Linear Cutting Blocking Sets and Minimal Codes in the Rank Metric

Gianira Alfarano, Martino Borello, Alessandro Neri, Alberto Ravagnani

Linear Cutting Blocking Sets and Minimal Codes in the Rank Metric

Gianira N. Alfarano*[1], Martino Borello[2], Alessandro Neri[3], and Alberto Ravagnani[4]

[1]Institute of Mathematics, University of Zurich, Switzerland
[2]Université Paris 8, Laboratoire de Géométrie, Analyse et Applications, LAGA, Université Sorbonne Paris Nord, CNRS, UMR 7539, France
[3]Max-Planck-Institute for Mathematics in the Sciences, Leipzig, Germany
[4]Department of Mathematics and Computer Science, Eindhoven University of Technology, the Netherlands

Abstract

This work investigates the structure of rank-metric codes in connection with concepts from finite geometry, most notably the q-analogues of projective systems and blocking sets. We also illustrate how to associate a classical Hamming-metric code to a rank-metric one, in such a way that various rank-metric properties naturally translate into the homonymous Hamming-metric notions under this correspondence. The most interesting applications of our results lie in the theory of minimal rank-metric codes, which we introduce and study from several angles. Our main contributions are bounds for the parameters of a minimal rank-metric codes, a general existence result based on a combinatorial argument, and an explicit code construction for some parameter sets that uses the notion of a scattered linear set. Throughout the paper we also show and comment on curious analogies/divergences between the theories of error-correcting codes in the rank and in the Hamming metric.

1 Introduction

Block codes with the Hamming metric have been extensively (and traditionally) studied in connections with several topics in finite geometry, including arcs, blocking sets, and modular curves to mention a few; see [13, 14, 21] among many others. In the last decade, especially thanks to the advent of network coding [1, 27, 28, 42], the novel class of rank-metric codes has been the subject of intense mathematical research. Interesting progress has been recently made in the attempt of understanding the connection between rank-metric codes and finite geometry [36], yet this link is still not fully understood and rather unexplored. This paper contributes to fill in this important gap.

The starting point of our investigation is a connection between rank-metric codes and the q-analogues of projective systems. This link has been observed already in [36], whose contributions we survey with short proofs and extend. Among the various new results, we show that the maximum rank of a nondegenerate rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is $\min\{m, n\}$, a quite simple property that nonetheless has interesting consequences in the theory of anticodes and minimal rank-metric codes (see below).

We then apply the theory of q-systems to show how one can associate a Hamming-metric code to a given rank-metric code. This correspondence translates various properties of a rank-metric codes into the homonymous properties in the Hamming metric. In particular, the Hamming-metric code associated to the simplex rank-metric code is (essentially) the classical simplex code.

*Gianira N. Alfarano is supported by the Swiss National Science Foundation through grant no. 188430.

The interplay between the rank and the Hamming metric also motivates us to investigate one of the best-known parameters of a code, namely, its *total weight*. We identify a suitable rank-metric analogue of the total Hamming weight of a code and show that it has a constant value for all nondegenerate rank-metric codes with the same dimension and length. We then compute its asymptotic behaviour as the field size q tends to infinity, as well as the asymptotic behaviour of its variance under certain assumptions. This illustrates the general behaviour of these parameters over large finite fields.

Several applications of the above-mentioned results and concepts can be seen in theory of minimal rank-metric codes, a research line which is seemingly unexplored. We call a rank-metric code *minimal* if all its codewords have minimal *rank support*. Minimal rank-metric codes are the natural analogues (in the rank-metric) of minimal Hamming-metric codes, a class of objects that have been extensively studied in connection with finite geometry; see e.g. [2,10,43].

The stepping stone in our approach is a characterization of minimal rank-metric codes via q-systems. The correspondence described above between rank-metric codes and these geometric/combinatorial structures induces a correspondence between minimal rank-metric codes and *linear cutting blocking sets*. The latter concept can be regarded as the q-analogue of the classical notion of a *cutting blocking set*.

The description of minimal rank-metric codes via the q-analogues of cutting blocking sets allows us to establish a lower bound for their length. More precisely, we find that a minimal rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k must satisfy

$$n \geq k + m - 1. \tag{1.1}$$

We also show that a nondegenerate rank-metric code is minimal if and only if the associated Hamming-metric code is minimal (under the correspondence described earlier). This result naturally connects the theories of minimal codes in the two metrics and makes it possible to transfer/compare results across them.

A major, rather curious difference between minimal codes in the rank and in the Hamming metric appears to be in the role played by the field size q with respect to bounds and existence results. While in the Hamming metric the field size q is a crucial parameter (e.g., minimal codes do not exist for lengths that are too small compared to a suitable multiple of the field size), most of the bounds and existence results we derive for minimal rank-metric codes do not depend on q, even when this quantity explicitly shows up in the computations. We will elaborate more on this later in the paper.

Our main contributions to the theory of minimal codes in the rank metric lies in existence results and constructions, which we now describe very briefly. We start by giving simple examples of minimal rank-metric codes (the simplex rank-metric code and nondegenerate codes of very large length). Next, we propose a general construction of 3-dimensional minimal rank-metric codes based on the theory of scattered linear sets. The construction also proves that our lower bound for the length of a minimal rank-metric code is sharp for some (infinite) parameter sets. We then establish a general existence result for minimal rank-metric codes based on a combinatorial argument. More precisely, we show that a minimal rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension $k \geq 2$ exists whenever $m \geq 2$ and

$$n \geq 2k + m - 2. \tag{1.2}$$

Comparing (1.1) with (1.2) we see that, in general, the existence of minimal rank-metric codes remains an open question only for $k - 1$ values of n (for any fixed m, k and q).

We conclude the paper by introducing a structural quantity of a q-system, which we call its *linearity index*. This allows us to attach a new parameter to a rank-metric code $\mathcal{C}$ via its associated q-system. We investigate which structural properties of a rank-metric code are captured by its linearity index, showing also a connection with the theory of generalized rank weights. Finally, we apply these concept to describe further minimal codes in the rank metric.

Outline. The remainder of the paper is organized as follows. Section 2 contains the preliminaries on rank-metric code, Hamming-metric codes and (cutting) blocking sets. In Section 3 we describe the geometric structure of rank-metric codes via the theory of q-systems. In particular, we study simplex rank-metric codes. Section 4 illustrates how to associate a Hamming-metric code to a rank-metric code and how code properties behave under this correspondence. Sections 5 and 6 are entirely devoted to the study of minimal codes in the rank metric: geometric structure, properties, constructions and existence. Finally, the Appendix contains some technical proofs.

2 Preliminaries

2.1 Rank-Metric Codes

Throughout this paper, q denotes a prime power and n, m are positive integers. We start by introducing the main object studied in this work, namely, rank-metric codes.

For a vector $v \in \mathbb{F}_{q^m}^n$ and an ordered basis $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ of the field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$, let $\Gamma(v) \in \mathbb{F}_q^{n\times m}$ be the matrix defined by

$$v_i = \sum_{j=1}^{m} \Gamma(v)_{ij}\gamma_j.$$

Note that $\Gamma(v)$ is constructed by simply transposing v and then expanding each entry over the basis Γ. The **Γ-support** of a vector $v \in \mathbb{F}_{q^m}^n$ is the column space of $\Gamma(v)$. It is denoted by $\sigma_\Gamma(v) \subseteq \mathbb{F}_q^n$. The following result can be obtained by a standard linear algebra argument.

Proposition 2.1. Let $v \in \mathbb{F}_{q^m}^n$.

1. We have $\sigma_\Gamma(v) = \sigma_\Gamma(\alpha v)$ for all nonzero $\alpha \in \mathbb{F}_{q^m}$ and all bases Γ.
2. The Γ-support of v does not depend on the choice of the basis Γ.
3. For all matrices $A \in \mathbb{F}_q^{n\times n}$ we have $\Gamma(vA) = A^\top\Gamma(v)$.

