Common Complements of Linear Subspaces and the Sparseness of MRD Codes

SIAM J. APPL. ALGEBRA GEOMETRY
Vol. 6, No. 2, pp. 79–110

Common Complements of Linear Subspaces and the Sparseness of MRD Codes*

Anina Gruica† and Alberto Ravagnani†

Abstract. Motivated by applications to the theory of rank-metric codes, we study the problem of estimating the number of common complements of a family of subspaces over a finite field in terms of the cardinality of the family and its intersection structure. We derive upper and lower bounds for this number, along with their asymptotic versions as the field size tends to infinity. We then use these bounds to describe the general behavior of common complements with respect to sparseness and density, showing that the decisive property is whether or not the number of spaces to be complemented is negligible with respect to the field size. By specializing our results to matrix spaces, we obtain upper and lower bounds for the number of maximum-rank-distance (MRD) codes in the rank metric. In particular, we answer an open question in coding theory, proving that MRD codes are sparse for all parameter sets as the field size grows, with only very few exceptions. We also investigate the density of MRD codes as their number of columns tends to infinity, obtaining a new asymptotic bound. Using properties of the Euler function from number theory, we then show that our bound improves on known results for most parameter sets. We conclude the paper by establishing general structural properties of the density function of rank-metric codes.

Key words. rank-metric code, MRD code, density

AMS subject classifications. 11T71, 05A16

DOI. 10.1137/21M1428947

A *rank-metric code* is a linear space of matrices over a finite field $\mathbb{F}_q$ in which every nonzero matrix has rank bounded from below by an integer d (called the *minimum distance* of the code). Originally introduced by Delsarte for combinatorial interest [10], in the last few decades rank-metric codes have been extensively studied in connection with various applications in information technology [12, 16, 22, 25] and several areas of pure and applied mathematics, including combinatorial designs, rook theory, semifields, polymatroids, and linear sets; see [5, 8, 10, 14, 18, 23, 24] among many others.

An open question in coding theory asks one to compute the asymptotic density of rank-metric codes having maximum dimension, also known as *maximum-rank-distance* (MRD) *codes*; see for example [1, 6]. In more detail, one fixes a value for the minimum distance and attempts to compute the asymptotics, as $q \to +\infty$, of the proportion of MRD codes having that distance within the set of codes sharing the same dimension. To date, three independent approaches have been developed in the attempt to solve this problem, based on

*Received by the editors June 23, 2021; accepted for publication (in revised form) October 26, 2021; published electronically April 11, 2022.
https://doi.org/10.1137/21M1428947
Funding: The authors were partially supported by the Dutch Research Council through grant OCENW.KLEIN.539.
†Department of Mathematics and Computer Science, Eindhoven University of Technology, 5612 AZ, The Netherlands (anina.gruica@gmail.com, a.ravagnani@tue.nl).

enumerative combinatorics, the theory of spectrum-free matrices, and semifields; see [1, 6, 13]. All these techniques show that $\mathbb{F}_q$-linear MRD codes are not dense within the set of codes having a certain dimension. This is in sharp contrast with the behavior of maximum distance separable (MDS) codes in the Hamming metric and of $\mathbb{F}_{q^m}$-linear MRD codes, which are natural analogues of $\mathbb{F}_q$-linear MRD codes and are instead dense as the field size tends to infinity [6, 20].

In this paper, we reinterpret the above question as a broader problem intersecting combinatorial geometry and extremal combinatorics, which is interesting in its own right. More precisely, we study the problem of estimating the number of complements shared by a family of subspaces of $\mathbb{F}_q^N$, say $\mathscr{A}$, all of which have the same codimension k. The bounds that we derive take into account the *intersection structure* of the spaces in $\mathscr{A}$ (i.e., how many subspace pairs intersect in a given dimension), as well as the cardinality of $\mathscr{A}$. The question of estimating the density of MRD codes turns out to be a very special instance of this general problem.

Our strategy to obtain upper and lower bounds for the number of common complements of the spaces in $\mathscr{A}$ relies on the rigidity of certain graphs constructed from a linear lattice. We introduce a simple notion of regularity of a bipartite graph with respect to a function defined on its left-vertices, which we call an *association*. This extends the concept of *left-regularity* and defines a set of numerical parameters of the underlying graph. We then describe the aforementioned complements as the isolated right-vertices of such a regular bipartite graph, estimating their number in terms of the fundamental graph's parameters. In turn, these parameters can be computed using classical methods from the theory of *critical problems* in combinatorial geometry.

Of particular interest for us are the asymptotic versions of these bounds which, under certain assumptions, lead to the following general behavior of the common complements with respect to sparseness/density. If the cardinality of $\mathscr{A}$ is negligible with respect to the field size q, then almost all k-subspaces of $\mathbb{F}_q^N$ are common complements of the spaces in $\mathscr{A}$; moreover, the proportion of noncommon complements is on $O(|\mathscr{A}|/q)$ as $q \to +\infty$. Vice versa, if the cardinality of $\mathscr{A}$ is preponderant with respect to the field size q, then the common complements are sparse (precise asymptotic estimates will be given). In our asymptotic analysis, we find particularly useful the notion of an *asymptotic partial spread*, which we propose as the asymptotic analogue of the classical and homonymous definition from discrete geometry.

In the second part of the paper we turn to the theory of rank-metric codes, specializing our results to matrix spaces over $\mathbb{F}_q$. Our main result is an upper bound on the number of MRD codes with given parameters; see Theorem 5.7. We also prove that the density of $n \times m$ MRD codes of minimum distance d is on

$$O\left(q^{-(d-1)(n-d+1)+1}\right) \quad \text{as } q \to +\infty;$$

see Theorem 5.9 for a precise statement. This shows that MRD codes are very sparse, unless $d = 1$ or $n = d = 2$, answering the question stated at the beginning of this introduction.

The third part of the paper concentrates on the asymptotic density of $n \times m$ MRD codes as $m \to +\infty$. We apply the graph theory machinery described above and obtain an upper bound on the limit superior of the density of these codes. Our estimates involve the *Euler* *function* ϕ from the theory of q-series. In fact, with the aid of Euler's pentagonal number theorem we show that our asymptotic bounds improve on known results for most parameter sets. The question of determining whether or not MRD codes are sparse for m large remains open.

In the last section of the paper we investigate some general properties of density functions in the rank metric, without restricting to MRD codes necessarily. This also gives us the chance to reinterpret known results from a new perspective.

Outline. The remainder of the paper is organized as follows. In section 1 we illustrate the problems we study and introduce the relevant terminology. Section 2 contains preliminary formulas on linear spaces and tuples of functionals, which we will need repeatedly throughout the paper. In section 3 we present our main results, deriving upper and lower bounds for the number of common complements of a family of subspaces using a graph theory approach. The asymptotic versions of these bounds are obtained in section 4. We study the density function of MRD codes (and sometimes of more general rank-metric codes) for $q \to +\infty$ and $m \to +\infty$ in sections 5 and 6, respectively. Finally, structural properties of the density functions of rank-metric codes are established in section 7.

1. Problem formulation.

In this section we recall some concepts from combinatorial geometry and state the main problems studied throughout the paper, illustrating their connection with the theory of rank-metric codes. In the following, q denotes a prime power and $\mathbb{F}_q$ is the finite field of q elements. We let

$$\mathrm{bin}_q(a,b) = \prod_{i=0}^{b-1} \frac{q^a - q^i}{q^b - q^i}$$

be the q-binomial coefficient of integers $a \geq b \geq 0$; see, e.g., [27]. It is well known that $\mathrm{bin}_q(a,b)$ counts the number of b-subspaces of an a-space over $\mathbb{F}_q$.

Definition 1.1. *Let X be a vector space over $\mathbb{F}_q$ and let $W \leq X$ be a subspace. A* complement *of W in X is a subspace $W' \leq X$ with $W \oplus W' = X$, i.e., a complement of W in the lattice of subspaces of X (we denote by "$\leq$" the inclusion relation of linear spaces).*

This paper focuses on the problem of estimating the number of complements shared by a collection of subspaces. A strong motivation to study this problem comes from the theory of rank-metric codes, as we will explain shortly.

Problem 1.2. *Let X be a vector space of finite dimension $N \geq 3$ over $\mathbb{F}_q$ and let $1 \leq k \leq N-1$ be an integer. Let $\mathscr{A}$ be a nonempty collection of subspaces of X, all of which have codimension k. Give upper and lower bounds for the number of common complements in X of the spaces in $\mathscr{A}$.*

When studying Problem 1.2, we take into account structural properties of the set $\mathscr{A}$ of combinatorial flavor, as we will explain later. In this paper we also investigate the asymptotic version of Problem 1.2 as the field size tends to infinity, which can be stated as follows.

Problem 1.3. *Let Q be the set of prime powers and let $(X_q)_{q \in Q}$ be a sequence of vector spaces, all of which have the same dimension $N \geq 3$ over $\mathbb{F}_q$. Let $1 \leq k \leq N-1$ be an integer and let $(\mathscr{A}_q)_{q \in Q}$ be a sequence of nonempty collections of linear spaces, all of which* *have codimension* k*, with* $A_q \le X_q$ *for all* $q \in Q$ *and all* $A_q \in \mathscr{A}_q$*. Determine the asymptotic behavior as* $q \to +\infty$ *of the ratio* $|\mathscr{F}_q|/\mathrm{bin}_q(N,k)$*, where* $\mathscr{F}_q$ *is the collection of* k*-subspaces* $W_q \le X_q$ *that intersect some space in* $\mathscr{A}_q$ *nontrivially.*

In the notation of Problem 1.3, we say that the family of subspaces $(\mathscr{F}_q)_{q\in Q}$ is *sparse* if $\lim_{q\to+\infty} |\mathscr{F}_q|/\mathrm{bin}_q(N,k) = 0$ and *dense* if $\lim_{q\to+\infty} |\mathscr{F}_q|/\mathrm{bin}_q(N,k) = 1$.

The asymptotic version of Problem 1.2, which we will study in section 4, is closely connected to an open question in coding theory on the density of MRD codes. We now briefly review some concepts from coding theory and explain this connection more in detail.

In the following, m and n denote integers with $m \ge n \ge 2$ and $\mathbb{F}_q^{n\times m}$ is the space of $n \times m$ matrices with entries in $\mathbb{F}_q$.

Definition 1.4. *A* (linear rank-metric) code *is a nonzero* $\mathbb{F}_q$*-linear subspace* $\mathscr{C} \le \mathbb{F}_q^{n\times m}$*. Its minimum distance is the integer*

$$d(\mathscr{C}) := \min\{\mathrm{rk}(M) \mid M \in \mathscr{C},\ M \ne 0\}.$$

A rank-metric code cannot have large dimension and minimum distance simultaneously. The trade-off between these quantities is captured by the following result of Delsarte.

Theorem 1.5 (singleton-like bound; see [10]). *Let* $\mathscr{C} \le \mathbb{F}_q^{n\times m}$ *be a nonzero rank-metric code. We have*

$$\dim(\mathscr{C}) \le m(n - d(\mathscr{C}) + 1).$$

The most studied rank-metric codes are those having the maximum possible dimension allowed by their minimum distance.

Definition 1.6. *A code* $\mathscr{C} \le \mathbb{F}_q^{n\times m}$ *is called* MRD *if it attains the bound of Theorem 1.5 with equality.*

The coding theory problem we are interested in asks one to compute the asymptotics, as the field size tends to infinity, of the proportion of MRD codes among all codes with a given dimension. More formally (and more generally), we propose the following terminology.

Definition 1.7. *For* $1 \le k \le mn$ *and* $1 \le d \le n$*, let*

$$\delta_q(n\times m, k, d) := \frac{|\{\mathscr{C} \le \mathbb{F}_q^{n\times m} \mid \dim(\mathscr{C}) = k,\ d(\mathscr{C}) \ge d\}|}{\mathrm{bin}_q(mn,k)}$$

denote the density (function) *of rank-metric codes with minimum distance at least* d *among all* k*-dimensional codes. Their* symptotic density *is instead* $\lim_{q\to+\infty} \delta_q(n\times m, k, d)$*, when the limit exists.*

The following is currently an open question in coding theory.

Problem 1.8. *Compute* $\lim_{q\to+\infty} \delta_q(n\times m, m(n-d+1), d)$ *for all* $1 \le d \le n$*, when it exists.*

We are also interested in determining the asymptotic density of MRD codes as their number of columns tends to infinity, which is another open problem.

Problem 1.9. *Compute* $\lim_{m\to+\infty}\delta_q(n\times m, m(n-d+1), d)$ *for all* $1 \le d \le n$*, when it exists.*

In this paper, we regard the above two problems as special instances of Problem 1.3. This allows us to solve Problem 1.8 and to make progress on Problem 1.9 in sections 5 and 6, respectively. In those sections, we will also survey the literature centered around these problems and briefly describe the three approaches that have been explored so far to solve them.

In the following remark we describe in more detail the connection between Problems 1.2, 1.8, and 1.9. This will be needed in later sections.

Remark 1.10. Consider the collection $\mathscr{U}$ of subspaces $U \le \mathbb{F}_q^n$ having $\dim(U) = d-1$. For any $U \in \mathscr{U}$, denote by $\mathbb{F}_q^{n\times m}(U)$ the set of all matrices whose column-space is contained in U. It is easy to see that $\mathbb{F}_q^{n\times m}(U)$ is a linear space of dimension $m(d-1)$ and that every element of $\mathbb{F}_q^{n\times m}(U)$ has rank smaller or equal to $d-1$ for all $U \in \mathscr{U}$. Finally, let $\mathscr{A} = \{\mathbb{F}_q^{n\times m}(U) \mid U \in \mathscr{U}\}$. By definition, the common complements of the spaces in $\mathscr{A}$ are the rank-metric codes $\mathscr{C} \le \mathbb{F}_q^{n\times m}$ that do not contain any matrix of rank smaller equal to $d-1$ and with dimension $\dim(\mathscr{C}) = mn - m(d-1) = m(n-d+1)$. This means that the common complements of the spaces in $\mathscr{A}$ are exactly the MRD codes of minimum distance d in $\mathbb{F}_q^{n\times m}$. This interpretation of MRD codes as common complements of linear spaces will be crucial in our approach.

