.g. [13, Section 4]. Moreover, if $n < 2(d-1)$, then $n > 2((n-d+2)-1)$ and $2 \leq n-d+2 \leq n$. We henceforth assume $n \geq 2(d-1)$ in the sequel.
2. Using results on *partial spreads* [2] and step 1, one shows that there exist $\mathbb{F}_q$-linear spaces $U_1, ..., U_q \leq \mathbb{F}_q^n$ of dimension $d-1$ with the property that $U_i \cap U_j = \{0\}$ for all $i, j \in \{1, ..., q\}$ with $i \neq j$. Then one defines

$$\mathcal{D}_i = \{X \in \mathbb{F}_q^{n\times m} \mid \text{columnspace}(X) \leq U_i\} \leq \mathbb{F}_q^{n\times m} \quad \text{for all } 1 \leq i \leq q,$$

and observes that $\mathcal{D}_i \cap \mathcal{D}_j = \{0\}$ for all $i, j \in \{1, ..., q\}$ with $i \neq j$. Moreover, each $\mathcal{D}_i$ only contains matrices of rank $\leq d-1$. Finally, the dimension of each $\mathcal{D}_i$ over $\mathbb{F}_q$ is $m(d-1)$ by [13, Lemma 26]. It remains to show that there are at least

$$q \cdot \Lambda_q(mn, mn-k, k) \cdot \left(1 - \frac{\left(q^k-1\right)\left(q^{mn-k}-1\right)}{2\left(q^{mn}-q^{mn-k}\right)}\right)$$

$k$-dimensional codes $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ that intersect non-trivially at least one space among $\mathcal{D}_1, ..., \mathcal{D}_q$. This is done in various steps and using the following auxiliary objects:

$$\begin{aligned}
&\mathcal{F}_i = \{\mathcal{C} \leq \mathbb{F}_q^{n\times m} \mid \dim(\mathcal{C}) = k,\ \mathcal{C} \cap \mathcal{D}_i \neq \{0\}\} \quad \text{for } 1 \leq i \leq q,\\
&A_1 = \emptyset,\\
&A_i = \bigcup_{1\leq j<i} \mathcal{D}_j \setminus \{0\} \quad \text{for } 2 \leq i \leq q,\\
&\overline{\mathcal{F}}_i = \{\mathcal{C} \in \mathcal{F} \mid \mathcal{C} \cap \mathcal{D}_i \neq \{0\} \text{ and } \mathcal{C} \cap A_i = \emptyset\} \subseteq \mathcal{F}_i \quad \text{for } 1 \leq i \leq q.
\end{aligned}$$

3. It easily follows from the definitions that the number of $k$-dimensional codes $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ that intersect non-trivially at least one space among $\mathcal{D}_1, ..., \mathcal{D}_q$ is at least

$$\sum_{i=1}^{q} |\overline{\mathcal{F}}_i|.$$

We will obtain a lower bound on the cardinality of each $\overline{\mathcal{F}}_i$.

4. Using results on partition-balanced families of codes [3], one shows that

$$|\{\mathcal{C} \in \mathcal{F}_i \mid X \in \mathcal{C}\}| \leq |\mathcal{F}_i| \cdot \frac{q^k - 1}{q^{mn} - q^{m(d-1)}}$$

for all $X \in \mathbb{F}_q^{n \times m}$ with $X \neq 0$ and for all $1 \leq i \leq q$. This in turn can be used to obtain that

$$|\overline{\mathcal{F}}_i| \geq |\mathcal{F}_i| \left(1 - (q-1)^{-1} \frac{q^k - 1}{q^{mn} - q^{m(d-1)}} \cdot |A_i|\right) \quad \text{for all } 1 \leq i \leq q.$$

5. Applying counting arguments based on Mœbius inversion, it can be shown that

$$|\mathcal{F}_i| = \Lambda_q(mn, mn-k, k) \quad \text{for all } 1 \leq i \leq q,$$

where the quantity on the right-hand side is given by the formula in the statement. See [3, Section 3] for details.