Definition 2.2. In the sequel, for $v \in \mathbb{F}_{q^m}^n$ we let $\sigma^{\mathrm{rk}}(v) := \sigma_\Gamma(v)$ be the (**rank**) **support** of v, where Γ is *any* basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$. The support is well-defined by Proposition 2.1. The **rank** (**weight**) of a vector v is the $\mathbb{F}_q$-dimension of its support, denoted by $\mathrm{rk}(v)$.

Rank-metric codes and their fundamental parameters are defined as follows. In this paper, we follow [20] and only concentrate on rank-metric codes that are linear over $\mathbb{F}_{q^m}$.

Definition 2.3. A (**rank-metric**) **code** is an $\mathbb{F}_{q^m}$-linear subspace $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. Its elements are called **codewords**. The integer n is the **length** of the code. The **dimension** of $\mathcal{C}$ is the dimension as an $\mathbb{F}_{q^m}$-vector space and the **minimum** (**rank**) **distance** of a nonzero code $\mathcal{C}$ is

$$d^{\mathrm{rk}}(\mathcal{C}) := \min\{\mathrm{rk}(v) \,:\, v \in \mathcal{C},\, v \neq 0\}.$$

We also define the minimum distance of the zero code to be $n + 1$. We say that $\mathcal{C}$ is an $[n, k, d]_{q^m/q}$ code if it has length n, dimension k and minimum distance d. When the minimum distance is not known or is irrelevant, we write $[n, k]_{q^m/q}$. A **generator matrix** of an $[n, k]_{q^m/q}$ code is a matrix $G \in \mathbb{F}_{q^m}^{k\times n}$ whose rows generate $\mathcal{C}$ as an $\mathbb{F}_{q^m}$-linear space. Finally, the (**rank**) **support** of an $\mathbb{F}_{q^m}$-linear rank-metric code $\mathcal{C}$ is the sum of the supports of its codewords, i.e.,

$$\sigma^{\mathrm{rk}}(\mathcal{C}) = \sum_{v\in\mathcal{C}} \sigma^{\mathrm{rk}}(v).$$

The support of a rank-metric codes is determined by the supports of any set of generators, as the following simple result shows.

Proposition 2.4. For every $v, w \in \mathbb{F}_{q^m}^n$, we have $\sigma^{\mathrm{rk}}(v+w) \subseteq \sigma^{\mathrm{rk}}(v) + \sigma^{\mathrm{rk}}(w)$. Moreover, if $\mathcal{C} = \langle c_1, \dots c_t \rangle_{\mathbb{F}_{q^m}} \subseteq \mathbb{F}_{q^m}^n$ is a rank-metric code, then $\sigma^{\mathrm{rk}}(\mathcal{C}) = \sigma^{\mathrm{rk}}(c_1) + \cdots + \sigma^{\mathrm{rk}}(c_t)$.

Recall that a (**linear**, **rank-metric**) **isometry** of $\mathbb{F}_{q^m}^n$ is an $\mathbb{F}_{q^m}$-linear automorphism φ of $\mathbb{F}_{q^m}^n$ that preserves the rank weight, i.e., such that $\mathrm{rk}(v) = \mathrm{rk}(\varphi(v))$ for all $v \in \mathbb{F}_{q^m}^n$. It is known that the isometry group of $\mathbb{F}_{q^m}^n$, say $\mathcal{G}(q,m,n)$, is generated by the (nonzero) scalar multiplications of $\mathbb{F}_{q^m}$ and the linear group $\mathrm{GL}_n(q)$; see e.g. [8]. More precisely, $\mathcal{G}(q,m,n) \cong \mathbb{F}_{q^m}^* \times \mathrm{GL}_n(q)$, which (right-)acts on $\mathbb{F}_{q^m}^n$ via

$$\begin{array}{rcl} (\mathbb{F}_{q^m}^* \times \mathrm{GL}_n(q)) \times \mathbb{F}_{q^m}^n & \longrightarrow & \mathbb{F}_{q^m}^n \\ ((\alpha, A), v) & \longmapsto & \alpha v A. \end{array}$$

Definition 2.5. Rank-metric codes $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_{q^m}^n$ are (**linearly**) **equivalent** if there exists $\varphi \in \mathcal{G}(q,m,n)$ such that $\mathcal{C}' = \varphi(\mathcal{C})$.

Observe that, by $\mathbb{F}_{q^m}$-linearity, when studying linear equivalence of $[n,k]_{q^m/q}$ codes the action of $\mathbb{F}_{q^m}^*$ is trivial. In particular, $[n,k]_{q^m/q}$ codes $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if and only if there exists $A \in \mathrm{GL}_n(q)$ such that

$$\mathcal{C}' = \mathcal{C} \cdot A := \{vA \,:\, v \in \mathcal{C}\}.$$

We conclude this section with the definition of dual code, which we will use often throughout the paper.

Definition 2.6. The **dual** of a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is the rank-metric code

$$\mathcal{C}^\perp = \{v \in \mathbb{F}_{q^m}^n \,:\, u \cdot v^\top = 0 \text{ for all } u \in \mathcal{C}\} \subseteq \mathbb{F}_{q^m}^n.$$

Recall moreover that $\dim_{\mathbb{F}_{q^m}}(\mathcal{C}) + \dim_{\mathbb{F}_{q^m}}(\mathcal{C}^\perp) = n$ for all rank-metric codes $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. There are several relations between a code and its dual, the most elegant of which are probably the MacWilliams(-type) identities. These were established by Delsarte in [18] for $\mathbb{F}_q$-linear rank-metric codes endowed with the trace product. A simpler proof and their connection with the theory of $\mathbb{F}_{q^m}$-linear rank-metric codes considered here can be found in [38].

2.2 Hamming-Metric Codes

In this paper, we will often consider codes endowed with the Hamming metric and compare their behaviour with that of rank-metric codes with respect to several properties. We therefore briefly recall some classical notions from coding theory. For more details the reader is referred to [25, 44].

Definition 2.7. The (**Hamming**) **support** of a vector $v \in \mathbb{F}_q^n$ is $\sigma^{\mathrm{H}}(v) = \{i \,:\, v_i \neq 0\} \subseteq \{1, \dots, n\}$ and its **Hamming weight** is $\omega^{\mathrm{H}}(v) = |\sigma^{\mathrm{H}}(v)|$.

An $[n,k]_q$ **Hamming-metric code** $\mathcal{C}$ is an $\mathbb{F}_q$-linear subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k. The **minimum distance** of $\mathcal{C}$ is the integer $d^{\mathrm{H}}(\mathcal{C}) = \min\{\omega^{\mathrm{H}}(c) \,:\, c \in \mathcal{C},\, c \neq 0\}$. If $d = d^{\mathrm{H}}(\mathcal{C})$ is known, we say that $\mathcal{C}$ is an $[n,k,d]_q$ code. A **generator matrix** of $\mathcal{C}$ is a matrix $G \in \mathbb{F}_q^{k \times n}$ whose rows generate $\mathcal{C}$ as an $\mathbb{F}_q$-linear space. Finally, we say that $\mathcal{C}$ and $\mathcal{C}'$ are (**monomially**) **equivalent** if there exists an $\mathbb{F}_q$-linear isometry $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ with $f(\mathcal{C}) = \mathcal{C}'$.

Recall that the **Hamming support** $\sigma^{\mathrm{H}}(\mathcal{C})$ of a code $\mathcal{C}$ is the union of the supports of its codewords. The code $\mathcal{C}$ is called **Hamming-nondegenerate** if $\sigma^{\mathrm{H}}(\mathcal{C}) = \{1, \dots, n\}$ and **Hamming-degenerate** otherwise.