We conclude this section by stating a fifth problem considered in this paper. Although our main focus is not on this question, its solution will facilitate the study of Problem 1.3. We need the following terminology.

Definition 1.11. *Let* X *be a vector space over* $\mathbb{F}_q$*. A* cone *in* X *is a nonempty subset* $K \subseteq X$ *with* $\lambda v \in K$ *for all* $v \in K$ *and* $\lambda \in \mathbb{F}_q$*.*

Let $S \subseteq X$ *be a set with* $0 \in S$*. We say that a subspace* $W \le X$ distinguishes S *if* $W \cap S = \{0\}$*. If this is not the case, then we say that* W intersects S *and write* $W \triangleright S$*.*

Problem 1.12. *Let* X *be a vector space of finite dimension* $N \ge 3$ *over* $\mathbb{F}_q$ *and let* $K \subseteq X$ *be a cone. For* $1 \le k \le N$*, give upper and lower bounds for the number of* k*-spaces* $W \le X$ *that distinguish* K*.*

In the notation of Problem 1.12, the task of computing the *exact* number of k-spaces W distinguishing K is known to be difficult in general. This is the celebrated critical problem for combinatorial geometries, proposed by Crapo and Rota in [7, Chapter 16]. Its solution heavily depends on the combinatorics of the cone K, in a precise lattice theory sense; see [11, 17, 21, 29]. There is also a very nice connection between Problem 1.12 and *Sperner theory*, which indirectly provides a partial solution for it. We will comment on this in Remark 3.9.

Remark 1.13. Since the union of linear subspaces is clearly a cone, at a first glance Problem 1.12 might be seen as a special instance of Problem 1.2. Our approach to the latter problem however takes into account information that gets lost when replacing a collection of subspaces with their union. More precisely, the bounds that we will derive take into account the cardinality of $\mathscr{A}$ (in the notation of Problem 1.2) as well as their intersection structure, i.e., the number of subspace pairs intersecting in a given dimension. Both these pieces of information are lost when replacing $\mathscr{A}$ with $\bigcup \mathscr{A}$. For this reason, in this paper Problems 1.2 and 1.12 are treated as very different questions. We will return to this discussion in Remark 3.10 and Example 3.11.

2. Counting linear spaces and functionals. The goal of this section is to provide a combinatorial interpretation for the following expression, which will be used repeatedly throughout the paper to derive bounds and their asymptotic versions.

Notation 2.1. For a prime power q and nonnegative integers N, k, and ℓ with $N \geq 3$, $k < N$, and $N - 2k \leq \ell \leq N - k$, let

$$\nu_q(N,k,\ell) := \mathrm{bin}_q(N,k) - 2q^{k(N-k)} + q^{(2k-N+\ell)(N-k)} \prod_{i=\ell}^{N-k-1} (q^{N-k} - q^i), \tag{2.1}$$

where throughout this paper a product over an empty index set is 1 by convention.

We will show that $\nu_q(N,k,\ell)$ counts the number of k-subspaces of an N-space over $\mathbb{F}_q$ having a particular property. More precisely, the following holds.

Theorem 2.2. *Let N, k, and ℓ be as in Notation 2.1. Let X be an N-space over $\mathbb{F}_q$ and let $A, A', B, B' \leq X$ be $(N-k)$-subspaces with $\ell = \dim(A \cap B) = \dim(A' \cap B')$. We have*

$$|\{W \leq X \mid \dim(W) = k,\, W \triangleright A,\, W \triangleright B\}| = |\{W \leq X \mid \dim(W) = k,\, W \triangleright A',\, W \triangleright B'\}|.$$

In words, the number of k-spaces $W \leq X$ intersecting $(N-k)$-spaces $A, B \leq X$ only depends on $\ell = \dim(A \cap B)$. Moreover, this number is precisely $\nu_q(N,k,\ell)$.

Theorem 2.2 will be established after a series of preliminary results on linear functionals, which are natural objects in the theory of critical problems [7, 17]. While there are more direct approaches to obtain a closed formula for the quantity in Theorem 2.2, the expressions we obtained with such approaches are difficult to estimate as $q \to +\infty$ (and we will need these asymptotic estimates in section 4).

To simplify the study of $\nu_q(N,k,\ell)$, throughout this section we fix a prime power q, an integer $N \geq 3$, and a vector space X having dimension N over $\mathbb{F}_q$. The particular choice of X is irrelevant. We start by introducing the following simple concepts.

Definition 2.3.
(1) *A* functional *on X is a linear function $f : X \to \mathbb{F}_q$. The space of functionals on X is denoted by X^*.*
(2) *Let $r \geq 1$ be an integer. The* kernel *of an r-tuple $F = (f_1, \ldots, f_r) \in (X^*)^r$ is the linear space $\ker(F) := \ker(f_1) \cap \cdots \cap \ker(f_r)$.*
(3) *Let $S \subseteq X$ be a set with $0 \in S$ and let $r \geq 1$ be an integer. We say that $F \in (X^*)^r$ distinguishes S if $\ker(F)$ distinguishes S. Similarly, we say that F intersects S if $\ker(F)$ intersects S. In the latter case we write $F \triangleright S$. Finally, we let*

$$\tau_q(r,S) := |\{F \in (X^*)^r \mid F \text{ distinguishes } S\}|.$$

A celebrated theorem by Crapo and Rota [7, Chapter 16] expresses $\tau_q(r,S)$ in terms of the combinatorics of the set S. More precisely, it shows that $\tau_q(r,S)$ is obtained by evaluating the characteristic polynomial of the geometric lattice generated by S at q^s.

Definition 2.4. *Let $S \subseteq X$ be a subset with $0 \in S$. We denote by $\mathscr{L}(S)$ the geometric lattice whose elements are the subspaces of X having a basis made of elements of S, ordered by inclusion. We also let μ_S and $\mathrm{rk}(S)$ denote its Möbius function and rank, respectively (note that $\mathrm{rk}(S)$ is simply the dimension of the space generated by the elements of S). The* characteristic polynomial *of S is*

$$\chi(S,\lambda) := \sum_{W \in \mathscr{L}(S)} \mu_S(W)\, \lambda^{\mathrm{rk}(S)-\dim(W)} \in \mathbb{Z}[\lambda].$$

For some sets S, the characteristic polynomial $\chi(S,\lambda)$ can be explicitly computed, although this is a very difficult task in general.

Example 2.5. For a k-space $A \leq X$ we have $\chi(A,\lambda) = \prod_{i=0}^{k-1}(\lambda - q^i)$. This formula is well known and follows, for example, from [26, section 3].

We can now state the result of Crapo and Rota.

Theorem 2.6 (see [7, Chapter 16]). *Let $S \subseteq X$ be a subset with $0 \in X$ and let $r \geq 1$ be an integer. We have*

$$\tau_q(r,S) = q^{r(N-r)}\, \chi(S, q^r).$$

In particular, for all k-spaces $A \leq X$ we have

$$\tau_q(r,A) = q^{r(N-k)} \prod_{i=0}^{k-1}(q^r - q^i).$$

Counting functionals that distinguish a set of vectors is equivalent to counting spaces that distinguish the same set. For some parameters, the mentioned relation between functionals and spaces is particularly simple, as the next lemma illustrates.

Lemma 2.7. *Let $S \subseteq X$ be a subset with $0 \in S$. Fix any integer k with the property that $k \geq \max\{\dim(W) \mid W \leq X,\, W$ distinguishes $S\}$. The number of k-spaces $W \leq X$ distinguishing S is*

$$\frac{\tau_q(N-k,S)}{\prod_{i=0}^{N-k-1}(q^{N-k} - q^i)}.$$

Proof. Define the sets

$$\mathbf{A} := \{F \in (X^*)^{N-k} \mid F \text{ distinguishes } S\},$$
$$\mathbf{B} := \{W \leq X \mid \dim(W) = k,\ W \text{ distinguishes } S\}.$$

Let $\varphi : \mathbf{A} \to \mathbf{B}$ be the map defined by $\varphi : F \mapsto \ker(F)$ for all $F \in \mathbf{A}$. We claim that φ is well-defined. To see this, note that $\dim(\ker(F)) \geq N - N + k = k$. Since we have $k \geq \max\{\dim(W) \mid W \leq X,\, W \text{ distinguishes } S\}$ by assumption, it must hold that $\dim(\ker(F)) = k$. This shows that φ is indeed well-defined. As a next step, we compute the size of the fiber of an arbitrary $W \in \mathbf{B}$ as follows,

$$|\varphi^{-1}(W)| = |\{F \in (X^*)^{N-k} \mid \ker(F) = W\}| = \prod_{i=0}^{N-k-1}(q^{N-k} - q^i),$$

where the latter equality is not difficult to see and is left to the reader. Therefore

$$\tau_q(N-k,S) = \sum_{W\in\mathbf{B}} |\varphi^{-1}(W)| = |\mathbf{B}| \prod_{i=0}^{N-k-1} (q^{N-k}-q^i),$$

as desired. ∎

The final step towards a combinatorial interpretation for $\nu_q(N,k,\ell)$ is the following formula relating tuples of functionals distinguishing linear spaces. The proof technique combines the aforementioned result by Crapo and Rota (Theorem 2.6 above) with Stanley's modular factorization theorem for geometric lattices [26].

Lemma 2.8. *Let $A,B \leq X$ be subspaces. For all $r \geq 1$ we have*

$$\tau_q(r, A\cup B)\,\tau_q(r, A\cap B) = \tau_q(r,A)\,\tau_q(r,B).$$

Proof. Consider the geometric lattice $\mathscr{L}(A\cup B)$; see Definition 2.4. The rank of $A\cup B$ is $\mathrm{rk}(A\cup B) = \dim(A+B)$. It is easy to see that A is a modular element of $\mathscr{L}(A\cup B)$ and thus we can use Stanley's modular factorization theorem [26, Theorem 2] as follows:

$$\begin{aligned}\chi(A\cup B,\lambda) &= \chi(A,\lambda) \sum_{\substack{W\in\mathscr{L}(A\cup B)\\ W\cap A=\{0\}}} \mu_{A\cup B}(W)\,\lambda^{\mathrm{rk}(A\cup B)-\dim(A)-\dim(W)}\\ &= \chi(A,\lambda) \sum_{\substack{W\in\mathscr{L}(B)\\ W\cap A=\{0\}}} \mu_{B}(W)\,\lambda^{\dim(B)-\dim(A\cap B)-\dim(W)}. \end{aligned} \tag{2.2}$$

We now apply again Stanley's modular factorization theorem to the lattice $\mathscr{L}(B)$ and the modular element $A\cap B$ of $\mathscr{L}(B)$, obtaining

$$\chi(B,\lambda) = \chi(A\cap B,\lambda) \sum_{\substack{W\in\mathscr{L}(B)\\ W\cap A=\{0\}}} \mu_{B}(W)\,\lambda^{\dim(B)-\dim(A\cap B)-\dim(W)}. \tag{2.3}$$

Using (2.2) and (2.3) together we get $\chi(A\cup B,\lambda)\,\chi(A\cap B,\lambda) = \chi(A,\lambda)\,\chi(B,\lambda)$. Finally, the statement of the lemma can easily be derived by combining the latter identity with Theorem 2.6. ∎

We are now ready to establish the main result of this section, providing a combinatorial interpretation for $\nu_q(N,k,\ell)$.

Proof of Theorem 2.2. Fix arbitrary $(N-k)$-spaces $A,B \leq X$ that intersect in dimension ℓ. The largest dimension of a subspace $W \leq X$ that distinguishes $A\cup B$ is at most k. Therefore by Lemma 2.7 we have

$$\begin{aligned}&|\{W \leq X \mid \dim(W)=k,\ W \rhd A \text{ and } W \rhd B\}| = \\ &\mathrm{bin}_q(N,k) - \frac{\tau_q(N-k,A)}{\prod_{i=0}^{N-k-1}(q^{N-k}-q^i)} - \frac{\tau_q(N-k,B)}{\prod_{i=0}^{N-k-1}(q^{N-k}-q^i)} + \frac{\tau_q(N-k,A\cup B)}{\prod_{i=0}^{N-k-1}(q^{N-k}-q^i)}.\end{aligned} \tag{2.4}$$

Using Lemma 2.8 we can rewrite the last term of this expression as

$$\frac{\tau_q(N-k, A\cup B)}{\prod_{i=0}^{N-k-1}(q^{N-k}-q^i)} = \frac{\tau_q(N-k,A)\tau_q(N-k,B)}{\tau_q(N-k, A\cap B)\prod_{i=0}^{N-k-1}(q^{N-k}-q^i)}.$$

Finally, by the second part of Theorem 2.6 we have that

$$|\{W \leq X \mid \dim(W)=k,\ W \rhd A \text{ and } W \rhd B\}| = \\ \mathrm{bin}_q(N,k) - \frac{2q^{k(N-k)}\prod_{i=0}^{N-k-1}(q^{N-k}-q^i)}{\prod_{i=0}^{N-k-1}(q^{N-k}-q^i)} \\ + \frac{q^{2k(N-k)}\prod_{i=0}^{N-k-1}(q^{N-k}-q^i)^2}{q^{(N-\ell)(N-k)}\prod_{i=0}^{\ell-1}(q^{N-k}-q^i)\prod_{i=0}^{N-k-1}(q^{N-k}-q^i)},$$

which simplifies to $\nu_q(N,k,\ell)$. Note moreover that this expression does not depend on the choice of A and B, concluding the proof. ∎

3. Upper and lower bounds.

In this section we present some of the main results of this paper, providing an answer to Problems 1.2 and 1.12. The approach we take is based on the study of isolated vertices in bipartite graphs. Throughout the paper we use the following definition of bipartite graph and isolated vertex.