6. Combining steps 4 and 5 we see that

$$|\overline{\mathcal{F}}_i| \geq \Lambda_q(mn, mn-k, k) \cdot \left(1 - (q-1)^{-1} \frac{q^k - 1}{q^{mn} - q^{m(d-1)}} \cdot |A_i|\right)$$

for all $1 \leq i \leq q$.

7. We can also explicitly compute the cardinality of each $A_i$ as

$$|A_i| = (i-1)\left(q^{m(d-1)-1}\right), \quad 1 \leq i \leq q.$$

The formulas follow from the fact that the $\mathcal{D}_i$'s are pairwise disjoint (step 2), which heavily relies upon the partial spread property of the $U_i$'s.

8. Combining steps 3, 6 and 7 we finally deduce that the number of $k$-dimensional codes $\mathcal{C} \leq \mathbb{F}_q^{n \times m}$ that intersect non-trivially at least one among $\mathcal{D}_1, ..., \mathcal{D}_q$ is lower bounded by

$$\begin{aligned}
&\sum_{i=1}^{q} \Lambda_q(mn, mn-k, k) \cdot \left(1 - (q-1)^{-1} \frac{q^k - 1}{q^{mn} - q^{mn-k}} \cdot |A_i|\right) \\
&\quad = \Lambda_q(mn, mn-k, k) \cdot \left(q - \frac{\left(q^k - 1\right)\left(q^{mn-k} - 1\right)}{(q-1)\left(q^{mn} - q^{mn-k}\right)} \frac{q(q-1)}{2}\right) \\
&\quad = q \cdot \Lambda_q(mn, mn-k, k) \cdot \left(1 - \frac{\left(q^k - 1\right)\left(q^{mn-k} - 1\right)}{2\left(q^{mn} - q^{mn-k}\right)}\right),
\end{aligned}$$

where the first equality follows from the identity

$$\sum_{i=1}^{q} (i-1) = \frac{q(q-1)}{2}.$$

This yields the desired result by step 2 and concludes the proof.

## 5 Applications

In this section we show that Theorem 4 implies the non-density of MRD matrix codes, both as $q \to +\infty$ and as $m \to +\infty$, and the sparsity of binary MRD codes as $m \to +\infty$. We start by giving a partial proof for the non-density of MRD codes as $q \to +\infty$.

**Corollary 1.** *Let $k$ be a multiple of $m$ with $m \leq k \leq m(n-1)$. Define the families $\mathcal{F}_q := \{\mathcal{C} \leq \mathbb{F}_q^{n\times m} \mid \dim(\mathcal{C}) = k\}$ and $\mathcal{F}'_q := \{\mathcal{C} \in \mathcal{F}_q \mid \mathcal{C} \text{ is not MRD}\}$. Then for every $\varepsilon \in \mathbb{R}_{>0}$ there exists $q_\varepsilon \in \mathbb{N}$ such that*

$$|\mathcal{F}'_q|/|\mathcal{F}_q| \geq \frac{1}{2} - \varepsilon$$

*for all prime powers $q \geq q_\varepsilon$. In particular, $\lim_{q\to\infty} |\mathcal{F}'_q|/|\mathcal{F}_q| \geq 1/2$, provided the limit exists.*

*Proof.* By Theorem 4 we have

$$\frac{|\mathcal{F}'_q|}{|\mathcal{F}_q|} \geq \frac{q \cdot \Lambda_q(mn, mn-k, k)}{|\mathcal{F}_q|} \left(1 - \frac{\left(q^k-1\right)\left(q^{mn-k}-1\right)}{2\left(q^{mn}-q^{mn-k}\right)}\right). \tag{2}$$

It can be shown [3, Section 3] that

$$\Lambda_q(mn, mn-k, k) \sim q^{k(mn-k)-1} \quad \text{as } q \to +\infty,$$

while it is well-known that

$$|\mathcal{F}_q| = \begin{bmatrix} mn \\ k \end{bmatrix}_q \sim \ q^{k(mn-k)} \quad \text{as } q \to +\infty.$$