There is a well-known geometric interpretation of codes endowed with the Hamming metric. To describe it, we recall the following setting. The projective geometry $\mathrm{PG}(k-1,q)$ with underlying vector space $\mathbb{F}_q^k$ is defined as

$$\mathrm{PG}(k-1,q) := \left(\mathbb{F}_q^k \setminus \{0\}\right)/\!\sim,$$

where $\sim$ denotes the proportionality relation, i.e., $u \sim v$ if and only if $u = \lambda v$ for some nonzero element $\lambda \in \mathbb{F}_q$.

Definition 2.8. A **projective** $[n,k,d]_q$ **system** $(\mathcal{P}, \mathrm{m})$ is a finite multiset, where $\mathcal{P} \subseteq \mathrm{PG}(k-1,q)$ is a set of points that do not all lie on a hyperplane, and $\mathrm{m} : \mathrm{PG}(k-1,q) \to \mathbb{N}$ is the multiplicity function, with $\mathrm{m}(P) > 0$ if and only if $P \in \mathcal{P}$ and $\sum_{P\in\mathcal{P}} \mathrm{m}(P) = n$. The parameter d is defined as

$$d = n - \max\left\{ \sum_{P\in H} \mathrm{m}(P) \,:\, H \subseteq \mathrm{PG}(k-1,q),\ \dim(H) = k-2 \right\}.$$

Projective $[n,k,d]_q$ systems $(\mathcal{P}, \mathrm{m})$ and $(\mathcal{P}', \mathrm{m}')$ are **equivalent** if there exists a projective isomorphism $\phi \in \mathrm{PGL}(k,q)$ mapping $\mathcal{P}$ to $\mathcal{P}'$ that preserves the multiplicities of the points, i.e., such that $\mathrm{m}(P) = \mathrm{m}'(\phi(P))$ for every $P \in \mathrm{PG}(k-1,q)$.

There exists a 1-to-1 correspondence between (monomial) equivalence classes of $[n,k,d]_q$ Hamming-nondegenerate codes and equivalence classes of projective $[n,k,d]_q$ systems; see e.g. [44, Theorem 1.1.6]. The correspondence can be formalized by two maps

$$\begin{aligned} \Phi^{\mathrm{H}} : C[n,k,d]_q &\longrightarrow \mathcal{P}[n,k,d]_q, \\ \Psi^{\mathrm{H}} : \mathcal{P}[n,k,d]_q &\longrightarrow C[n,k,d]_q, \end{aligned}$$

which are the inverse of each other. For a given equivalence class $[C]$ of nondegenerate $[n,k,d]_q$ codes, choose a generator matrix $G \in \mathbb{F}_q^{k\times n}$ of one of the codes in $[C]$. Let $g_1, \ldots, g_n$ be the columns of G and take the set $\mathcal{P} = \{[g_1], \ldots, [g_n]\} \subseteq \mathrm{PG}(k-1,q)$. Moreover, define the multiplicity function m as

$$\mathrm{m}(P) = |\{i \,:\, P = [g_i]\}|.$$

Then, the map Φ^{H} is defined to be $\Phi^{\mathrm{H}}([C]) = [(\mathcal{P}, \mathrm{m})]$. On the other hand, for a given equivalence class $[(\mathcal{P}, \mathrm{m})]$ of projective $[n,k,d]_q$ systems, we construct a matrix G by taking as columns representatives of the points P_i's in $\mathcal{P}$, each counted with multiplicity $\mathrm{m}(P_i)$. We then set $\Psi^{\mathrm{H}}([\mathcal{P}, \mathrm{m}]) = [\mathrm{rowsp}(G)]$.

Definition 2.9. Let $\mathcal{C}$ be an $[n,k]_q$ code. A codeword $c \in \mathcal{C}$ is **Hamming-minimal** if every nonzero codeword c' with $\sigma^{\mathrm{H}}(c') \subseteq \sigma^{\mathrm{H}}(c)$ is a multiple of c. A code is **Hamming-minimal** if all its codewords are Hamming-minimal.

Minimal codes in the Hamming metric have been extensively studied not only for their applications to secret sharing schemes [33], but also for their geometric and combinatorial properties. We recall the following definition.

Definition 2.10. A t**-fold blocking set** in $\mathrm{PG}(k-1,q)$ is a set $\mathcal{P} \subseteq \mathrm{PG}(k-1,q)$ such that for every hyperplane H of $\mathrm{PG}(k-1,q)$ we have $|H \cap \mathcal{P}| \geq t$. When $t = 1$ we call $\mathcal{P}$ a **blocking set**. A blocking set $\mathcal{P}$ is called **cutting** if for every hyperplane H of $\mathrm{PG}(k-1,q)$ we have $\langle \mathcal{P} \cap H \rangle = H$.

Cutting blocking sets have been introduced in connection to minimal codes in [10]. However, the same objects were already known under different names and analyzed under different point of view. In [16], they were called *strong blocking sets* and used for constructing saturating sets

in projective spaces over finite fields. Moreover, they were also known as *generator sets* and constructed as union of disjoint lines in [19].

The following result relates cutting blocking sets and Hamming-minimal codes and can be found in [2, 43].

Theorem 2.11. The maps Ψ^{H} and Φ^{H} define a 1-to-1 correspondence between equivalence classes of cutting blocking sets and equivalence classes of nondegenerate Hamming-minimal codes.

3 The Geometry of Rank-Metric Codes

In this section we study the geometric structure of rank-metric codes and their connection with the theory of q-systems, introducing fundamental tools that will be needed later. We also describe one-weight and simplex codes in the rank metric.

Although most of the results contained in this section have already appeared in [40] and [36], we are not aware of any organic survey of the topic, which we offer here. For convenience of the reader, we include concise proofs and state results in the form that will be needed in later sections of the paper.

3.1 Geometric Characterization of Rank-Metric Codes

We start by introducing the natural analogue of the notion of "nondegenerate" code in the rank-metric setting.

Definition 3.1. An $[n,k]_{q^m/q}$ rank-metric code $\mathcal{C}$ is (**rank-**)**nondegenerate** if $\sigma^{\mathrm{rk}}(\mathcal{C}) = \mathbb{F}_q^n$. We say that $\mathcal{C}$ is (**rank-**)**degenerate** if it is not nondegenerate. Moreover, we call $\dim(\sigma^{\mathrm{rk}}(\mathcal{C}))$ the **effective length** of the code $\mathcal{C}$.

Proposition 3.2. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a rank-metric code. The following are equivalent.

1. $\mathcal{C}$ is rank-nondegenerate.
2. For every $A \in \mathrm{GL}_n(q)$, the code $\mathcal{C} \cdot A$ is Hamming-nondegenerate.
3. The $\mathbb{F}_q$-span of the columns of any generator matrix of G has $\mathbb{F}_q$-dimension n.
4. $d^{\mathrm{rk}}(\mathcal{C}^\perp) \geq 2$.

Proof. (1) $\Rightarrow$ (2): Assume that $\mathcal{C} \cdot A$ is Hamming-degenerate for some $A \in \mathrm{GL}_n(q)$. Then there exists $1 \leq i \leq n$ with $(vA)_i = 0$ for all $v \in \mathcal{C}$. In particular, $\sigma^{\mathrm{rk}}(vA) \subseteq V := \langle e_j : j \neq i \rangle$. Using Proposition 2.1, we see that $\sigma^{\mathrm{rk}}(\mathcal{C})$ is contained in an $(n-1)$-dimensional subspace of $\mathbb{F}_q^n$, hence $\mathcal{C}$ is rank-degenerate.

(2) $\Rightarrow$ (4): Let $\Gamma := \{\gamma_1, \ldots, \gamma_m\}$ be an $\mathbb{F}_{q^m}/\mathbb{F}_q$ basis. If $d(\mathcal{C}^\perp) = 1$, then there exists $v \in \mathcal{C}^\perp$ with $\mathrm{rk}(\Gamma(v)) = 1$. Therefore there exists $A \in \mathrm{GL}_n(q)$ with $v = (0, \ldots, 0, 1) \in (\mathcal{C} \cdot A)^\perp$. Thus $\mathcal{C} \cdot A$ is Hamming-degenerate code.