Definition 3.1. *A* (directed) bipartite graph *is a* 3*-tuple* $\mathscr{B}=(\mathscr{V},\mathscr{W},\mathscr{E})$*, where* $\mathscr{V}$*,* $\mathscr{W}$ *are finite nonempty sets and* $\mathscr{E}\subseteq\mathscr{V}\times\mathscr{W}$*. The elements of* $\mathscr{V}\cup\mathscr{W}$ *are called* vertices*. We say that a vertex* $W\in\mathscr{W}$ *is* isolated *if there is no* $V\in\mathscr{V}$ *with* $(V,W)\in\mathscr{E}$*.*

Finally, a bipartite graph $\mathscr{B}=(\mathscr{V},\mathscr{W},\mathscr{E})$ *is* left-regular *of* degree ∂ *if for all* $V\in\mathscr{V}$ *we have* $\partial=|\{W\in\mathscr{W}\mid (V,W)\in\mathscr{E}\}|$*.*

We start with a very simple upper bound for the number of nonisolated vertices in a left-regular bipartite graph.

Lemma 3.2. *Let* $\mathscr{B}=(\mathscr{V},\mathscr{W},\mathscr{E})$ *be a bipartite and left-regular graph of degree* $\partial>0$*. Let* $\mathscr{F}\subseteq\mathscr{W}$ *be the collection of nonisolated vertices of* $\mathscr{W}$*. We have*

$$|\mathscr{F}|\leq|\mathscr{V}|\,\partial.$$

Proof. We count the elements in the set $\mathbf{A}=\{(V,W)\in\mathscr{E}\mid V\in\mathscr{V},\ W\in\mathscr{F}\}$ in two ways, obtaining

$$|\mathscr{V}|\,\partial=|\mathbf{A}|=\sum_{W\in\mathscr{F}}|\{V\in\mathscr{V}\mid (V,W)\in\mathscr{E}\}|\geq|\mathscr{F}|.$$

The latter inequality follows from the fact, by assumption, no vertex in $\mathscr{F}$ is isolated. ∎

The next step is to derive a lower bound for the number of nonisolated vertices in a bipartite graph. We concentrate on a class of such graphs that exhibit strong regularity properties with respect to certain maps defined on their left-vertices. More precisely, we will use the following concepts.

Definition 3.3. *Let* $\mathscr{V}$ *be a finite nonempty set and let* $r\geq 0$ *be an integer. An association on* $\mathscr{V}$ *of* magnitude r *is a function* $\alpha:\mathscr{V}\times\mathscr{V}\to\{0,\ldots,r\}$ *that satisfies the following:*

(1) $\alpha(V,V) = r$ *for all* $V \in \mathscr{V}$;
(2) $\alpha(V,V') = \alpha(V',V)$ *for all* $V, V' \in \mathscr{V}$.

Definition 3.4. *Let* $\mathscr{B} = (\mathscr{V}, \mathscr{W}, \mathscr{E})$ *be a finite bipartite graph and let* α *be an association on* $\mathscr{V}$ *of magnitude* r. *We say that* $\mathscr{B}$ *is* α***-regular*** *if for all* $(V,V') \in \mathscr{V} \times \mathscr{V}$ *the number of vertices* $W \in \mathscr{W}$ *with* $(V,W) \in \mathscr{E}$ *and* $(V',W) \in \mathscr{E}$ *only depends on* $\alpha(V,V')$. *We denote this number by* $\mathscr{W}_\ell(\alpha)$, *where* $\ell = \alpha(V,V') \in \{0,\ldots,r\}$, *i.e., we have*

$$\mathscr{W}_\ell(\alpha) = |\{W \in \mathscr{W} \mid (V,W) \in \mathscr{E}, (V',W) \in \mathscr{E}\}|$$

for any pair $(V,V') \in \mathscr{V} \times \mathscr{V}$ *such that* $\alpha(V,V') = \ell$.

Note that an α-regular bipartite graph $\mathscr{B}$ as in Definition 3.4 is necessarily left-regular of degree $\partial = \mathscr{W}_r(\alpha)$. The following lemma gives a lower bound for the number of nonisolated vertices.

Lemma 3.5. *Let* $\mathscr{B} = (\mathscr{V}, \mathscr{W}, \mathscr{E})$ *be a finite bipartite* α*-regular graph, where* α *is an association on* $\mathscr{V}$ *of magnitude* r. *Let* $\mathscr{F} \subseteq \mathscr{W}$ *be the collection of nonisolated vertices of* $\mathscr{W}$. *If* $\mathscr{W}_r(\alpha) > 0$, *then*

$$|\mathscr{F}| \geq \frac{\mathscr{W}_r(\alpha)^2\,|\mathscr{V}|^2}{\sum_{\ell=0}^{r} \mathscr{W}_\ell(\alpha)\,|\alpha^{-1}(\ell)|}.$$

Proof. Define the set $\mathbf{A} = \{(V,V',W) \in \mathscr{V}^2 \times \mathscr{W} \mid (V,W) \in \mathscr{E},\ (V',W) \in \mathscr{E}\}$. Since all vertices in $\mathscr{W} \setminus \mathscr{F}$ are isolated, we have

$$\begin{aligned} |\mathscr{F}| \cdot |\mathbf{A}| &= |\mathscr{F}| \sum_{W \in \mathscr{F}} |\{V \in \mathscr{V} \mid (V,W) \in \mathscr{E}\}|^2 \\ &\geq \left(\sum_{W \in \mathscr{F}} |\{V \in \mathscr{V} \mid (V,W) \in \mathscr{E}\}| \right)^2, \end{aligned} \tag{3.1}$$

where the latter bound follows from the Cauchy–Schwarz inequality. As in the proof of Lemma 3.2, we have

$$\sum_{W \in \mathscr{F}} |\{V \in \mathscr{V} \mid (V,W) \in \mathscr{E}\}| = \sum_{V \in \mathscr{V}} |\{W \in \mathscr{W} \mid (V,W) \in \mathscr{E}\}| = \mathscr{W}_r(\alpha)\,|\mathscr{V}|. \tag{3.2}$$

Therefore combining (3.1) with (3.2) we obtain

$$|\mathscr{F}| \cdot |\mathbf{A}| \geq \mathscr{W}_r(\alpha)^2\,|\mathscr{V}|^2. \tag{3.3}$$

Observe moreover that, by the definition of an association,

$$\begin{aligned} |\mathbf{A}| &= \sum_{\ell=0}^{r} \sum_{\substack{(V,V') \in \mathscr{V}^2 \\ \alpha(V,V')=\ell}} |\{W \in \mathscr{W} \mid (V,W) \in \mathscr{E},\ (V',W) \in \mathscr{E}\}| \\ &= \sum_{\ell=0}^{r} \mathscr{W}_\ell(\alpha) \cdot |\{(V,V') \in \mathscr{V}^2 \mid \alpha(V,V') = \ell\}| \\ &= \sum_{\ell=0}^{r} \mathscr{W}_\ell(\alpha)\,|\alpha^{-1}(\ell)|. \end{aligned} \tag{3.4}$$

Since $\mathscr{W}_r(\alpha) > 0$, by (3.3) we have $|\mathbf{A}| \neq 0$. Therefore to conclude the proof it suffices to combine (3.3) with (3.4). ■

We now apply Lemmas 3.2 and 3.5 to derive upper and lower bounds for the number of common complements of a collection of subspaces. This will provide an answer to Problem 1.2, establishing the main result of this section.

Theorem 3.6. *Let X be a vector space of finite dimension $N \geq 3$ over $\mathbb{F}_q$ and let $1 \leq k \leq N-1$ be an integer. Let $\mathscr{A}$ be a nonempty collection of subspaces of X, all of which have codimension k. Let $\mathscr{F}$ be the collection of k-spaces $W \leq X$ that are not common complements of the spaces in $\mathscr{A}$. We have*

$$\frac{\nu_q(N,k,N-k)^2\,|\mathscr{A}|^2}{\sum_{\ell=0}^{N-k} \nu_q(N,k,\ell)\cdot|\{(A,A') \in \mathscr{A}^2 \mid \dim(A\cap A') = \ell\}|} \leq |\mathscr{F}| \leq |\mathscr{A}|\,\nu_q(N,k,N-k).$$

In particular, if $|\mathscr{A}| \geq 2$ and

$$\ell_{max} := \max\{\dim(A\cap A') \mid A, A' \in \mathscr{A},\ A \neq A'\},$$

then

$$\frac{\nu_q(N,k,N-k)^2\,|\mathscr{A}|}{\nu_q(N,k,N-k) + (|\mathscr{A}|-1)\,\nu_q(N,k,\ell_{max})} \leq |\mathscr{F}| \leq |\mathscr{A}|\,\nu_q(N,k,N-k).$$

Proof. We apply Lemmas 3.2 and 3.5 to the bipartite graph $\mathscr{B} = (\mathscr{A}, \mathscr{W}, \mathscr{E})$, where $\mathscr{W}$ is the collection of k-subspaces of X and $(A,W) \in \mathscr{E}$ if W intersects A. We define an association α of magnitude $N-k$ on $\mathscr{A}$ by setting $\alpha(A,A') := \dim(A \cap A')$ for all $A,\ A' \in \mathscr{A}$. By Theorem 2.2, the graph $\mathscr{B}$ is α-regular with $\mathscr{W}_\ell(\alpha) = \nu_q(N,k,\ell)$ for all $\ell \in \{0,\dots,N-k\}$. Note that $\mathscr{W}_{N-k}(\alpha) = \nu_q(N,k,N-k) > 0$, since every subspace has a complement. The desired upper and lower bounds on $|\mathscr{F}|$ now follow directly from Lemmas 3.2 and 3.5.

To prove the last part of the statement, observe that the map $\ell \mapsto \nu_q(N,k,\ell)$ is increasing in ℓ. This can be seen, for example, from (A.1) in the appendix. Therefore

$$\begin{aligned}\sum_{\ell=0}^{N-k} \nu_q(N,k,\ell)\,|\alpha^{-1}(\ell)| &\leq \sum_{\ell=0}^{N-k-1} \nu_q(N,k,\ell_{\max})\,|\alpha^{-1}(\ell)| + |\mathscr{A}|\,\nu_q(N,k,N-k)\\ &= \nu_q(N,k,\ell_{\max}) \sum_{\ell=0}^{N-k-1} |\alpha^{-1}(\ell)| + |\mathscr{A}|\,\nu_q(N,k,N-k)\\ &= \nu_q(N,k,\ell_{\max})\,|\mathscr{A}|\,(|\mathscr{A}|-1) + |\mathscr{A}|\,\nu_q(N,k,N-k).\end{aligned}$$

Combining this with Lemma 3.5 we obtain

$$|\mathscr{F}| \geq \frac{\nu_q(N,k,N-k)^2\,|\mathscr{A}|^2}{|\mathscr{A}|\,\nu_q(N,k,N-k) + |\mathscr{A}|\,(|\mathscr{A}|-1)\,\nu_q(N,k,\ell_{\max})},$$

which is the lower bound in the second part of the statement. ■

Note that the lower bound on $|\mathscr{F}|$ in Theorem 3.6 takes into account the number of spaces to be complemented, but also their "intersection structure." More precisely, it takes into account how many subspace pairs intersect in a given dimension. The latter information will be crucial when deriving upper bounds on the density function of MRD codes in section 5; see in particular Theorem 5.7.

Remark 3.7. A lower bound for the number of common complements of a collection of subspaces was obtained in [28, Theorem 5]. Following the notation and the assumptions of Theorem 3.6, the result of [28] states that if $|\mathscr{A}| \leq q$, then the number of common complements of the spaces in $\mathscr{A}$ is at least $q+1-|\mathscr{A}|$. For $|\mathscr{A}| = q$, the lower bound of [28] is 1, whereas the bound given in Theorem 3.6 is negative. Therefore, for this particular case, the result of [28] is sharper. For $|\mathscr{A}| < q$ and sufficiently large q, it is possible to check that the bound following from Theorem 3.6 is at least as good as the one in [28].

We conclude this section with an upper and lower bound for the number of spaces of a given dimension that distinguish a given cone. This provides an answer to Problem 1.12.

Theorem 3.8. *Let X be a vector space of finite dimension $N \geq 3$ over $\mathbb{F}_q$ and let $K \subseteq X$ be a cone with $|K| \geq q$. Let $1 \leq k \leq N-1$ be an integer. Denote by $\mathscr{F}$ the collection of k-subspaces $W \leq X$ that intersect K. We have*

$$\frac{\frac{|K|-1}{q-1}\operatorname{bin}_q(N-1,k-1)}{1+\left(\frac{|K|-1}{q-1}-1\right)\left(\frac{q^{k-1}-1}{q^{N-1}-1}\right)} \leq |\mathscr{F}| \leq \frac{|K|-1}{q-1}\operatorname{bin}_q(N-1,k-1).$$

Proof. This time we apply Lemmas 3.2 and 3.5 to the bipartite graph $\mathscr{B} = (\mathscr{V},\mathscr{W},\mathscr{E})$ defined as follows: $\mathscr{V}$ is the collection of 1-subspaces generated by the nonzero elements of K, $\mathscr{W}$ is the collection of k-subspaces of X, and $(L,W) \in \mathscr{E}$ if $L \leq W$. We further define an association α on $\mathscr{V}$ by setting $\alpha(V,V') := \dim(V \cap V')$ for all V, $V' \in \mathscr{V}$. It is easy to see that α has magnitude 1 and that the graph $\mathscr{B}$ is α-regular. Moreover,

$$\begin{aligned} \mathscr{W}_0 &= \operatorname{bin}_q(N-2,k-2), & \mathscr{W}_1 &= \operatorname{bin}_q(N-1,k-1),\\ |\alpha^{-1}(0)| &= |\mathscr{V}|\,(|\mathscr{V}|-1), & |\alpha^{-1}(1)| &= |\mathscr{V}|. \end{aligned}$$

The upper bound on $|\mathscr{F}|$ is an immediate consequence of Lemma 3.2 and the fact that $\mathscr{B}$ is left-regular of degree $\mathscr{W}_1$, as observed right after Definition 3.4. Furthermore, by applying Lemma 3.5 we get

$$|\mathscr{F}| \geq \frac{|\mathscr{V}|\operatorname{bin}_q(N-1,k-1)^2}{\operatorname{bin}_q(N-1,k-1)+(|\mathscr{V}|-1)\operatorname{bin}_q(N-2,k-2)}.$$

The lower bound in the statement can easily be obtained from this inequality using the fact that $|\mathscr{V}| = (|K|-1)/(q-1)$, along with the definition of the q-binomial coefficient and some straightforward computations. ∎

Remark 3.9. While drafting this paper, we found that the lower bound on $|\mathscr{F}|$ in Theorem 3.8 can also be derived from a known result in Sperner theory. More precisely, lengthy computations show that the lower bound of Theorem 3.8 coincides with that of [4, Lemma 12] for $\ell = 1$ (and the same value of k). This result is used in [4] towards the derivation of a *polynomial LYM inequality* for the linear lattice and is more general than our Theorem 3.8. Although both proofs partially rely on the Cauchy–Schwarz inequality, our argument has a more "enumerative" flavor thanks to the concept of an association. This allows us to avoid the eigenvalue machinery in the proof of [4]. In this paper, the best bounds are obtained by applying Theorem 3.6 (rather than Theorem 3.8), which is instead not related to the problems studied in [4].