Therefore

$$\lim_{q\to+\infty} \frac{q \cdot \Lambda_q(mn, mn-k, k)}{|\mathcal{F}_q|} = \lim_{q\to+\infty} \frac{q \cdot q^{k(mn-k)-1}}{q^{k(mn-k)}} = 1.$$

As a consequence,

$$\lim_{q\to+\infty} \frac{q \cdot \Lambda_q(mn, mn-k, k)}{|\mathcal{F}_q|} \cdot \left(1 - \frac{\left(q^k-1\right)\left(q^{mn-k}-1\right)}{2\left(q^{mn}-q^{mn-k}\right)}\right) = \frac{1}{2}. \tag{3}$$

The statement can now be obtained by combining (2) and (3).

MRD matrix codes are not dense also for $m \to +\infty$. The proof of the next corollary is quite technical and therefore we only sketch it here.

**Corollary 2.** *Fix an integer $d$ with $2 \leq d \leq n$, and let $k := m(n-d+1)$. Define $\mathcal{F}_m := \{\mathcal{C} \leq \mathbb{F}_q^{n\times m} \mid \dim(\mathcal{C}) = k\}$ and $\mathcal{F}'_m := \{\mathcal{C} \in \mathcal{F}_m \mid \mathcal{C} \text{ is not MRD}\}$. Then for every $\varepsilon \in \mathbb{R}_{>0}$ there exists $m_\varepsilon \in \mathbb{N}$ such that*

$$|\mathcal{F}'_m|/|\mathcal{F}_m| \geq \frac{1}{2}\left(\frac{q}{q-1} - \frac{1}{(q-1)^2}\right) - \varepsilon$$

*for all integers $m \geq m_\varepsilon$. In particular, $\lim_{m\to\infty} |\mathcal{F}'_m|/|\mathcal{F}_m| \geq 1/2$, provided the limit exists.*

*Proof (sketch).* The idea is to obtain a lower bound for the limit, as $m \to +\infty$, of the ratio

$$\frac{E_m}{|\mathcal{F}_m|}, \quad \text{where } E_m = q \cdot \Lambda_q(mn, mn-k, k) \cdot \left(1 - \frac{\left(q^k-1\right)\left(q^{mn-k}-1\right)}{2\left(q^{mn}-q^{mn-k}\right)}\right)$$

is the expression in Theorem 4. To simplify notation, we let $N = mn$ and $t = N - k = m(d-1)$. The first step is to obtain the following lower bound:

$$\Lambda_q(N,t,k) \geq \begin{bmatrix} t \\ 1 \end{bmatrix}_q \begin{bmatrix} N-1 \\ t \end{bmatrix}_q - \begin{bmatrix} t \\ 1 \end{bmatrix}_q \begin{bmatrix} t-1 \\ 1 \end{bmatrix}_q \begin{bmatrix} N-2 \\ t \end{bmatrix}_q. \tag{4}$$

The above inequality is not immediate; for more details, see the proof of [3, Corollary 6.4]. Using (4) one shows that

$$\frac{q \cdot \Lambda_q(N,t,k)}{|\mathcal{F}_m|} \geq \frac{q(q^t-1)(q^{N-t}-1)}{(q-1)(q^N-1)} - \frac{q(q^t-1)(q^{t-1}-1)(q^{N-t-1}-1)(q^{N-t}-1)}{(q-1)^2(q^N-1)(q^{N-1}-1)}. \tag{5}$$

Denote by $\beta(m)$ the expression on the right-hand side of (5). Then

$$\frac{E_m}{|\mathcal{F}_m|} \geq \beta(m) \cdot \left(1 - \frac{\left(q^k-1\right)\left(q^{mn-k}-1\right)}{2\left(q^{mn}-q^{mn-k}\right)}\right). \tag{6}$$

Now the right-hand side of (6) tends to

$$\frac{1}{2}\left(\frac{q}{q-1} - \frac{1}{(q-1)^2}\right)$$

as $m \to +\infty$, since $k \leq m(n-1)$ by assumption. This yields the desired lower bound on

$$\lim_{m \to +\infty} E_m/|\mathcal{F}_m|.$$

The corollary now follows from the fact that $|\mathcal{F}'_m|/|\mathcal{F}_m| \geq E_m/|\mathcal{F}_m|$ by Theorem 4.