(4) $\Rightarrow$ (1): A rank-degenerate code $\mathcal{C}$ is equivalent to a code $\mathcal{C} \cdot A$ in which all codewords have a 0 in the last component. Hence $(0, \ldots, 0, 1) \in (\mathcal{C} \cdot A)^\perp$ and $d(\mathcal{C}^\perp) = 1$.

(2) $\Rightarrow$ (3): Let G be a generator matrix of $\mathcal{C}$. Since $\mathcal{C} \cdot A$ is Hamming-nondegenerate for any $A \in \mathrm{GL}_n(q)$, the columns of G are linearly independent over $\mathbb{F}_q$. This implies that $n = \dim(\sigma^{\mathrm{rk}}(\mathcal{C}))$ is equal to the dimension of the $\mathbb{F}_q$-space of the columns of G.

(3) $\Rightarrow$ (1): This immediately follows from the definition of rank-nondegenerate code. □

Remark 3.3. By Proposition 3.2, a degenerate code can be isometrically embedded in $\mathbb{F}_{q^m}^{n'}$, where $n' = \dim(\sigma^{\mathrm{rk}}(\mathcal{C}))$.

The following result shows that the parameters of a nondegenerate code must obey certain constraints.

Proposition 3.4. (see [26, Corollary 6.5]) Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ nondegenerate rank-metric code. Then $n \leq km$.

Proof. Let $\{c_1, \ldots, c_k\}$ be a set of generators for $\mathcal{C}$. Then, by Proposition 2.4, $\sigma^{\mathrm{rk}}(\mathcal{C})$ is generated by $\sigma^{\mathrm{rk}}(c_i)$ for $i = 1, \ldots, k$. Since $\dim(\sigma^{\mathrm{rk}}(c_i)) \leq m$ for all i and $\sigma^{\mathrm{rk}}(\mathcal{C}) = \mathbb{F}_q^n$, we conclude that $n \leq km$. □

Our next move is to identify geometric objects able to capture the structure of rank-metric codes. We re-formulate the definition of q-analogue of a projective system proposed in [36] as follows.

Definition 3.5. An $[n,k,d]_{q^m/q}$ **system** is an n-dimensional $\mathbb{F}_q$-space $\mathcal{U} \subseteq \mathbb{F}_{q^m}^k$ with the properties that $\langle \mathcal{U} \rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^k$ and

$$d = n - \max\left\{\dim_{\mathbb{F}_q}(\mathcal{U} \cap H) \,:\, H \text{ is an } \mathbb{F}_{q^m}\text{-hyperplane of } \mathbb{F}_{q^m}^k\right\}. \tag{3.1}$$

Note that (3.1) can be re-written as

$$\min\left\{\dim_{\mathbb{F}_q}(\mathcal{U} + H) \,:\, H \text{ is an } \mathbb{F}_{q^m}\text{-hyperplane in } \mathbb{F}_{q^m}^k\right\} - m(k-1).$$

When the parameters are not relevant, we simply call such an object a **q-system**.

Two $[n,k]_{q^m/q}$ systems $\mathcal{U}, \mathcal{V}$ are said to be **equivalent** if there exists an $\mathbb{F}_{q^m}$-isomorphism $\phi : \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}^k$ such that $\phi(\mathcal{U}) = \mathcal{V}$.

The following simple result is a geometric formulation of one of the *Standard Equations* (stated in our context), which will be of great help throughout the paper. Recall that for integers $a \geq b \geq 0$ and a prime power Q, the symbol

$$\begin{bmatrix} a \\ b \end{bmatrix}_Q$$

denotes the number of b-dimensional subspaces of an a-dimensional space over $\mathbb{F}_Q$. This quantity is called a **Gaussian binomial coefficient**.

Lemma 3.6. (The Standard Equations) Let $\mathcal{U}$ be an $[n,k]_{q^m/q}$ system and let Λ_r be the set of all r-dimensional $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}^k$. We have

$$\sum_{H \in \Lambda_r} |H \cap (\mathcal{U} \setminus \{0\})| = (q^n - 1)\begin{bmatrix} k-1 \\ r-1 \end{bmatrix}_{q^m}. \tag{3.2}$$

Proof. Every element in $\mathcal{U} \setminus \{0\}$ belongs to exactly $\begin{bmatrix} k-1 \\ r-1 \end{bmatrix}_{q^m}$ r-dimensional subspaces in Λ_r. Therefore,

$$\sum_{H \in \Lambda_r} |H \cap (\mathcal{U} \setminus \{0\})| = \sum_{u \in \mathcal{U} \setminus \{0\}} |\{H \in \Lambda \,:\, u \in H\}| = (q^n - 1)\begin{bmatrix} k-1 \\ r-1 \end{bmatrix}_{q^m},$$

which is the desired result. □

In the remainder of this section we describe the 1-to-1 correspondence between equivalence classes of nondegenerate $[n,k,d]_{q^m/q}$ codes and equivalence classes of $[n,k,d]_{q^m/q}$ systems. We denote the set of equivalence classes of nondegenerate $[n,k,d]_{q^m/q}$ codes by $\mathcal{C}[n,k,d]_{q^m/q}$, and the set of equivalence classes of $[n,k,d]_{q^m/q}$ systems by $\mathcal{U}[n,k,d]_{q^m/q}$. Next, we define a map

$$\Phi : \mathcal{C}[n,k,d]_{q^m/q} \to \mathcal{U}[n,k,d]_{q^m/q}$$

as follows: Given an equivalence class $[\mathcal{C}] \in \mathcal{C}[n,k,d]_{q^m/q}$, let $\Phi([\mathcal{C}])$ be the equivalence class of the $\mathbb{F}_q$-span of the columns of a generator matrix of $\mathcal{C}$. Vice versa, given an equivalence class $[\mathcal{U}] \in \mathcal{U}[n,k,d]_{q^m/q}$, fix an $\mathbb{F}_q$-basis $\{g_1,\dots,g_n\}$ of $\mathcal{U}$ and let $\Psi([\mathcal{U}])$ be the equivalence class of the code generated by the matrix having the g_i's as columns. In Theorem 3.8 we will show that Φ and Ψ are the inverse of each other.

We recall that the minimum rank distance of a code $\mathcal{C}$ coincides with the minimum $\mathbb{F}_q$-dimension of the linear space generated over $\mathbb{F}_q$ by the entries of $v \in \mathcal{C}$. In particular, $d^{\mathrm{rk}}(\mathcal{C}) \leq d^{\mathrm{H}}(\mathcal{C})$. More precisely, the rank of a vector can be rewritten as

$$\mathrm{rk}(v) = \min\{\omega^{\mathrm{H}}(vA) \,:\, A \in \mathrm{GL}_n(q)\}. \tag{3.3}$$

We will also repeatedly use the following simple fact: Let $V, H \subseteq W$ be nonzero finite dimensional vector spaces over $\mathbb{F}_q$ and let $\mathcal{B}$ be the set of $\mathbb{F}_q$-bases of V; then

$$\max\{|B \cap H| \,:\, B \in \mathcal{B}\} = \dim(V \cap H). \tag{3.4}$$

Finally, we will often use the following characterization of the rank of a vector.

Lemma 3.7. Let $\mathcal{C}$ be a nondegenerate $[n,k]_{q^m/q}$ code and let G be a generator matrix of $\mathcal{C}$. For any nonzero $v \in \mathbb{F}_{q^m}^k$ we have

$$\mathrm{rk}(vG) = n - \dim_{\mathbb{F}_q}(\mathcal{U} \cap \langle v\rangle^{\perp}), \tag{3.5}$$

where $\mathcal{U}$ is the $[n,k]_{q^m/q}$ system generated by the $\mathbb{F}_q$-span of the columns of G.