Remark 3.10. We continue the discussion started in Remark 1.13. Even though the union of linear subspaces is a cone, Theorems 3.6 and 3.8 have different applicability. Theorem 3.6 can be used when information about the intersection structure of the subspaces to be complemented (along with their number) is known, without requiring any particular knowledge about the cardinality of their union. Vice versa, Theorem 3.8 can be used to give an answer to Problem 1.2 when the size of $\bigcup \mathscr{A}$ is known.

The following example illustrates two situations in which the information needed to compute the lower bounds in Theorems 3.6 and 3.8 is completely available, showing that Theorem 3.6 provides a sharper bound in both scenarios. This will be the case also when estimating the density function of MRD codes in sections 5 and 6.

Example 3.11.
1. Let X be a vector space of dimension 5 over $\mathbb{F}_2$. Select a subspace $X' \leq X$ of dimension 4 and let $\mathscr{A}$ be a 2-spread of X'; see [15, Chapter 4]. Then any two (distinct) elements of $\mathscr{A}$ intersect in $\{0\}$ and $|\mathscr{A}| = (2^4 - 1)/(2^2 - 1) = 5$. Denote by $\mathscr{F}$ the family of 3-subspaces of X that intersect at least one element of $\mathscr{A}$. The lower bound of Theorem 3.6 reads $|\mathscr{F}| \geq 141$ and the one of Theorem 3.8 reads instead $|\mathscr{F}| \geq 139$. Since $\bigcup \mathscr{A}$ is a 4-dimensional subspace of X, all 155 subspaces of X of dimension 3 intersect some element of $\mathscr{A}$.
2. Let X be a vector space of dimension 5 over $\mathbb{F}_2$. Select a subspace $X' \leq X$ of dimension 3 and let $\mathscr{A}$ be the collection of 2-subspaces of X'. We have $|\mathscr{A}| = \mathrm{bin}_2(3, 2) = 7$. Denote by $\mathscr{F}$ the family of 3-subspaces of X that intersect at least one element of $\mathscr{A}$. The lower bound of Theorem 3.6 reads $|\mathscr{F}| \geq 131$, while that of Theorem 3.8 reads $|\mathscr{F}| \geq 112$ and is therefore coarser. Again, all 155 subspaces of X of dimension 3 intersect at least one element of $\mathscr{A}$.

4. Asymptotic results. This section is entirely devoted to the asymptotic versions of Theorems 3.6 and 3.8. These will be stated in the following language.

Notation 4.1. We will use the Bachmann–Landau notation ("big O," "little o," and "$\sim$") to describe the asymptotic growth of real-valued functions defined on an infinite set of natural numbers; see, e.g., [9]. We also denote by Q the set of prime powers and omit "$q \in Q$" when writing $q \to +\infty$.

In the remainder of the paper we will repeatedly need the asymptotic estimate for the q-binomial coefficient as q grows, i.e.,

$$\mathrm{bin}_q(a, b) \sim q^{b(a-b)} \quad \text{as } q \to +\infty \tag{4.1}$$

for all integers $a \geq b \geq 0$. In the following we will apply this well-known fact without explicitly referring to it.

For convenience of exposition and to simplify arguments in the following, we start by establishing the asymptotic version of Theorem 3.8.

Theorem 4.2. *Let $(X_q)_{q \in Q}$ be a sequence of vector spaces, all of which have the same dimension $N \geq 3$ over $\mathbb{F}_q$. Let $(K_q)_{q \in Q}$ be a sequence of cones with $K_q \subseteq X_q$ and $|K_q| \geq q$*

for all $q \in Q$, and let $1 \leq k \leq N-1$ be an integer. For $q \in Q$, denote by $\mathscr{F}_q$ and $\mathscr{F}'_q$ the collections of k-subspaces $W_q \leq X_q$ intersecting and distinguishing K_q, respectively. The following hold.

(1) *We have*

$$\frac{|\mathscr{F}_q|}{\mathrm{bin}_q(N,k)} \in O\left(\frac{|K_q|}{q^{N-k+1}}\right) \quad \text{as } q \to +\infty.$$

In particular, if $|K_q| \in o(q^{N-k+1})$ as $q \to +\infty$, then

$$\lim_{q\to+\infty} \frac{|\mathscr{F}_q|}{\mathrm{bin}_q(N,k)} = 0.$$

(2) *We have*

$$\frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)} \in O\left(\frac{q^{N-k+1}}{|K_q|}\right) \quad \text{as } q \to +\infty.$$

In particular, if $q^{N-k+1} \in o(|K_q|)$ as $q \to +\infty$, then

$$\lim_{q\to+\infty} \frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)} = 0.$$

Proof. In the following, all asymptotic estimates are for $q \to +\infty$. By the upper bound in Theorem 3.8 we have

$$\frac{|\mathscr{F}_q|}{\mathrm{bin}_q(N,k)} \leq \frac{\frac{|K_q|-1}{q-1}\,\mathrm{bin}_q(N-1,k-1)}{\mathrm{bin}_q(N,k)},$$

which establishes the first part of the statement by taking the limit. For the second part, observe first that $|\mathscr{F}_q|+|\mathscr{F}'_q| = \mathrm{bin}_q(N,k)$. Therefore by the lower bound for $|\mathscr{F}_q|$ in Theorem 3.8 we have

$$\frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)} \leq 1 - \frac{\frac{|K_q|-1}{q-1}\,\mathrm{bin}_q(N-1,k-1)}{\mathrm{bin}_q(N,k)\left(1+\left(\frac{|K_q|-1}{q-1}-1\right)\left(\frac{q^{k-1}-1}{q^{N-1}-1}\right)\right)}. \tag{4.2}$$

The latter inequality can be rewritten as

$$\frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)} \leq \frac{1-\frac{q^{k-1}-1}{q^{N-1}-1}-\frac{|K_q|-1}{q-1}\left(\frac{\mathrm{bin}_q(N-1,k-1)}{\mathrm{bin}_q(N,k)}-\frac{q^{k-1}-1}{q^{N-1}-1}\right)}{1+\left(\frac{|K_q|-1}{q-1}-1\right)\left(\frac{q^{k-1}-1}{q^{N-1}-1}\right)}. \tag{4.3}$$

Note that the quantity

$$\frac{\mathrm{bin}_q(N-1,k-1)}{\mathrm{bin}_q(N,k)} - \frac{q^{k-1}-1}{q^{N-1}-1} = \frac{q^k-1}{q^N-1} - \frac{q^{k-1}-1}{q^{N-1}-1}$$

is positive for any q. Thus from (4.3) we obtain

$$\frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)} \leq \frac{1-\dfrac{q^{k-1}-1}{q^{N-1}-1}}{1+\left(\dfrac{|K_q|-1}{q-1}-1\right)\left(\dfrac{q^{k-1}-1}{q^{N-1}-1}\right)} \leq \frac{1}{\left(\dfrac{|K_q|-1}{q-1}-1\right)\left(\dfrac{q^{k-1}-1}{q^{N-1}-1}\right)},$$

from which the second part of the statement follows easily by taking the limit. ■

Remark 4.3. Theorem 4.2 does not predict any asymptotic behavior in the case where $|K_q| \sim \gamma\, q^{N-k+1}$ as $q \to +\infty$ for some constant $\gamma \in \mathbb{R}_{>0}$. The following Proposition 4.4 shows that for any such γ the family $(\mathscr{F}'_q)_{q\in Q}$ is not dense. Right after Proposition 4.4 we will include an example showing that, when $|K_q| \sim q^{N-k+1}$ as $q \to +\infty$, $(\mathscr{F}'_q)_{q\in Q}$ may or may not be sparse.

The following result is easy to obtain by computing the asymptotics in (4.2). The details of the proof are omitted.

Proposition 4.4. *Let $(X_q)_{q\in Q}$ be a sequence of vector spaces, all of which have the same dimension $N \geq 3$ over $\mathbb{F}_q$. Let $(K_q)_{q\in Q}$ be a sequence of cones with $K_q \sim \gamma\, q^{N-k+1}$ for $q \to +\infty$, where $\gamma \in \mathbb{R}_{>0}$ is a constant. Let $1 \leq k \leq N-1$ be an integer and for $q \in Q$ denote by $\mathscr{F}'_q$ the collection of k-subspaces $W_q \leq X_q$ distinguishing K_q. We have*

$$\limsup_{q\to+\infty} \frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)} \leq \frac{1}{\gamma+1} < 1.$$

We now provide the examples mentioned in Remark 4.3, illustrating two possible behaviors in the case $|K_q| \sim q^{N-k+1}$ as $q \to +\infty$.

Example 4.5. (1) Let $(X_q)_{q\in Q}$ be a sequence of linear spaces, all of which have the same dimension $N \geq 3$ over $\mathbb{F}_q$. Let $1 \leq k \leq N-1$ be an integer and fix a sequence $(K_q)_{q\in Q}$ of $(N-k+1)$-spaces with $K_q \leq X_q$ for all $q \in Q$. By dimension considerations, for all $q \in Q$, there are no k-spaces in X_q avoiding the cone K_q. In particular, the k-spaces avoiding K_q are (trivially) sparse.

(2) By definition, the m-dimensional rank-metric codes in $\mathbb{F}_q^{2\times m}$ of minimum distance 2 are exactly the m-dimensional spaces distinguishing the cone of matrices of rank strictly smaller than 2. There are $\boldsymbol{b}_q(2\times m, 1) \sim q^{m+1}$ such matrices for $q \to +\infty$; see the estimate in (5.2) below. As shown in [1, Corollary VII.5], we have $\delta_q(2\times m, m, 2) \sim \sum_{i=0}^{m}(-1)^i/i! > 0$ as $q \to +\infty$. In particular, the m-dimensional subspaces of $\mathbb{F}_q^{2\times m}$ distinguishing the ball in $\mathbb{F}_q^{2\times m}$ of radius 1 are not sparse.

We now turn to the main result of this section (Theorem 4.7). As we will see later, of particular interest for the study of MRD codes are families of linear spaces that, asymptotically, behave like a *partial spread* (we refer the reader to [3] for the notion of partial spread in finite geometry). More precisely, we propose the following concept.

Definition 4.6. *Let $(X_q)_{q\in Q}$ be a sequence of vector spaces of the same dimension $N \geq 3$ over $\mathbb{F}_q$. Let $(\mathscr{A}_q)_{q\in Q}$ be a sequence of collections of subspaces $A_q \leq X_q$, all of which have the same dimension k. We say that $(\mathscr{A}_q)_{q\in Q}$ is an asymptotic partial spread if*

$$\left|\bigcup_{A_q\in\mathscr{A}_q} A_q\right| \sim |\mathscr{A}_q|\, q^k \quad \textit{as } q\to+\infty,$$

i.e., if the cardinality of the union $\bigcup_{A_q\in\mathscr{A}_q} A_q$ *has the largest possible asymptotics for the given parameters.*

We are now ready to state the asymptotic version of Theorem 3.6. The result gives asymptotic estimates for the proportion of common complements of a collection of subspaces. Notice that part (2) of the next theorem will play a central role in establishing Theorem 5.9, which is one of the main results of this paper.

Theorem 4.7. *Let* $(X_q)_{q\in Q}$ *be a sequence of vector spaces, all of which have the same dimension* $N\geq 3$ *over* $\mathbb{F}_q$. *Let* $1\leq k\leq N-1$ *be an integer and let* $(\mathscr{A}_q)_{q\in Q}$ *be a sequence of nonempty collections of linear spaces, all of which have codimension* k *with* $A_q\leq X_q$ *for all* $q\in Q$ *and* $A_q\in\mathscr{A}_q$. *For* $q\in Q$, *denote by* $\mathscr{F}_q$ *and* $\mathscr{F}'_q$ *the collections of* k*-subspaces* $W_q\leq X_q$ *that intersect some* $A_q\in\mathscr{A}_q$ *and that distinguish every* $A_q\in\mathscr{A}_q$, *respectively. Then the following hold.*

(1) *We have*

$$\frac{|\mathscr{F}_q|}{\mathrm{bin}_q(N,k)} \in O\left(\frac{|\mathscr{A}_q|}{q}\right) \quad \textit{as } q\to+\infty.$$

In particular, if $|\mathscr{A}_q|\in o(q)$ *as* $q\to+\infty$, *then*

$$\lim_{q\to+\infty}\frac{|\mathscr{F}_q|}{\mathrm{bin}_q(N,k)}=0.$$

(2) *Suppose that* $(\mathscr{A}_q)_{q\in Q}$ *is an asymptotic partial spread. Then*

$$\frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)} \in O\left(\frac{q}{|\mathscr{A}_q|}\right) \quad \textit{as } q\to+\infty.$$

In particular, if $q\in o(|\mathscr{A}_q|)$ *as* $q\to+\infty$, *then*

$$\lim_{q\to+\infty}\frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)}=0.$$

(3) *Suppose that* $q\in o(|\mathscr{A}_q|)$ *as* $q\to+\infty$ *and that there exist* $\overline{q}\in Q$ *and an integer* ℓ *with* $\max\{0,N-2k\}\leq\ell<N-k-1$ *or* $\ell=\max\{0,N-2k\}=N-k-1$ *that satisfy the following property:*

$$\max\{\dim(A_q\cap A'_q)\mid (A_q,A'_q)\in\mathscr{A}_q^2,\ A_q\neq A'_q\}\leq\ell \quad \forall\, q\in Q,\ q\geq\overline{q}. \tag{4.4}$$

Then the following hold.