## References


1. J. Antrobus, H. Gluesing-Luerssen. *Maximal Ferrers Diagram Codes: Constructions and Genericity Considerations.* Preprint: `https://arxiv.org/abs/1804.00624`.
2. A. Beutelspacher. *On t-Covers in Finite Projective Spaces.* Journal of Geometry, **12**, 1, pp. 10–16, 1979.
3. E. Byrne, A. Ravagnani, *Partition-Balanced Familes of Codes and Asymptotic Enumeration in Coding Theory.* Preprint: `https://arxiv.org/abs/1805.02049`.
4. P. Delsarte. *Bilinear Forms over a Finite Field with Applications to Coding Theory.* Journal of Combinatorial Theory, Series A, **25**, pp. 226–241, 1978.

5. E. Gabidulin. *Theory of Codes with Maximum Rank Distance*. Problems of Information Transmission, **2**, pp. 1–12, 1985.
6. P. Gaborit, A. Otmani, H. Tal Kalachi, *Polynomial-Time Key Recovery Attack on the Faure–Loidreau Scheme Based on Gabidulin Codes*, Designs Codes and Cryptography, 2017.
7. E. Gorla, A. Ravagnani. *Codes Endowed with the Rank Metric*. In *Network Coding and Subspace Designs*, Eds. M. Greferath, M. Pavčević, A. Vázquez-Castro, N. Silberstein, Springer-Verlag Berlin, 2018.
8. H. Halberstam, K. F. Roth. *Sequences*. Springer-Verlag, 1983.
9. J. F. MacWillams, N. J. A. Sloane. *The Theory of Error Correcting Codes*. North-Holland Mathematical Library, 1977.
10. A. Neri, A. Horlemann-Trautmann, T. Randrianarisoa, J. Rosenthal. *On the Genericity of Maximum Rank Distance and Gabidulin Codes*. Designs, Codes and Cryptography, **86**, 2, pp. 341–363, 2018.
11. I. Niven. *The Asymptotic Density of Sequences*. Bulletin of the American Mathematical Society, **57**, 6, pp. 420–434, 1951.
12. A. Ravagnani, *Duality of Codes Supported on Regular Lattices, with an Application to Enumerative Combinatorics*. Designs, Codes and Cryptography, **86**, No. 9, pp. 2035–2063, 2018.
13. A. Ravagnani. *Rank-Metric Codes and their Duality Theory*. Designs, Codes and Cryptography, **80**, 1, pp. 197–216, 2016.
14. R. M. Roth. *Maximum-Rank Array Codes and their Application to Criss-cross Error Correction*. IEEE Transactions on Information Theory, **37**, 2, pp. 328–336, 1991.
15. J. Schwartz. *Fast Probabilistic Algorithms for Verification of Polynomial Identities*. Journal of the ACM, **27**, pp. 701–717, 1980.
16. D. Silva, F. Kschischang, R. Kötter. *A Rank-Metric Approach to Error Control in Random Network Coding*. IEEE Transactions on Information theory, **54**, 9, pp. 3951–3967, 2008.
17. R. C. Singleton. *Maximum distance q-nary codes*. IEEE Transactions on Information Theory, **10**, 2, pp. 116 –118, 1964.
18. R. Zippel. *Probabilistic Algorithms for Sparse Polynomials*. Symbolic and Algebraic Computation, Lecture Notes in Computer Science, **72**, pp. 216–226, 1979.