Proof. Using (3.3) we see that for all nonzero $v \in \mathbb{F}_{q^m}^k$ we have

$$\mathrm{rk}(vG) = \min\{\omega^{\mathrm{H}}(vGA) \,:\, A \in \mathrm{GL}_n(q)\} = \min\{n - |\{i \,:\, (GA)_i \in \langle v\rangle^{\perp}\}|\},$$

where $(GA)_i$ is the i-th column of GA and $\langle v\rangle^{\perp}$ is the dual of the 1-dimensional code generated by v. As A ranges over $\mathrm{GL}_n(q)$, the columns of GA range over all bases of $\mathcal{U}$. Therefore we conclude by the identity in (3.4). □

The following result has already been shown in [36]. We include a complete proof in the Appendix.

Theorem 3.8. The maps Φ and Ψ are well-defined and are the inverse of each other. In particular, they give a 1-to-1 correspondence between equivalence classes of nondegenerate $[n,k,d]_{q^m/q}$ rank-metric codes and equivalence classes of $[n,k,d]_{q^m/q}$ systems.

We also observe that combining Lemma 3.7 with Remark 3.3 one obtains the following lower bound for the minimum distance of a rank-metric code.

Corollary 3.9. Let $\mathcal{C}$ be an $[n,k,d]_{q^m/q}$ code. Then

$$d \geq \dim_{\mathbb{F}_q}(\sigma^{\mathrm{rk}}(\mathcal{C})) - (k-1)m.$$

As an application of Theorem 3.8, we show that a nondegenerate rank-metric code always have a codeword of rank $\min\{n,m\}$. Note that this the largest possible rank a codeword can possibly have.

Notation 3.10. We denote by $w^{\mathrm{rk}}(\mathcal{C})$ the maximum rank of the codewords of a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$.

Proposition 3.11. Let $\mathcal{C}$ be a nondegenerate $[n,k]_{q^m/q}$ code, then $w^{\mathrm{rk}}(\mathcal{C}) = \min\{n,m\}$. In particular, if $n = m$ then an $[n,k]_{q^n/q}$ code is nondegenerate if and only if $w^{\mathrm{rk}}(\mathcal{C}) = n$.

Proof. If $w^{\mathrm{rk}}(\mathcal{C}) = n$ then the statement is trivially true, so we may assume that $w^{\mathrm{rk}}(\mathcal{C}) < n$. Let $\mathcal{U}$ be any $[n,k]_{q^m/q}$ system associated with $\mathcal{C}$ via Theorem 3.8. By Lemma 3.7 we have that $\dim(H \cap \mathcal{U}) \geq n - w^{\mathrm{rk}}(\mathcal{C})$ for each $\mathbb{F}_{q^m}$-hyperplane H of $\mathbb{F}_{q^m}^k$. Denote by Λ the set of all $\mathbb{F}_{q^m}$-hyperplanes of $\mathbb{F}_{q^m}^k$. Then we have

$$(q^n-1)\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_{q^m} = \sum_{H \in \Lambda} |H \cap (\mathcal{U} \setminus \{0\})| \geq (q^{n-w^{\mathrm{rk}}(\mathcal{C})}-1)\begin{bmatrix} k \\ 1 \end{bmatrix}_{q^m},$$

where the first equality follows from Lemma 3.6. The above inequality is equivalent to

$$(q^n-1)(q^{(k-1)m}-1) \geq (q^{n-w^{\mathrm{rk}}(\mathcal{C})}-1)(q^{km}-1).$$

Dividing both sides by $(q^{(k-1)m}-1)$, we obtain

$$\begin{aligned} q^n - 1 &\geq (q^{n-w^{\mathrm{rk}}(\mathcal{C})}-1)\left(q^m + \frac{q^m-1}{q^{(k-1)m}-1}\right) \\ &= q^{n+m-w^{\mathrm{rk}}(\mathcal{C})} - q^m + \frac{(q^{n-w^{\mathrm{rk}}(\mathcal{C})}-1)(q^m-1)}{q^{(k-1)m}-1} \\ &\geq q^{n+m-w^{\mathrm{rk}}(\mathcal{C})} - q^m. \end{aligned}$$

Since $n - w^{\mathrm{rk}}(\mathcal{C}) \geq 1$, this implies $m \leq w^{\mathrm{rk}}(\mathcal{C})$. Since, clearly, $w^{\mathrm{rk}}(\mathcal{C}) \leq m$, then they must be equal. □

As an application of Proposition 3.11, we recover the characterization of optimal $\mathbb{F}_{q^m}$-linear anticodes given in [37, Theorem 18] with a new and concise proof.

Corollary 3.12. Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code with $k = w^{\mathrm{rk}}(\mathcal{C})$. If $m \geq n$, then $\mathcal{C}$ has a basis made of vectors with entries in $\mathbb{F}_q$.

Proof. We prove the result by induction on $n-k$. The case $n = k$ is immediate. Now assume that $n \geq k+1$ and that $\mathcal{C}$ has $k = w^{\mathrm{rk}}(\mathcal{C})$. Fix a generator matrix G for $\mathcal{C}$. Since $k < n$, by Proposition 3.11 there exists $A \in \mathrm{GL}_n(q)$ such that the last column of $G \cdot A$ is zero. Denote by G' the matrix obtained from $G \cdot A$ by deleting its last column. The code generated by G' has $k = w^{\mathrm{rk}}(\mathcal{C})$ and therefore, by the induction hypothesis, has a basis made of vectors with entries in $\mathbb{F}_q$. This means that there exists $B \in \mathrm{GL}_k(q)$ such that BG' (and thus BGA) has entries in $\mathbb{F}_q$. Therefore $BG = BGAA^{-1}$ has entries in $\mathbb{F}_q$ as well. □

We conclude this subsection by surveying the connection between the generalized rank weights of an $[n,k]_{q^m/q}$ rank-metric code and any corresponding $[n,k]_{q^m/q}$ system. The definitions given here are equivalent to those of [36]. We denote the set of Frobenius-closed subspaces of $\mathbb{F}_{q^m}^n$ by $\Lambda_q(n,m)$, that is,

$$\Lambda_q(n,m) := \left\{\mathcal{V} \leq \mathbb{F}_{q^m}^n \,:\, \theta(\mathcal{V}) = \mathcal{V}\right\},$$

where $\theta : x \longmapsto x^q$ is the q-Frobenius automorphism in $\mathbb{F}_{q^m}$ (extended component-wise to vectors). It is known that $\Lambda_q(n,m)$ corresponds to the set of subspaces of $\mathbb{F}_{q^m}^n$ that have a basis of vectors in $\mathbb{F}_q^n$; see [22, Theorem 1].

Definition 3.13. Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code. For every $r = 1, \ldots, k$, the **r-th generalized rank weight** of $\mathcal{C}$ is the integer

$$d_r^{\mathrm{rk}}(\mathcal{C}) := \min\left\{\dim(\mathcal{V}) \,:\, \mathcal{V} \in \Lambda_q(n,m),\ \dim(\mathcal{V} \cap \mathcal{C}) \geq r\right\}.$$

The following result was shown in [36]. We state it here for completeness and give a proof in the Appendix.

Theorem 3.14. Let $\mathcal{C}$ be an $[n,k,d]_{q^m/q}$ nondegenerate code and let $\mathcal{U}$ be any $[n,k,d]_{q^m/q}$ system associated to $\mathcal{C}$. For any $r=1,\dots,k$ the r-th generalized rank weight is given by

$$\begin{aligned} d_r^{\mathrm{rk}}(C) &= n - \max\left\{\dim_{\mathbb{F}_q}(\mathcal{U}\cap H) \,:\, H \text{ is an } \mathbb{F}_{q^m}\text{-subspace of codim. } r \text{ of } \mathbb{F}_{q^m}^k\right\} \\ &= \min\left\{\dim_{\mathbb{F}_q}(\mathcal{U}+H) \,:\, H \text{ is an } \mathbb{F}_{q^m}\text{-subspace of codim. } r \text{ of } \mathbb{F}_{q^m}^k\right\} - m(k-r). \end{aligned}$$

In particular, the minimum rank distance of $\mathcal{C}$ is given by

$$d = n - \max\{\dim_{\mathbb{F}_q}(\mathcal{U}\cap H) \,:\, H \text{ is an } \mathbb{F}_{q^m}\text{-hyperplane of } \mathbb{F}_{q^m}^k\}.$$

3.2 Simplex and One-Weight Codes in the Rank Metric

In this subsection we use the geometric approach on rank-metric codes to define simplex codes as the natural counterpart of simplex Hamming-metric codes. In particular, this allows to characterize one-weight codes in the rank metric, recovering the results of [36] in this context.