(3a) *If* $\ell=\max\{0,N-2k\}$, *then*

$$\frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)} \in O\left(\frac{q}{|\mathscr{A}_q|}\right) \quad \textit{as } q\to+\infty.$$

(3b) *If* $\ell > \max\{0, N-2k\}$, *then*

$$\frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)} \in O\left(\frac{q}{|\mathscr{A}_q|} + q^{-N+k+\ell+1}\right) \quad \textit{as } q \to +\infty.$$

In either case we have

$$\lim_{q\to+\infty} \frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)} = 0.$$

Before proceeding with the proof of Theorem 4.7, we describe its statement from a more "qualitative" viewpoint.

Remark 4.8. Theorem 4.7 illustrates the general behavior of the common complements of the spaces in $(\mathscr{A}_q)_{q\in Q}$ as the field size grows. With the only exception being when $\ell = N-k-1$ (the case in which we are not able to predict the behavior), the decisive property for sparsity/density is whether or not the integer sequence $(|\mathscr{A}_q|)_{q\in Q}$ is negligible with respect to the field size q in the asymptotics. It is interesting to observe that Theorem 4.7 does not extend to the case where, for example, $|\mathscr{A}_q| \sim q$ as $q \to +\infty$. We will elaborate on this at the end of the section; see Example 4.10.

In the remainder of the section we establish Theorem 4.7. We start with a technical lemma, whose proof can be found in the appendix.

Lemma 4.9. *Let* N*,* k*, and* ℓ *be integers as in Notation* 2.1*. The following estimates hold as* $q \to +\infty$*:*

$$\nu_q(N,k,\ell) \sim \begin{cases} q^{k(N-k)-2} & \text{if } \max\{0,N-2k\} \le \ell < N-k-1 \\ & \text{or } \ell = N-k-1 = \max\{0,N-2k\}, \\ 2q^{k(N-k)-2} & \text{if } \ell = N-k-1 > \max\{0,N-2k\}, \\ q^{k(N-k)-1} & \text{if } \ell = N-k, \end{cases}$$

$$\frac{\nu_q(N,k,N-k)^2}{\mathrm{bin}_q(N,k)} - \nu_q(N,k,\ell) \sim \begin{cases} q^{k(N-k)-N+k-1} & \text{if } \ell = N-2k, \\ q^{k(N-k)-k-1} & \text{if } \ell = 0, \\ -q^{k(N-k)-N+k+\ell-1} & \text{if } \ell > \max\{0,N-2k\}. \end{cases}$$

Proof of Theorem 4.7. All asymptotic estimates in this proof are for $q \to +\infty$. We examine the three cases in the statement separately.

(1) By Theorem 3.6 we have

$$\frac{|\mathscr{F}_q|}{\mathrm{bin}_q(N,k)} \le \frac{|\mathscr{A}_q|}{\mathrm{bin}_q(N,k)}\, \nu_q(N,k,N-k),$$

which, together with Lemma 4.9, gives the desired asymptotic estimate.

(2) Consider the cone

$$K_q := \bigcup_{A_q \in \mathscr{A}_q} A_q.$$

Since $\mathscr{A}_q$ is an asymptotic partial spread by assumption, we have $K_q \sim |\mathscr{A}_q|\, q^{N-k}$. The statement now follows from Theorem 4.2(2).

(3) Denote by $\ell_{\max}$ the maximum on the left-hand side of the condition in (4.4). Since $|\mathscr{F}_q| + |\mathscr{F}'_q| = \mathrm{bin}_q(N,k)$, the lower bound for $|\mathscr{F}_q|$ in Theorem 3.6 tells us that, for all $q \geq \overline{q}$,

$$\frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)} \leq 1 - \frac{\nu_q(N,k,N-k)^2\,|\mathscr{A}_q|}{\mathrm{bin}_q(N,k)\,(\nu_q(N,k,N-k) + (|\mathscr{A}_q|-1)\,\nu_q(N,k,\ell_{\max}))}$$

$$\leq 1 - \frac{\nu_q(N,k,N-k)^2\,|\mathscr{A}_q|}{\mathrm{bin}_q(N,k)\,(\nu_q(N,k,N-k) + (|\mathscr{A}_q|-1)\,\nu_q(N,k,\ell))}, \tag{4.5}$$

where the latter inequality follows from the fact that $\ell \mapsto \nu_q(N,k,\ell)$ is increasing (for this, see again (A.1) in the appendix). Define the difference

$$\Delta_q(N,k,\ell) := \frac{\nu_q(N,k,N-k)^2}{\mathrm{bin}_q(N,k)} - \nu_q(N,k,\ell).$$

We rewrite the inequality in (4.5) as follows:

$$\frac{|\mathscr{F}'_q|}{\mathrm{bin}_q(N,k)} \leq \frac{\nu_q(N,k,N-k) - \nu_q(N,k,\ell) - |\mathscr{A}_q|\,\Delta_q(N,k,\ell)}{\nu_q(N,k,N-k) + (|\mathscr{A}_q|-1)\,\nu_q(N,k,\ell)}. \tag{4.6}$$

Since $q \in o(|A_q|)$ and $\max\{0, N-2k\} \leq \ell < N-k-1$ or $\ell = \max\{0, N-2k\} = N-k-1$, using the asymptotic estimates from Lemma 4.9 we get

$$\nu_q(N,k,N-k) - \nu_q(N,k,\ell) \sim q^{k(N-k)-1}, \tag{4.7}$$

$$\nu_q(N,k,N-k) + (|\mathscr{A}_q|-1)\,\nu_q(N,k,\ell) \sim |\mathscr{A}_q|\,q^{k(N-k)-2}. \tag{4.8}$$

If $\ell = \max\{0, N-2k\}$, then Lemma 4.9 tells us that $\Delta_q(N,k,\ell)$ is positive for q sufficiently large. Therefore case (3a) follows by combining (4.6), (4.7), and (4.8). In particular, $\lim_{q\to+\infty} |\mathscr{F}'_q|/\mathrm{bin}_q(N,k) = 0$.
Now suppose that $\ell > \max\{0, N-2k\}$, which in turn implies $\ell < N-k-1$. Using again Lemma 4.9 we obtain

$$\frac{\Delta_q(N,k,\ell)}{q^{k(N-k)-2}} \sim -q^{-N+k+\ell+1}.$$

Combining this estimate with (4.6), (4.7), and (4.8) one establishes case (3b). Finally, the fact that $\lim_{q\to+\infty} |\mathscr{F}'_q|/\mathrm{bin}_q(N,k) = 0$ follows from $q \in o(|\mathscr{A}_q|)$ and $\ell < N-k-1$, which implies $-N+k+\ell+1 \leq -1$. ∎

We conclude this section with two examples focusing on the case $|\mathscr{A}_q| \sim q$ as $q \to +\infty$, which is not covered by Theorem 4.7. We show that in such a case the common complements can be sparse or not.

Example 4.10. (1) Let $(X_q)_{q\in Q}$ be a sequence of linear spaces, all of which have the same dimension $N \geq 3$ over $\mathbb{F}_q$. Fix a sequence $(V_q)_{q\in Q}$ of 2-dimensional spaces $V_q \leq X_q$. For $q \in Q$, denote by $\mathscr{A}_q$ the set of 1-dimensional subspaces of V_q. We then have $|\mathscr{A}_q| \sim \mathrm{bin}_q(2,1) \sim q$ as $q \to +\infty$. In particular, there are no $(N-1)$-dimensional subspaces of X_q that distinguish V_q and the common complements of the spaces in $\mathscr{A}_q$ are sparse.

(2) Let $m \geq 2$ be an integer. By Remark 1.10, the MRD codes of minimum distance 2 in $\mathbb{F}_q^{2\times m}$ are the common complements of $\mathrm{bin}_q(2,1) \sim q$ subspaces of $\mathbb{F}_q^{2\times m}$ having dimension m, where the estimate is for $q \to +\infty$. Their asymptotic density is then $\delta_q(2\times m, m, 2) \sim \sum_{i=0}^{m}(-1)^i/i! > 0$ as $q \to +\infty$; see [1, Corollary VII.5] and the discussion right after our Theorem 5.3. In particular, they are not sparse.

5. The density function of rank-metric codes.

In this section we apply the theory developed in the previous sections to matrix spaces over a finite field, obtaining upper and lower bounds for the density functions of MRD codes. By computing the limit as $q \to +\infty$ in these bounds we then solve Problem 1.8, stated in the introduction of this paper. In particular, we prove that MRD codes in $\mathbb{F}_q^{n\times m}$ of minimum distance d are sparse unless $d = 1$ or $d = n = 2$.

Before presenting the main theorems of this section and their proofs, we briefly survey the current literature connected to Problem 1.8. This will also serve to put our results in the context of previous work.

Notation 5.1. For ease of exposition, throughout this section we work with fixed integers m, n, and d with $m \geq n \geq 2$ and $1 \leq d \leq n$.

The density limit considered in Problem 1.8 has been studied in [1, 6, 13], showing in particular that

$$\limsup_{q\to+\infty} \delta(n\times m, m(n-d+1), d) < 1 \text{ whenever } d \geq 2.$$

This result appears quite surprising when thinking of MRD codes as the rank-metric analogues of MDS codes in the Hamming metric, which are classically known to be dense. It turns out that the approach developed in this paper provides a clear explanation for the divergence in the behavior of these two classes of codes; see Remark 5.11 below.

The methods used in [6], [1], and [13] are very different from each other. The approach of [6] uses a combinatorial machinery based on families of codes that are *balanced* with respect to a given partition of the ambient space, leading to the following result.

Theorem 5.2 (see [6, Corollary 6.2]). *If $d \geq 2$, then*

$$\limsup_{q\to+\infty} \delta_q(n\times m, m(n-d+1), d) \leq 1/2.$$

A sharper bound is obtained in [1] using the theory of spectrum-free matrices, combined with a probability argument. The result reads as follows.

Theorem 5.3 (see [1, Theorem VII.6]). *We have*

$$\limsup_{q\to+\infty} \delta_q(n\times m, m(n-d+1), d) \leq \left(\sum_{i=0}^{m}\frac{(-1)^i}{i!}\right)^{(d-1)(n-d+1)}.$$

In [1] it is also shown that the bound of Theorem 5.3 is sharp whenever $d = n = 2$ (and for arbitrary $m \geq 2$). This means that, in general, MRD codes are neither sparse, nor dense.

Finally, in [13] the exact density of MRD codes with parameters $m = n = d = 3$ is computed, showing that these 3×3 codes are sparse. The approach of [13] is based on an original argument that connects full-rank square MRD codes with the theory of semifields.

Theorem 5.4 (see [13, Theorem 2.4]). *We have*

$$\delta_q(3\times 3,3,3)=\frac{(q-1)\,(q^3-1)\,(q^3-q)^3\,(q^3-q^2)^2\,(q^3-q^2-q-1)}{3\,(q^7-1)\,(q^9-1)\,(q^9-q)}.$$

In particular, $\lim_{q\to+\infty}\delta_q(3\times 3,3,3)=0$.

In this paper we approach Problem 1.8 from a different viewpoint, which allows us to obtain sharper bounds for the density function of MRD codes. As an application, we conclude that MRD codes are sparse as $q\to+\infty$, unless $d=1$ or $n=d=2$. We therefore show that the nonsparseness result of [1] for $d=n=2$ is the only nontrivial exception to a general "sparseness behavior."

We start with an upper bound on the density of MRD codes, which is the main result of this section. In the statement, we will need the following quantity.

Notation 5.5. For a prime power q and nonnegative integers u and i with $u\le n$ and $2u-n\le i\le u$, we let $\theta_q(n,u,i)$ denote the number of pairs (U,U') of u-spaces $U,U'\le\mathbb{F}_q^n$ with the property that $\dim(U\cap U')=i$.

The next lemma gives a closed expression for $\theta_q(n,u,i)$.