Lemma 3.15. Let a,b,c,d be positive integers such that $a\le b$ and $c\le d$, and let $t\ge 2$ be an integer. Suppose that $(t^a-1)(t^b-1)=(t^c-1)(t^d-1)$. Then $a=c$ and $b=d$.

Proof. By contradiciton, assume that $(a,b)\neq(c,d)$. Moreover, without loss of generality we can assume $a\le c$. Since $(a,b)\neq(c,d)$, then we need to have $a<c\le d$ (if $a=c$ clearly also $b=d$). Moreover, we also have that $b>a$, otherwise the equality is not possible. By expanding the equality $(t^a-1)(t^b-1)-(t^c-1)(t^d-1)=0$, and dividing by t^a, we get

$$t^b - t^{b-a} - t^{c+d-a} + t^{c-a} + t^{d-a} - 1 = 0.$$

All the exponents of t appearing above are positive integers, hence we get a contradiction, since the left hand side is equal to $-1 \mod t$. □

Proposition 3.16. Let $k\ge 2$, let $\mathcal{C}$ be a $[km,k]_{q^m/q}$ code, and let G be a generator matrix of $\mathcal{C}$. The following are equivalent.

1. $\mathcal{C}$ is nondegenerate.
2. The $\mathbb{F}_q$-span of the columns of G is $\mathbb{F}_{q^m}^k$.
3. $\mathcal{C}$ is a one-weight code (with minimum distance m).
4. $d^{\mathrm{rk}}(\mathcal{C}^\perp)>1$.
5. $d^{\mathrm{rk}}(\mathcal{C}^\perp)=2$.
6. $\mathcal{C}$ is linearly equivalent to a code whose generator matrix is

$$\left(\; I_k \;\middle|\; \alpha I_k \;\middle|\; \cdots \;\middle|\; \alpha^{m-1} I_k \;\right), \tag{3.6}$$

where $\alpha\in\mathbb{F}_{q^m}$ satisfies $\mathbb{F}_{q^m}=\mathbb{F}_q(\alpha)$.

Proof. (1) ⇒ (2): If $\mathcal{C}$ is nondegenerate, then its support has dimension km, which is also the dimension of the associated $[km,k]_{q^m/q}$ system.

(2) ⇒ (6): The code $\mathcal{C}$ has effective length km ands $\mathcal{U}=\mathbb{F}_{q^m}^k$ as corresponding $[n,k]_{q^m/q}$ system. Hence, $\mathcal{U}$ has a basis given by $\mathcal{B}=\{\alpha^i e_j \,:\, 0\le i\le m-1, 0\le j\le k-1\}$. Thus, $\mathcal{C}$ belongs to the same equivalence class of the code whose generator matrix is (3.6).

(6) ⇒ (5): Without loss of generality, we can assume that $\mathcal{C}$ is the code whose generator matrix G is (3.6). Since $\mathcal{C}$ is nondegenerate, by Proposition 3.2 we have $d^{\mathrm{rk}}(\mathcal{C}^\perp)>1$. Moreover, G is a parity check matrix for $\mathcal{C}^\perp$ and from that it is easy to see that the vector $v=\alpha e_1-e_{k+1}$ belongs to $\mathcal{C}^\perp$ and has rank weight 2. Thus $d^{\mathrm{rk}}(\mathcal{C}^\perp)=2$.

(5) ⇒ (4): Clear.

(4) $\Rightarrow$ (1): The equivalence between (4) and (1) holds for every rank-metric code, by Proposition 3.2.

(2) $\Rightarrow$ (3): Let $\mathcal{C}$ be the $[n,k]_{q^m/q}$ code generated by G. By hypothesis, the $[n,k]_{q^m/q}$ system corresponding to $\mathcal{C}$ is $\mathcal{U} = \mathbb{F}_{q^m}^k$. Moreover, for every nonzero $v \in \mathbb{F}_{q^m}^k$, by (3.5) it holds that

$$\mathrm{rk}(vG) = km - \dim_{\mathbb{F}_q}(\mathcal{U} \cap \langle v \rangle^\perp) = km - (k-1)m = m.$$

(3) $\Rightarrow$ (1): Let $\mathcal{C}$ be a $[km,k]_{q^m/q}$ code. Let $n \leq km$ be its effective length, that is, $n = \dim(\sigma^{\mathrm{rk}}(\mathcal{C}))$. This means that $\mathcal{C}$ can be isometrically embedded in $\mathbb{F}_{q^m}^n$, obtaining a code $\mathcal{C}'$. Then $\mathcal{C}'$ is a nondegenerate $[n,k]_{q^m/q}$ code with the same weight distribution as $\mathcal{C}$. In particular, $\mathcal{C}'$ is a one-weight code as well. Fix a generator matrix for $\mathcal{C}'$ and consider the associated $[n,k]_{q^m/q}$ system, which we call $\mathcal{U}$. Since $\mathcal{C}'$ is a one-weight code, we have $|H \cap (\mathcal{U} \setminus \{0\})| = (q^a - 1)$ for every $\mathbb{F}_{q^m}$-hyperplane of $\mathbb{F}_{q^m}^k$. Therefore, if we denote by Λ the set of all the $\mathbb{F}_{q^m}$-hyperplanes in $\mathbb{F}_{q^m}^k$, we have

$$\sum_{H \in \Lambda} |H \cap (\mathcal{U} \setminus \{0\})| = \binom{k}{1}_{q^m} (q^a - 1).$$

Moreover, by applying Equation (3.2) to the right-hand side, we obtain

$$(q^{km} - 1)(q^a - 1) = (q^{(k-1)m} - 1)(q^n - 1).$$

By Lemma 3.15, we have $a = (k-1)m$ and $n = km$. Hence $\mathcal{C}$ itself is nondegenerate. □

We call **simplex rank-metric code** a code that satisfies any of the equivalent conditions in Proposition 3.16. Note that Proposition 3.16 also implies the following characterization of one-weight codes in the rank metric, which is the analogue of the main result of [11].

Corollary 3.17 (Classification of one-weight rank-metric codes)**.** Let $k \geq 2$ and let $\mathcal{C}$ be an $[n,k,d]_{q^m/q}$ one-weight code. Then, the effective length of $\mathcal{C}$ is km and $d = m$. That is, $\mathcal{C}$ is isometric to a simplex rank-metric $[km,k,m]_{q^m/q}$ code.

Proof. If $n \leq km$, as shown in the proof of Proposition 3.16, it has to be $n = km$ and $\mathcal{C}$ is a simplex rank-metric code. Assume now $n > km$. Since the effective length of an $[n,k]_{q^m/q}$ is always at most km, then we can isometrically embed $\mathcal{C}$ in a $[km,k]_{q^m/q}$ code $\mathcal{C}'$, with the same weight distribution. By Proposition 3.16, $\mathcal{C}'$ has to be a simplex rank-metric code. □

We remark that there is a strong analogy between simplex rank-metric codes and their homonyms in the Hamming metric, which is confirmed by both their weight distributions and by geometric characterization.

Indeed, by Corollary 3.17, simplex rank-metric codes are the only nondegenerate one-weight codes in the rank-metric, just like simplex codes in the Hamming metric, up to repetition. In fact, simplex codes in the Hamming metric are the only projective one-weight codes (where **projective** means that no two columns of one, and thus any, generator matrix are linearly dependent).

From a geometric point of view, simplex codes in the Hamming metric have a generator matrix whose columns are formed by all the points of $\mathrm{PG}(k-1,q)$. In the rank-metric, simplex codes are associated to the $[km,k]_{q^m/q}$ system $\mathbb{F}_{q^m}^k$, which is the natural analogue in the rank metric.

We conclude by observing that a definition of simplex code in the rank metric has been recently proposed in [32] (the definition has been given for sum-rank-metric codes, which specialize to rank-metric codes by taking a single matrix block). The simplex codes defined in [32] are different from the simplex codes considered in this paper. For example, one can check they are not one-weight in general. From a geometric viewpoint, the definition of simplex code proposed in this paper appears therefore more natural.

4 From Rank-Metric to Hamming-Metric Codes

In this section we explore various connections between codes in the rank and in the Hamming metric. In particular, we show how to construct a Hamming-metric code from a rank-metric one and describe how the parameters of the two codes relate to each other.

4.1 Linear Sets

Linear sets in finite geometry can be viewed as a generalizations of subgeometries. Their name was first proposed by Lunardon in [29], where linear sets are used for special constructions of blocking sets. The very first example of linear set is probably due to Brouwer and Wilbrink; see [12]. The interested reader is referred to [34] for an in-depth treatment of linear sets.

A special family of linear sets, which is of particular interest for this paper, is the one of scattered linear sets introduced by Blokhuis and Lavrauw in [9]. Recently, Sheekey and Van de Voorde observed a connection between scattered linear sets and rank-metric codes with optimal parameters in [39, 41]; see [35] for a survey on this topic.

Definition 4.1. Let $\mathcal{U}$ be an $[n,k]_{q^m/q}$ system. The $\mathbb{F}_q$**-linear set** in $\mathrm{PG}(k-1,q^m)$ of rank n associated to $\mathcal{U}$ is the set

$$L_{\mathcal{U}} := \{\langle u\rangle_{\mathbb{F}_{q^m}} \ : \ u \in \mathcal{U}\setminus\{0\}\},$$

where $\langle u\rangle_{\mathbb{F}_{q^m}}$ denotes the projective point corresponding to u.

Let $\Lambda = \mathrm{PG}(W,\mathbb{F}_{q^m})$ be the projective subspace corresponding to the $\mathbb{F}_{q^m}$-subspace W of $\mathbb{F}_{q^m}^k$. We define the **weight** of Λ in $L_{\mathcal{U}}$ as the integer

$$\mathrm{wt}_{\mathcal{U}}(\Lambda) := \dim_{\mathbb{F}_q}(\mathcal{U}\cap W).$$

If Λ is an hyperplane, that is, if $\Lambda = \mathrm{PG}(W,\mathbb{F}_{q^m})$ with $W = \langle v\rangle^{\perp}$ for some nonzero $v \in \mathbb{F}_{q^m}^k$, then $\mathrm{wt}_{\mathcal{U}}(\Lambda) = n - \mathrm{rk}(vG)$, where G is a $k\times n$ matrix associated to $\mathcal{U}$; see Lemma 3.7. Observe moreover that for a point $P \in \mathrm{PG}(k-1,q^m)$ we have that $P \in L_{\mathcal{U}}$ if and only if $\mathrm{wt}_{\mathcal{U}}(P) \geq 1$.

Remark 4.2. The original definition of linear sets does not assume the space $\mathcal{U}$ to be a $[n,k]_{q^m/q}$ system, i.e., that $\langle\mathcal{U}\rangle_{\mathbb{F}_{q^m}}$ is the whole space $\mathbb{F}_{q^m}^k$. However, if $\dim_{\mathbb{F}_{q^m}}(\langle\mathcal{U}\rangle_{\mathbb{F}_{q^m}}) = k-i$, one can assume up to equivalence that $\mathcal{U} \subseteq \langle e_1,\dots,e_{k-i}\rangle_{\mathbb{F}_{q^m}} =: V$, and then study $\mathcal{U}$ in the projective subspace $\mathrm{PG}(k-i-1,q^m)$ induced by V.

For any $[n,k]_{q^m/q}$ system $\mathcal{U}$, the cardinality of the associated linear set $L_{\mathcal{U}}$ satisfies

$$|L_{\mathcal{U}}| \leq \frac{q^n-1}{q-1}. \tag{4.1}$$

A linear set $L_{\mathcal{U}}$ whose cardinality meets (4.1) with equality is said to be **scattered**. Equivalently, a linear set $L_{\mathcal{U}}$ is scattered if and only if $\mathrm{wt}_{\mathcal{U}}(P) = 1$ for each $P \in L_{\mathcal{U}}$. We also observe that (4.1) can be refined as follows.

Lemma 4.3. Let $\mathcal{U}$ be an $[n,k]_{q^m/q}$ system. Then

$$\sum_{P\in\mathrm{PG}(k-1,q^m)} \frac{q^{\mathrm{wt}_{\mathcal{U}}(P)}-1}{q-1} = \frac{q^n-1}{q-1}.$$

Proof. Let Λ_1 be the set of 1-dimensional $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}^k$. Then, we have

$$\sum_{P\in\mathrm{PG}(k-1,q^m)} \frac{q^{\mathrm{wt}_{\mathcal{U}}(P)}-1}{q-1} = \frac{1}{q-1}\sum_{V\in\Lambda_1}(q^{\dim_{\mathbb{F}_q}(\mathcal{U}\cap V)}-1) = \frac{1}{q-1}\sum_{V\in\Lambda_1}|V\cap(\mathcal{U}\setminus\{0\})| = \frac{q^n-1}{q-1},$$

where the latter equality follows from Lemma 3.6. ∎

4.2 The Associated Hamming-Metric Code

The notion of a linear set allows us to describe a connection between rank-metric codes and some particular codes in the Hamming metric. This connection was also observed in [40]. For a $[n,k]_{q^m/q}$ system $\mathcal{U}$ and a point $P \in \mathrm{PG}(k-1,q^m)$, define

$$\mathrm{m}_{\mathcal{U}}(P) := \frac{q^{\mathrm{wt}_{\mathcal{U}}(P)}-1}{q-1}.$$

The identity of Lemma 4.3 can be written as

$$\sum_{P\in\mathrm{PG}(k-1,q^m)} \mathrm{m}_{\mathcal{U}}(P) = \frac{q^n-1}{q-1}. \tag{4.2}$$

Denote by $\mathcal{U}(n,k)_{q^m/q}$ the set of $[n,k]_{q^m/q}$ system and by $\mathcal{P}(n,k)_{q^m}$ the set of projective $[n,k]_{q^m}$ systems. Define the map

$$\begin{array}{ccc} \mathcal{U}(n,k)_{q^m/q} & \longrightarrow & \mathcal{P}(\frac{q^n-1}{q-1},k)_{q^m}, \\ \mathcal{U} & \longmapsto & (L_{\mathcal{U}},\mathrm{m}_{\mathcal{U}}), \end{array}$$

where $(L_{\mathcal{U}},\mathrm{m}_{\mathcal{U}})$ denotes the multiset $L_{\mathcal{U}}$ with multiplicity function $\mathrm{m}_{\mathcal{U}}$. The parameters $\frac{q^n-1}{q-1}$ and k of the projective system $(L_{\mathcal{U}},\mathrm{m}_{\mathcal{U}})$ directly follow from (4.2). It is easy to see that this map is compatible with the equivalence relations on $\mathcal{U}(n,k)_{q^m/q}$ and on $\mathcal{P}(\frac{q^n-1}{q-1},k)_{q^m}$. Indeed, the actions defining the equivalence classes are given in both cases by the group $\mathrm{PGL}(k,q^m)$. We thus constructed a map

$$\mathrm{Ext}^{\mathrm{H}}: \quad \mathcal{U}[n,k]_{q^m/q} \quad \longrightarrow \quad \mathcal{P}[\tfrac{q^n-1}{q-1},k]_{q^m},$$

where $\mathcal{U}[n,k]_{q^m/q}$ and $\mathcal{P}[\frac{q^n-1}{q-1},k]_{q^m}$ denote the set of equivalence classes of $[n,k]_{q^m/q}$ systems and the set of equivalence classes of projective $[\frac{q^n-1}{q-1},k]_{q^m}$ systems, respectively. This maps leaves also the parameter d of the projective $[\frac{q^n-1}{q-1},k]_{q^m}$ system fixed, as the following result shows.