Lemma 5.6. *Let q, u, and i be as in Notation 5.5. We have*

$$\theta_q(n,u,i)=\sum_{j=i}^{u}(-1)^{j-i}q^{\binom{j-i}{2}}\,\mathrm{bin}_q(n,i)\,\mathrm{bin}_q(n-i,j-i)\,\mathrm{bin}_q(n-j,u-j)^2.$$

Proof. We will use Möbius inversion in the lattice of subspaces of $\mathbb{F}_q^n$. For a subspace $W\le\mathbb{F}_q^n$, let $f(W):=|\{(U,U')\mid U,U'\le\mathbb{F}_q^n,\ \dim(U)=\dim(U')=u,\ U\cap U'=W\}|$. Observe that for all $W\le\mathbb{F}_q^n$ we have

$$g(W):=\sum_{\substack{L\le\mathbb{F}_q^n\\ L\ge W}}f(L)=\mathrm{bin}_q(n-\dim(W),u-\dim(W))^2.$$

We now use the Möbius inversion formula for the lattice of subspaces of $\mathbb{F}_q^n$ (see, e.g., Proposition 3.7.2 and Example 3.10.2 in [27]), finding that for every $W\le\mathbb{F}_q^n$ of dimension i we have

$$\begin{aligned}f(W)&=\sum_{j=i}^{u}(-1)^{j-i}q^{\binom{j-i}{2}}\sum_{\substack{L\ge W\\ \dim(L)=j}}g(L)\\ &=\sum_{j=i}^{u}(-1)^{j-i}q^{\binom{j-i}{2}}\,\mathrm{bin}_q(n-i,j-i)\,\mathrm{bin}_q(n-j,u-j)^2.\end{aligned}$$

The desired expression for $\theta_q(n,u,i)$ can be obtained by summing the previous identity over all subspaces $W\le\mathbb{F}_q^n$ having dimension i. ∎

Our main result on the density function of MRD codes is the following. It provides an upper bound for the number of MRD codes with given parameters in terms of the quantities ν and θ defined/computed earlier in the paper (Notation 2.1 and Lemma 5.6).

Theorem 5.7. *Suppose $d \geq 2$ and let $k = m(n-d+1)$. We have*

$$\delta_q(n \times m, k, d) \leq 1 - \frac{\mathrm{bin}_q(n, d-1)^2\, \nu_q(mn, k, m(d-1))^2}{\mathrm{bin}_q(mn, k) \sum_{i=0}^{d-1} \nu_q(mn, k, mi)\, \theta_q(n, d-1, i)}. \tag{5.1}$$

Proof. For $q \in Q$, consider the collection $\mathscr{U}_q$ of subspaces $U_q \leq \mathbb{F}_q^n$ with $\dim(U_q) = d-1 \geq 1$. We follow the notation of Remark 1.10 and let $\mathscr{A}_q = \{\mathbb{F}_q^{n\times m}(U_q) \mid U_q \in \mathscr{U}_q\}$ for all $q \in Q$. Note that $|\mathscr{A}_q| = \mathrm{bin}_q(n, d-1)$ and that the MRD codes $\mathscr{C}_q \leq \mathbb{F}_q^{n\times m}$ of minimum distance d are precisely the common complements of the spaces in $\mathscr{A}_q$. Furthermore, for $U_q, U_q' \in \mathscr{U}_q$ we have

$$\dim(\mathbb{F}_q^{n\times m}(U_q) \cap \mathbb{F}_q^{n\times m}(U_q')) = \dim(\mathbb{F}_q^{n\times m}(U_q \cap U_q')) = mi$$

for some $i \in \{0, 1, ..., d-1\}$. Therefore,

$$\begin{aligned}\sum_{\ell=0}^{mn-k} &\nu_q(mn, k, \ell) \cdot |\{(A_q, A_q') \in \mathscr{A}_q^2 \mid \dim(A_q \cap A_q') = \ell\}| \\ &= \sum_{i=0}^{d-1} \nu_q(mn, k, mi)\, \theta_q(n, d-1, i).\end{aligned}$$

The desired bound now immediately follows from Theorem 3.6. ■

Experimental results indicate that the quantity on the right-hand side (RHS) of (5.1) is asymptotically $q^{-(d-1)(n-d+1)+1}$ as $q \to +\infty$. Since this asymptotic estimate does not seem immediate to derive, we will obtain the sparseness of MRD codes using the concept of an asymptotic partial spread we introduced in Definition 4.6.

Definition 5.8. *The **ball** of radius $0 \leq r \leq n$ in $\mathbb{F}_q^{n\times m}$ is the set of matrices $M \in \mathbb{F}_q^{n\times m}$ with $\mathrm{rk}(M) \leq r$. It is well known that its size is*

$$\boldsymbol{b}_q(n \times m, r) := \sum_{i=0}^{r} \mathrm{bin}_q(n, i) \prod_{j=0}^{i-1} (q^m - q^j) \sim q^{r(m+n-r)} \quad \text{as } q \to +\infty. \tag{5.2}$$

The following result computes the asymptotic density of MRD codes as $q \to +\infty$ for all parameter sets, showing that they are (very) sparse whenever $n \geq 3$ and $d \geq 2$. This solves Problem 1.8.

Theorem 5.9. *We have*

$$\delta_q(n \times m, m(n-d+1), d) \in O\left(q^{-(d-1)(n-d+1)+1}\right) \quad \text{as } q \to +\infty.$$

Moreover,

$$\lim_{q\to+\infty} \delta_q(n \times m, m(n-d+1), d) = \begin{cases} 1 & \text{if } d = 1, \\ \sum_{i=0}^{m} \frac{(-1)^i}{i!} & \text{if } n = d = 2, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The statement immediately follows from the definitions if $d = 1$. We henceforth assume $d \geq 2$. For $q \in Q$, denote by $\mathscr{A}_q$ the family in the proof of Theorem 5.7. We have $|\mathscr{A}_q| = \mathrm{bin}_q(n, d-1) \sim q^{(d-1)(n-d+1)}$ as $q \to +\infty$. Since all the spaces in $\mathscr{A}_q$ have dimension $m(d-1)$ and $\boldsymbol{b}_q(n \times m, d) \sim q^{(d-1)(m+n-d+1)}$ as $q \to +\infty$ by (5.2), this shows that $(\mathscr{A}_q)_{q \in Q}$ is an asymptotic partial spread; see Definition 4.6. Therefore the first part of the statement follows from Theorem 4.7. In particular, the density limit is zero whenever $n \geq 3$ and $d \geq 2$. The limit for $n = d = 2$ has already been computed in [1, Proposition VII.5]. ■

Remark 5.10. In [13, Theorem 2.4] it was shown that $\delta_q(3 \times 3, 3, 3) \sim \frac{1}{3} q^{-3}$ as $q \to +\infty$. On the other hand, our Theorem 5.9 gives that $\delta_q(3 \times 3, 3, 3) \in O(q^{-1})$ as $q \to +\infty$. This shows that the asymptotic bound of Theorem 5.9 is not sharp in general.

We now turn to explaining why MDS and MRD codes behave so differently with respect to density properties.

Remark 5.11. The approach developed in this paper offers an explanation for why MDS and MRD codes exhibit different behaviors with respect to sparseness and density. Recall that, for $1 \leq k \leq n$, a *k-MDS code* is a k-dimensional subspace $C \leq \mathbb{F}_q^n$ that does not contain any nonzero vector of Hamming weight strictly smaller than $n - k + 1$; see [19, Chapter 11]. For a subset $S \subseteq \{1, ..., n\}$, let $\mathbb{F}_q^n(S) \leq \mathbb{F}_q^n$ denote the space of vectors $x \in \mathbb{F}_q^n$ with $x_i = 0$ for all $i \notin S$. Then k-MDS codes can be seen as the common complements of the spaces of the form $\mathbb{F}_q^n(S)$, where $S \subseteq \{1, ..., n\}$ has size $n - k$. The number of such spaces is $\binom{n}{k}$, which is negligible with respect to q as $q \to +\infty$. We can therefore use Theorem 4.7 to explain why MDS codes are dense as the field size tends to infinity: They are the common complements of a collection of subspaces whose cardinality is negligible with respect to the field size.

For the case of MRD codes the situation is exactly the opposite. As Remark 1.10 shows, MRD codes are the common complements of a collection of subspaces that form an asymptotic partial spread and whose cardinality, for $n \geq 3$ and $d \geq 2$, is far from being negligible with respect to the field size q as $q \to +\infty$. In particular, they must be sparse by Theorem 4.7.

Combining Theorems 3.8 and 4.2, and the estimate in (5.2) we can also study the density function of rank-metric codes for any minimum distance and any dimension (not just MRD codes). In the next result we give upper and lower bounds for this function and their asymptotic versions as q tends to infinity. For the case of MRD codes, we find that the bounds one obtains are in general worse than the ones given in Theorem 5.7; see Figure 5.1, which reflects the general behavior we observed.

Theorem 5.12. *For all* $2 \leq d \leq n$ *and* $1 \leq k \leq mn$ *we have*

$$1 - \delta_q(n \times m, k, d) \leq \frac{(\boldsymbol{b}_q(n \times m, d-1) - 1)\, \mathrm{bin}_q(mn-1, k-1)}{(q-1)\, \mathrm{bin}_q(mn, k)},$$

$$\delta_q(n \times m, k, d) \leq 1 - \frac{(\boldsymbol{b}_q(n \times m, d-1) - 1) \left(\dfrac{q^k - 1}{q^{mn} - 1} \right)}{(q-1) + (\boldsymbol{b}_q(n \times m, d-1) - q) \left(\dfrac{q^{k-1} - 1}{q^{mn-1} - 1} \right)}.$$

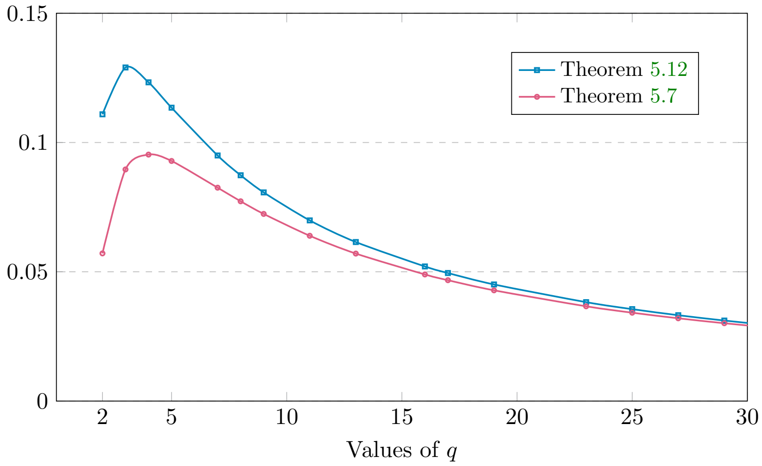

Figure 5.1. *Comparison of the upper bounds for $\delta_q(3 \times 5, 5, 3)$ as $q \to +\infty$ in Theorem 5.7 (red) and in Theorem 5.12 (blue).*

In particular,

$$1 - \delta_q(n \times m, k, d) \in O\left(q^{(d-1)(m+n-d+1)-(mn-k)-1}\right) \quad \text{as } q \to +\infty,$$
$$\delta_q(n \times m, k, d) \in O\left(q^{-(d-1)(m+n-d+1)+(mn-k)+1}\right) \quad \text{as } q \to +\infty.$$

Therefore,

$$\lim_{q \to +\infty} \delta_q(n \times m, k, d) = \begin{cases} 1 & \text{if } (d-1)(m+n-d+1) \leq mn - k, \\ 0 & \text{if } (d-1)(m+n-d+1) \geq mn - k + 2. \end{cases}$$

Remark 5.13. It is interesting to observe that Theorem 5.12 does not extend to the case $k = mn - (d-1)(m+n-d+1) + 1$. Proposition 4.4 shows that, for this value of k, $\limsup_{q \to +\infty} \delta_q(n \times m, k, d) \leq 1/2$. On the other hand, in [1, Corollary VII.5] the asymptotic density of $2 \times m$ MRD codes of dimension m was computed as $q \to +\infty$, proving that $\lim_{q \to +\infty} \delta_q(2 \times m, m, 2) > 0$. This shows that, in general, rank-metric codes of dimension $k = mn - (d-1)(m+n-d+1) + 1$ are neither sparse, nor dense, as $q \to +\infty$.

6. Asymptotic density of MRD codes for $m \to +\infty$. In this section we study the asymptotic density of MRD codes as their number of columns, namely, m, tends to infinity. Although our approach is not powerful enough to compute the "exact" asymptotic density in this setting, as we will see it improves on known results for several parameter sets.

Notation 6.1. In the following we fix a prime power q and integers n, d with $n \geq 2$ and $n \geq d \geq 1$. We omit "$m \in \mathbb{N}$, $m \geq n$" when writing $m \to +\infty$.

As for section 5, we start by surveying the previous literature. The analogue of Theorem 5.2 for $m \to +\infty$ is the following.

Theorem 6.2 (see [6, Corollary 6.4]). *For all $d \geq 2$ we have*

$$\limsup_{m \to +\infty} \delta_q(n \times m, m(n-d+1), d) \leq \frac{(q-1)(q-2)+1}{2(q-1)^2} \leq \frac{1}{2}.$$

The analogue of Theorem 5.3 for $m \to +\infty$ is [1, Theorem VII.6], which we directly state in the language of this paper for convenience. The equivalence with [1, Theorem VII.6] easily follows from the estimate in (6.2) below and [1, Theorem VII.1].

Theorem 6.3 (see [1, Theorem VII.6]). *For all $d \geq 2$ we have*

$$\limsup_{m \to +\infty} \delta_q(n \times m, m(n-d+1), d) \leq \prod_{i=1}^{\infty} \left(1 - \frac{1}{q^i}\right)^{q(d-1)(n-d+1)+1}.$$

In order to derive the asymptotic version of Theorem 5.7 for $m \to +\infty$, we will first compute the asymptotics of the quantities it involves (Lemma 6.5 below). For ease of notation, let

$$\pi(q) := \prod_{i=1}^{\infty} \left(\frac{q^i}{q^i - 1}\right). \tag{6.1}$$

The quantity $\pi(q)$ arises in the asymptotic estimate of the q-binomial coefficient $\text{bin}_q(ma, mb)$ as m tends to infinity. More precisely, for all integers $a > b > 0$ we have

$$\begin{aligned} \text{bin}_q(ma, mb) = \prod_{i=0}^{mb-1} \frac{(q^{ma} - q^i)}{(q^{mb} - q^i)} &= q^{mb(ma-mb)} \prod_{i=1}^{mb} \frac{1 - q^{i-ma-1}}{1 - q^{-i}} \\ &\sim q^{m^2 b(a-b)} \, \pi(q) \end{aligned} \tag{6.2}$$

as $m \to +\infty$. We will need this estimate later.

Remark 6.4. The infinite product $\pi(q)$ in (6.1) is closely related to the Euler function ϕ; see [2, section 14] for a standard reference. The latter is the function $\phi : (-1, 1) \to \mathbb{R}$ defined by

$$\phi(x) := \prod_{i=1}^{\infty} (1 - x^i) \tag{6.3}$$

for all $x \in (-1, 1)$. We then have $\pi(q) = 1/\phi(1/q)$ for all $q \in Q$. In particular, $\pi(q) > 1$ for all $q \in Q$. A classical result in number theory, due to Euler himself, expresses the infinite product in (6.3) as the infinite sum

$$\phi(x) = 1 + \sum_{k=1}^{\infty} (-1)^k \left(x^{k(3k+1)/2} + x^{k(3k-1)/2}\right) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \cdots.$$

This is the famous pentagonal number theorem [2, Theorem 14.3]. From the above expression for ϕ as a power series, we deduce the following asymptotic estimates:

$$\phi(x) \sim 1 \text{ as } x \to 0, \qquad \phi(x) - 1 \sim -x \text{ as } x \to 0. \tag{6.4}$$

The next result gives an asymptotic estimate for $\nu_q(mn, m(n-d+1), mi)$ for $1 \leq i \leq d-1$ as $m \to +\infty$. We will need it to establish Theorem 6.6. Note that we only examine dimensions that are a multiple of m, as for other dimensions MRD codes do not exist. Furthermore, we will only need multiples of m as intersection dimensions. The proof of the next lemma can be found in the appendix.

Lemma 6.5. *Let $d \geq 2$ and let $0 \leq i \leq d-1$ be an integer. The following asymptotic estimates hold as $m \to +\infty$:*

$$\nu_q(mn, m(n-d+1), mi) \sim \begin{cases} q^{m^2(n-d+1)(d-1)} \, (\pi(q)-1)^2/\pi(q) & \text{if } 0 \leq i \leq d-2, \\ q^{m^2(n-d+1)(d-1)} \, (\pi(q)-1) & \text{if } i = d-1. \end{cases}$$

We are now ready to derive the asymptotic version of Theorem 5.7 as $m \to +\infty$.

Theorem 6.6. *For all $d \geq 2$ we have*

$$\limsup_{m\to+\infty} \delta_q(n \times m, m(n-d+1), d) \leq \frac{1}{\text{bin}_q(n, d-1)\,(\pi(q)-1)+1}.$$

Proof. To simplify the notation throughout the proof, let $k_m = m(n-d+1)$. All estimates in the following are for $m \to +\infty$. The upper bound on $\delta_q(n \times m, k_m, d)$ given in Theorem 5.7 reads

$$\delta_q(n \times m, k_m, d) \leq \frac{a_m + b_m - c_m}{a_m + b_m}, \tag{6.5}$$

where

$$\begin{aligned} a_m &= \textstyle\sum_{i=0}^{d-2} \nu_q(mn, k_m, mi)\, \theta_q(n, d-1, i), \\ b_m &= \theta_q(n, d-1, d-1)\, \nu_q(mn, k_m, m(d-1)), \\ c_m &= \frac{\text{bin}_q(n, d-1)^2\, \nu_q(mn, k_m, m(d-1))^2}{\text{bin}_q(mn, k_m)}. \end{aligned}$$

The three quantities above can be conveniently estimated individually with the aid of Lemma 6.5. All the computations are tedious but straightforward, so we only include the final results:

$$\begin{cases} a_m \sim (\pi(q)-1)^2/\pi(q) \, \sum_{i=0}^{d-2} \theta_q(n, d-1, i)\, q^{k_m(mn-k_m)}, \\ b_m \sim \theta_q(n, d-1, d-1)\, (\pi(q)-1)\, q^{k_m(mn-k_m)}, \\ c_m \sim \text{bin}_q(n, d-1)^2\, (\pi(q)-1)^2/\pi(q)\, q^{k_m(mn-k_m)}. \end{cases} \tag{6.6}$$

Using Notation 5.5 directly we find

$$\begin{aligned} \textstyle\sum_{i=0}^{d-2} \theta_q(n, d-1, i) &= \text{bin}_q(n, d-1)\, (\text{bin}_q(n, d-1)-1), \\ \theta_q(n, d-1, d-1) &= \text{bin}_q(n, d-1). \end{aligned}$$

This allows us to rewrite (6.6) as

$$\begin{cases} a_m \sim (\pi(q)-1)^2/\pi(q)\, \text{bin}_q(n, d-1)\, (\text{bin}_q(n, d-1)-1)\, q^{k_m(mn-k_m)}, \\ b_m \sim (\pi(q)-1)\, \text{bin}_q(n, d-1)\, q^{k_m(mn-k_m)}, \\ c_m \sim \text{bin}_q(n, d-1)^2\, (\pi(q)-1)^2/\pi(q)\, q^{k_m(mn-k_m)}. \end{cases} \tag{6.7}$$

Now observe that the three estimates in (6.7) are of the form $a_m \sim af_m$, $b_m \sim bf_m$, and $c_m \sim cf_m$, where $f_m = q^{k_m(mn-k_m)}$ and $a, b, c \in \mathbb{R}$ are positive constants in m. Moreover, one can check that

$$\frac{a+b-c}{a+b} = \frac{1}{\mathrm{bin}_q(n, d-1)\,(\pi(q)-1)+1} \neq 0.$$

Therefore the desired theorem follows by taking the limit superior as $m \to +\infty$ in (6.5). ■

As for the case where $q \to +\infty$, the bound on the density of MRD codes that one obtains from Theorem 5.7 is better than the one from Theorem 3.8. We elaborate on this in the following remark.

Remark 6.7. For m sufficiently large, the bound on $\delta_q(n \times m, m(n-d+1), d)$ obtained from Theorem 3.8 is worse than the one of Theorem 5.7 (which we in turn derived from Theorem 3.6). This is true even in the asymptotics. More precisely, recall the following estimate for the size of the ball:

$$\boldsymbol{b}_q(n \times m, d-1) \sim \mathrm{bin}_q(n, d-1) q^{m(d-1)} \quad \text{as } m \to +\infty. \tag{6.8}$$

Using this estimate, one can obtain the following asymptotic version of the bound of Theorem 5.12:

$$\limsup_{m \to +\infty} \delta_q(n \times m, m(n-d+1), d) \leq \frac{q-1}{\mathrm{bin}_q(n, d-1)+q-1} \quad \text{whenever } d \geq 2. \tag{6.9}$$

An easy computation shows that the upper bound in Theorem 6.6 is always sharper than the one in (6.9).

Remark 6.8. The asymptotic upper bound of Theorem 6.6 is sharper than the bound of [1, Theorem VII.6] for q sufficiently large, $n \geq d \geq 2$ and $n > 2$, while it is coarser for small values of q. To show this, we first rewrite [1, Theorem VII.6] (in the form stated in Theorem 6.3) as

$$\limsup_{m \to +\infty} \delta_q(n \times m, m(n-d+1), d) \leq \frac{1}{\pi(q)^{q(d-1)(n-d+1)+1}}.$$

We now prove that

$$\lim_{q \to +\infty} \frac{\pi(q)^{q(d-1)(n-d+1)+1}}{\mathrm{bin}_q(n, d-1)(\pi(q)-1)+1} = 0 \quad \text{for } n \geq d \geq 2 \text{ and } n > 2, \tag{6.10}$$

from which it immediately follows that the bound of Theorem 6.6 is sharper than the one of [1, Theorem VII.6] for q sufficiently large. To see why (6.10) holds, we note first that

$$\lim_{q \to +\infty} \left(1 - \frac{1}{q^i}\right)^q = \begin{cases} 1/e & \text{if } i = 1, \\ 1 & \text{if } i \geq 2. \end{cases}$$

Therefore $\lim_{q \to +\infty} \phi(1/q)^q = \prod_{i=1}^{\infty} \left(1 - 1/q^i\right)^q = 1/e$. Since $\pi(q) = 1/\phi(1/q)$, as already observed in Remark 6.4, we have $\lim_{q \to +\infty} \pi(q)^q = e$. Furthermore, using the asymptotic estimates in (6.4) we find that

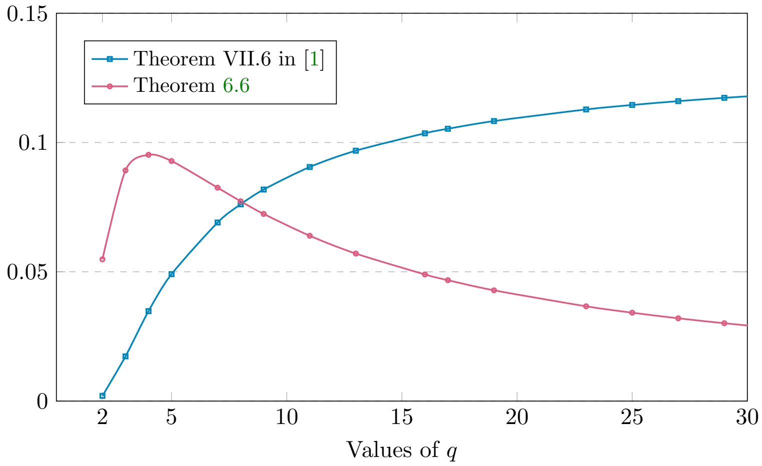

Figure 6.1. *The upper bounds for* $\limsup_{m\to+\infty} \delta_q(3\times m, m, 3)$ *from Theorem* 6.6 *(red) and* [1, Theorem VII.6] *(blue).*

$$\pi(q) - 1 = \frac{1-\phi(1/q)}{\phi(1/q)} \sim \frac{1}{q} \quad \text{as } q \to +\infty.$$

Combining this with the estimate for $\pi(q)^q$ given above we obtain, for $n \geq d \geq 2$,

$$\frac{\pi(q)^{q(d-1)(n-d+1)+1}}{\text{bin}_q(n, d-1)(\pi(q)-1)+1} \sim \frac{e^{(d-1)(n-d+1)+1}}{q^{(d-1)(n-d+1)-1}} \quad \text{as } q \to +\infty.$$

The fraction on the RHS of the previous estimate approaches 0 as q approaches $+\infty$, thereby establishing the desired limit in (6.10).

A comparison of the two bounds we just discussed can be seen in Figure 6.1. The plot shows that for $(n, d) = (3, 3)$ the bound of Theorem 6.6 is sharper than [1, Theorem VII.6] for all prime powers $q \geq 9$, and coarser for $2 \leq q \leq 8$. The two bounds are decreasing and increasing in q, respectively.

7. Further properties of density functions.

We devote the last section of the paper to general properties of the density function of rank-metric codes. More precisely, we initiate the study of how density functions relate to each other as the parameters (n, m, d, k) change. As an application of our results, we reinterpret the bounds of [1] via shortening and duality considerations.

Notation 7.1. In the following, q is a prime power and n, m, d denote positive integers with $m \geq n \geq 2$ and $1 \leq d \leq n$. When writing "$q \to +\infty$" or "$m \to +\infty$," the other parameters are treated as constants. As in section 4, the limit for $q \to +\infty$ is taken over the set of all prime powers, denoted by Q.

Lemma 7.2. *Every MRD code* $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$ *with minimum distance* $d \geq 2$ *admits a unique basis of the form*

$$\left\{ \left(\frac{E_{ij}}{A_{ij}} \right) \mid 1 \leq i \leq n-d+1,\ 1 \leq j \leq m \right\}, \tag{7.1}$$

where $A_{ij} \in \mathbb{F}_q^{(d-1)\times m}$ *is a suitable matrix and* $E_{ij} \in \mathbb{F}_q^{(n-d+1)\times m}$ *denotes the matrix having a* 1 *in position* (i,j) *and 0 elsewhere. Moreover, all the matrices in* (7.1) *have rank exactly* d.

Proof. The result follows from the fact that the projection $\pi : \mathscr{C} \to \mathbb{F}_q^{(n-d+1)\times m}$ on the first $n-d+1$ rows is an isomorphism. Injectivity is a consequence of the fact that $\mathscr{C}$ has minimum distance d and bijectivity follows from cardinality considerations. The last part of the statement can be seen by observing that $\mathscr{C}$ has minimum distance d and that all matrices in (7.1) have $n-d$ zero rows. ■

Proposition 7.3. *Suppose* $n \geq 3$ *and* $2 \leq d < n$. *We have*

$$\delta_q(n \times m, m(n-d+1), d) \leq \delta_q(d \times m, m, d)\, \delta_q((n-1)\times m, m(n-d), d)\, \frac{B_q(n\times m, d)}{A_q(n\times m, d)},$$

where

$$A_q(n\times m, d) = \mathrm{bin}_q(mn, m(n-d+1)),$$
$$B_q(n\times m, d) = \mathrm{bin}_q(md, m)\,\mathrm{bin}_q(m(n-1), m(n-d)).$$

Proof. We start by showing that every MRD code $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$ with minimum distance d can be decomposed as (the embedding of) a direct sum of an MRD code in $\mathbb{F}_q^{d\times m}$ and an MRD code in $\mathbb{F}_q^{(n-1)\times m}$, both of which have minimum distance exactly d. For this, let $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$ be an MRD code with minimum distance d. By Lemma 7.2, $\mathscr{C}$ has a basis of the form

$$\left\{ \begin{pmatrix} E_{ij} \\ \hline A_{ij} \end{pmatrix} \mid 1 \leq i \leq n-d+1,\ 1 \leq j \leq m \right\}$$

with A_{ij} and E_{ij} as in the statement of the lemma. We let $\mathscr{C}_1$ be the code with basis

$$\left\{ \begin{pmatrix} E_{1j} \\ \hline A_{1j} \end{pmatrix} \mid 1 \leq j \leq m \right\}.$$

It is easy to see that $\mathscr{C}_1$ is (after a suitable embedding) an MRD code in $\mathbb{F}_q^{d\times m}$ with minimum distance d. Furthermore, we have that the code $\mathscr{C}_2$ generated by the basis

$$\left\{ \begin{pmatrix} E_{ij} \\ \hline A_{ij} \end{pmatrix} \mid 2 \leq i \leq n-d+1,\ 1 \leq j \leq m \right\}$$

is (again after embedding) an MRD code in $\mathbb{F}_q^{(n-1)\times m}$, which also has minimum distance d by the second part of Lemma 7.2. It is not hard to see that the mapping $\mathscr{C} \mapsto (\mathscr{C}_1, \mathscr{C}_2)$ is injective, from which we obtain

$$|\{\mathscr{C} \leq \mathbb{F}_q^{n\times m} \mid d(\mathscr{C}) = d,\ \mathscr{C} \text{ is MRD}\}| \leq$$
$$|\{\mathscr{C} \leq \mathbb{F}_q^{d\times m} \mid d(\mathscr{C}) = d,\ \mathscr{C} \text{ is MRD}\}| \cdot |\{\mathscr{C} \leq \mathbb{F}_q^{(n-1)\times m} \mid d(\mathscr{C}) = d,\ \mathscr{C} \text{ is MRD}\}|.$$

Dividing both sides by $A_q(n\times m, d)B_q(n\times m, d)$ yields the desired result. ■

It is well known that the dual of an MRD code in $\mathbb{F}_q^{n\times m}$ of minimum distance d is an MRD code in $\mathbb{F}_q^{n\times m}$ of minimum distance $n-d+2$; see, e.g., [10, Theorem 5.5]. Since the map that sends a code to its dual is a bijection, this simple fact can be rephrased in terms of density functions as follows.

Proposition 7.4. *For all $d \geq 2$ we have*

$$\delta_q(n\times m, m(n-d+1), d) = \delta_q(n\times m, m(d-1), n-d+2).$$

We now combine Propositions 7.3 and 7.4 in order to illustrate how the density functions of MRD codes with different parameters behave with respect to each other.

Corollary 7.5. *For all $d \geq 2$ we have*

$$\delta_q(n\times m, m(n-d+1), d) \leq \delta_q(2\times m, m, 2)^{(n-d+1)(d-1)} \frac{\mathrm{bin}_q(2m,m)^{(n-d+1)(d-1)}}{\mathrm{bin}_q(mn, m(n-d+1))}.$$

Proof. By applying Proposition 7.3 $n-d+1$ times one obtains

$$\delta_q(n\times m, m(n-d+1), d) \leq \delta_q(d\times m, m, d)^{(n-d+1)} \frac{\mathrm{bin}_q(md,m)^{(n-d+1)}}{\mathrm{bin}_q(mn, m(n-d+1))}. \tag{7.2}$$

By applying the same proposition $d-1$ times one obtains

$$\delta_q(d\times m, m(d-1), 2) \leq \delta_q(2\times m, m, 2)^{(d-1)} \frac{\mathrm{bin}_q(2m,m)^{(d-1)}}{\mathrm{bin}_q(md, m(d-1))}. \tag{7.3}$$

Moreover, using Proposition 7.4 we find that $\delta_q(d\times m, m, d) = \delta_q(d\times m, m(d-1), 2)$ which, combined with (7.2) and (7.3), yields the desired result. ■

Remark 7.6. Taking the limit superior in Corollary 7.5 as $q\to+\infty$ and $m\to+\infty$, and combining it with [1, Corollary VII.5], we obtain the same asymptotic bounds for the density of MRD codes as [1, Theorem VII.6]. The q-binomial coefficients can be estimated using (4.1) and (6.2).

Appendix A. Some proofs.

Proof of Lemma 4.9. We establish the two groups of asymptotic estimates separately. Easy computations show that

$$\frac{\nu_q(N,k,\ell)}{q^{k(N-k)}} = \frac{\prod_{i=N-k+1}^{N}\left(1-\frac{1}{q^i}\right) - 2\prod_{i=1}^{k}\left(1-\frac{1}{q^i}\right) + \prod_{i=1}^{N-k-\ell}\left(1-\frac{1}{q^i}\right)\prod_{i=1}^{k}\left(1-\frac{1}{q^i}\right)}{\prod_{i=1}^{k}\left(1-\frac{1}{q^i}\right)}. \tag{A.1}$$

First note that

$$\prod_{i=1}^{k}\left(1-\frac{1}{q^i}\right) \sim 1 \qquad \text{as } q\to+\infty.$$

The different cases are treated separately and for each of them we focus on computing the asymptotics of the numerator of the right-hand side of (A.1).

Case 1. We first assume $\max\{0, N-2k\} \leq \ell < N-k-1$. Note that for $q \to +\infty$ we have

$$\prod_{i=N-k+1}^{N} \left(1-\frac{1}{q^i}\right) = 1 + O\left(\frac{1}{q^3}\right),$$

$$-2\prod_{i=1}^{k} \left(1-\frac{1}{q^i}\right) = -2 + \frac{2}{q} + \frac{2}{q^2} + O\left(\frac{1}{q^3}\right),$$

$$\prod_{i=1}^{N-k-\ell} \left(1-\frac{1}{q^i}\right) \prod_{i=1}^{k} \left(1-\frac{1}{q^i}\right) = 1 - \frac{2}{q} - \frac{1}{q^2} + O\left(\frac{1}{q^3}\right),$$

which all together show that the numerator's asymptotic for $q \to +\infty$ is q^{-2}.

Case 2. Next assume that $\ell = N-k-1 = \max\{0, N-2k\}$. If $k = N-1$ we have

$$\prod_{i=2}^{N} \left(1-\frac{1}{q^i}\right) - \prod_{i=1}^{N-1} \left(1-\frac{1}{q^i}\right) - \frac{1}{q}\prod_{i=1}^{N-1} \left(1-\frac{1}{q^i}\right) = \frac{1}{q^2} + O\left(\frac{1}{q^3}\right) \qquad \text{as } q \to +\infty,$$

since all terms in the expression which are preponderant with respect to q^{-2} vanish. We leave the case $k = 1$ to the reader.

Case 3. Assume that $\ell = N-k-1 > \max\{0, N-2k\}$. The numerator in (A.1) reduces to

$$\prod_{i=N-k+1}^{N} \left(1-\frac{1}{q^i}\right) - \prod_{i=1}^{k} \left(1-\frac{1}{q^i}\right) - \frac{1}{q}\prod_{i=1}^{k} \left(1-\frac{1}{q^i}\right) = \frac{2}{q^2} + O\left(\frac{1}{q^3}\right) \qquad \text{as } q \to +\infty,$$

from which the statement follows.

Case 4. Assume that $\ell = N-k$. By convention (Notation 2.1) we have

$$\prod_{i=1}^{N-k-\ell} \left(1-\frac{1}{q^i}\right) = 1$$

and therefore the numerator of the RHS of (A.1) becomes

$$\prod_{i=N-k+1}^{N} \left(1-\frac{1}{q^i}\right) - \prod_{i=1}^{k} \left(1-\frac{1}{q^i}\right) = \frac{1}{q} + O\left(\frac{1}{q^2}\right) \qquad \text{as } q \to +\infty.$$

The desired estimate follows.

In order to prove the second group of asymptotic estimates, observe first that by Notation 2.1 we have

$$\frac{\nu_q(N,k,N-k)^2}{\mathrm{bin}_q(N,k)} - \nu_q(N,k,\ell) = \frac{q^{2k(N-k)}}{\mathrm{bin}_q(N,k)} - q^{(2k-N+\ell)(N-k)} \prod_{i=\ell}^{N-k-1} (q^{N-k} - q^i).$$

Using the definition of the q-binomial coefficient we find that the above expression reduces to

$$q^{k(N-k)} \frac{\prod_{i=1}^{k}\left(1-\frac{1}{q^i}\right) - \prod_{i=1}^{N-k-\ell}\left(1-\frac{1}{q^i}\right)\prod_{i=N-k+1}^{N}\left(1-\frac{1}{q^i}\right)}{\prod_{i=N-k+1}^{N}\left(1-\frac{1}{q^i}\right)}.$$

The asymptotic estimates can be conveniently derived from this formula, examining the various cases separately. ■

Proof of Lemma 6.5. By (A.1) we have

$$\nu_q(mn, m(n-d+1), mi) = q^{m(n-d+1)m(d-1)}\left(\frac{\prod_{i=m(d-1)+1}^{mn}\left(1-\frac{1}{q^i}\right)}{\prod_{i=1}^{m(n-d+1)}\left(1-\frac{1}{q^i}\right)} - 2 + \prod_{i=1}^{m(d-1-i)}\left(1-\frac{1}{q^i}\right)\right). \tag{A.2}$$

By the definition of $\pi(q)$ from (6.1) we have

$$\frac{\prod_{i=m(d-1)+1}^{mn}\left(1-\frac{1}{q^i}\right)}{\prod_{i=1}^{m(n-d+1)}\left(1-\frac{1}{q^i}\right)} \sim \pi(q) \qquad \text{as } m \to +\infty. \tag{A.3}$$

Furthermore, as $m \to +\infty$, we have

$$\prod_{i=1}^{m(d-1-i)}\left(1-\frac{1}{q^i}\right) \sim \begin{cases} 1 & \text{if } i = d-1, \\ 1/\pi(q) & \text{if } i < d-1. \end{cases} \tag{A.4}$$

Combining (A.2), (A.3), and (A.4) the desired result follows. ■

Acknowledgment. The authors are very grateful to the referees of this paper for their careful reading of the manuscript and suggestions.

REFERENCES

[1] J. Antrobus and H. Gluesing-Luerssen, *Maximal Ferrers diagram codes: Constructions and genericity considerations*, IEEE Trans. Inform. Theory, 65 (2019), pp. 6204–6223.

[2] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, Berlin, 2013.

[3] A. Beutelspacher, *On t-covers in finite projective spaces*, J. Geom., 12 (1979), pp. 10–16.

[4] C. Bey, *Polynomial LYM inequalities*, Combinatorica, 25 (2004), pp. 19–38.

[5] M. Braun, T. Etzion, P. Östergård, A. Vardy, and A. Wassermann, *Existence of q-analogs of Steiner systems*, Forum Math., Pi, 4 (2016), E7.

[6] E. Byrne and A. Ravagnani, *Partition-balanced families of codes and asymptotic enumeration in coding theory*, J. Combin. Theory Ser. A, 171 (2020), 1051690.
[7] H. Crapo and G.-C. Rota, *On the Foundations of Combinatorial Theory: Combinatorial Geometries*, MIT Press, Cambridge, MA, 1970.
[8] B. Csajbók, G. Marino, O. Polverino, and F. Zullo, *Maximum scattered linear sets and MRD codes*, J. Algebraic Combin., 46 (2017), pp. 517–531.
[9] N. G. De Bruijn, *Asymptotic Methods in Analysis*, Dover, New York, 1981.
[10] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, J. Combin. Theory Ser. A, 25 (1978), pp. 226–241.
[11] T. A. Dowling, *Codes, packings and the critical problem*, in Atti del Convegno di Geometria Combinatoria e sue Applicazioni, A. Barlotti, ed., Tipografia Oderisi, Perugia, Italy, 1971, pp. 209–224.
[12] E. M. Gabidulin, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii, 21 (1985), pp. 3–16.
[13] H. Gluesing-Luerssen, *On the sparseness of certain linear MRD codes*, Linear Algebra Appl., 596 (2020), pp. 145–168.
[14] E. Gorla, R. Jurrius, H. H. López, and A. Ravagnani, *Rank-metric codes and q-polymatroids*, J. Algebraic Combin., 52 (2020), pp. 1–19.
[15] J. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, Oxford, 1998.
[16] R. Kötter and F. R. Kschischang, *Coding for errors and erasures in random network coding*, IEEE Trans. Inform. Theory, 54 (2008), pp. 3579–3591.
[17] J. Kung, *Critical Problems*, in Matroid Theory, Contemporary Mathematics 197, J. E. Bonin, ed., American Mathematical Society, Providence, RI, 1996, pp. 1–128.
[18] J. B. Lewis and A. H. Morales, *Rook theory of the finite general linear group*, Exp. Mathematics, 29 (2020), pp. 328–346.
[19] J. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*, Elsevier, Amsterdam, 1977.
[20] A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, and J. Rosenthal, *On the genericity of maximum rank distance and Gabidulin codes*, Des. Codes Cryptogr., 86 (2018), pp. 341–363.
[21] A. Ravagnani, *Whitney numbers of combinatorial geometries and higher-weight Dowling lattices*, SIAM J. Appl. Algebra Geom., to appear.
[22] R. M. Roth, *Maximum-rank array codes and their application to crisscross error correction*, IEEE Trans. Inform. Theory, 37 (1991), pp. 328–336.
[23] K.-U. Schmidt, *Quadratic and symmetric bilinear forms over finite fields and their association schemes*, Algebr. Comb., 3 (2020), pp. 161–189.
[24] J. Sheekey, *New semifields and new MRD codes from skew polynomial rings*, J. Lond. Math. Soc. (2), 101 (2020), pp. 432–456.
[25] D. Silva, F. R. Kschischang, and R. Kötter, *A rank-metric approach to error control in random network coding*, IEEE Trans. Inform. Theory, 54 (2008), pp. 3951–3967.
[26] R. Stanley, *Modular elements of geometric lattices*, Algebra Universalis, 1 (1971), pp. 214–217.
[27] R. Stanley, *Enumerative Combinatorics*, Vol. 1, 2nd ed., Cambridge University Press, Cambridge, 2011.
[28] D. Tingley, *Complements of linear subspaces*, Math. Mag., 64 (1991), pp. 98–103.
[29] T. Zaslavsky, *The Möbius function and the characteristic polynomial*, in Encyclopedia Math. Appl. 29, N. White, ed., Cambridge University Press, Cambridge, 1987, pp. 114–138.