Lemma 4.4. Let $[\mathcal{U}]$ be the equivalence class of $[n,k,d]_{q^m/q}$ systems. Then $[(L_{\mathcal{U}},\mathrm{m}_{\mathcal{U}})]$ is the equivalence class of a projective $[\frac{q^n-1}{q-1},k,\frac{q^n-q^{n-d}}{q-1}]_{q^m}$ system. In other words, the map

$$\mathrm{Ext}^{\mathrm{H}}: \mathcal{U}[n,k,d]_{q^m/q} \longrightarrow \mathcal{P}\left[\frac{q^n-1}{q-1},k,\frac{q^n-q^{n-d}}{q-1}\right]_{q^m}$$

is well-defined.

Proof. The fact that the map $\mathrm{Ext}^{\mathrm{H}}$ sends equivalence classes of $[n,k]_{q^m/q}$ systems in equivalence classes of projective $[\frac{q^n-1}{q-1},k]_q$ systems has already been observed above. We only need to show the compatibility between the third parameters. More precisely, we need to show that for a given $[n,k,d]_{q^m/q}$ system $\mathcal{U}$, every element in $\mathrm{Ext}^{\mathrm{H}}([\mathcal{U}])$ is a projective $[\frac{q^n-1}{q-1},k,\frac{q^n-q^{n-d}}{q-1}]_q$ system. Fix the projective $[\frac{q^n-1}{q-1},k,d']_q$ system $(L_{\mathcal{U}},\mathrm{m}_{\mathcal{U}})$, and denote by Λ_{k-1} the set of $\mathbb{F}_{q^m}$-hyperplanes of $\mathbb{F}_{q^m}^k$. Then for any $H \in \Lambda_{k-1}$ we have

$$\sum_{P\in\mathrm{PG}(H,\mathbb{F}_{q^m})} \mathrm{m}_{\mathcal{U}}(P) = \sum_{P\in\mathrm{PG}(H,\mathbb{F}_{q^m})} \frac{q^{\mathrm{wt}_{\mathcal{U}}(P)}-1}{q-1}$$

$$= \frac{1}{q-1} \sum_{\substack{V \subseteq H \\ \dim_{\mathbb{F}_{q^m}}(V)=1}} |V \cap (\mathcal{U} \setminus \{0\}|$$
$$= \frac{1}{q-1} |H \cup (\mathcal{U} \setminus \{0\})|$$
$$= \frac{q^{\dim_{\mathbb{F}_q}(H \cap \mathcal{U})} - 1}{q-1},$$

where the second to last identity follows from the fact that $\{V \setminus \{0\} : V \subseteq H, \dim_{\mathbb{F}_{q^m}}(V) = 1\}$ is a partition of $H \setminus \{0\}$. Therefore we obtain

$$d' = \frac{q^n - 1}{q-1} - \max\left\{ \frac{q^{\dim_{\mathbb{F}_q}(H \cap \mathcal{U})} - 1}{q-1} \, : \, H \in \Lambda_{k-1} \right\} = \frac{q^n - 1}{q-1} - \frac{q^{n-d} - 1}{q-1} = \frac{q^n - q^{n-d}}{q-1}. \quad \square$$

Definition 4.5. Let $\mathcal{C}$ be a nondegenerate $[n, k, d]_{q^m/q}$ rank-metric code. We will call any Hamming-metric code in $(\Psi^{\mathrm{H}} \circ \mathrm{Ext}^{\mathrm{H}} \circ \Phi)([\mathcal{C}])$ **associated** with $\mathcal{C}$. Note that any such an object is a $[\frac{q^n-1}{q-1}, k, \frac{q^n-q^{n-d}}{q-1}]_{q^m}$ code.

The Hamming-metric code associated to $\mathcal{C}$ in the previous definition is clearly not unique. However, the choice of the code is irrelevant when focusing on properties that are invariant under monomial equivalence. Therefore, for ease of notation, in the sequel we denote by $\mathcal{C}^{\mathrm{H}}$ any code that belongs to $(\Psi^{\mathrm{H}} \circ \mathrm{Ext}^{\mathrm{H}} \circ \Phi)([\mathcal{C}])$.

Example 4.6. Let $q = 2$, $n = 4$ and $m = 3$. Consider $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, where $\alpha^3 + \alpha + 1 = 0$. Moreover, let $\mathcal{C}$ be the $[4, 2, 1]_{8/2}$ code whose generator matrix

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

Take the $[4, 2, 1]_{8/2}$ system $\mathcal{U}$ spanned by the columns of G, i.e., $\mathcal{U} = \{(a, \beta) : a \in \mathbb{F}_2, \beta \in \mathbb{F}_8\}$. The weights of the points in $\mathrm{PG}(1, 8)$ with respect to $\mathcal{U}$ are given by

$$\begin{aligned} &\mathrm{wt}_{\mathcal{U}}([1 : a]) = 1, \qquad \text{for every } a \in \mathbb{F}_8 \\ &\mathrm{wt}_{\mathcal{U}}([0 : 1]) = 3. \end{aligned}$$

Hence, we obtain that $\mathrm{Ext}^{\mathrm{H}}(\mathcal{U}) = (\mathrm{PG}(1, 8), \mathrm{m}_{\mathcal{U}})$, where

$$\begin{aligned} &\mathrm{m}_{\mathcal{U}}([1 : a]) = 1, \qquad \text{for every } a \in \mathbb{F}_8 \\ &\mathrm{m}_{\mathcal{U}}([0 : 1]) = 7. \end{aligned}$$

At this point, any code $\mathcal{C}^{\mathrm{H}} = C \in (\Psi^{\mathrm{H}} \circ \mathrm{Ext}^{\mathrm{H}} \circ \Phi)([\mathcal{C}])$ is monomially equivalent to the $[15, 2, 8]_8$ (Hamming-metric) code whose generator matrix is

$$G_{\mathrm{Ext}} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Example 4.7 (Simplex Rank-Metric Code)**.** Take $\mathcal{C}$ to be the $[km, k, m]_{q^m/q}$ simplex rank-metric code, whose corresponding $[km, k, m]_{q^m/q}$ system is $\Phi([\mathcal{C}]) = [\mathbb{F}_{q^m}^k]$. Denote $\mathcal{U} := \mathbb{F}_{q^m}^k$ and consider the weight of each point $P \in \mathrm{PG}(k-1, q^m)$ in $L_{\mathcal{U}}$. For $P = [v]$, we have

$$\mathrm{wt}_{\mathcal{U}}(P) = \dim_{\mathbb{F}_q}(\mathcal{U} \cap \langle v \rangle_{\mathbb{F}_{q^m}}) = \dim_{\mathbb{F}_q}(\langle v \rangle_{\mathbb{F}_{q^m}}) = m.$$

Therefore by applying the map $\mathrm{Ext}^{\mathrm{H}}$ we obtain

$$\mathrm{Ext}^{\mathrm{H}}([\mathcal{U}]) = [(L_{\mathcal{U}}, \mathrm{m}_{\mathcal{U}})],$$

where $L_{\mathcal{U}} = \mathrm{PG}(k-1, q^m)$ and

$$\mathrm{m}_{\mathcal{U}}(P) = \frac{q^m - 1}{q - 1} \quad \text{for all } P \in \mathrm{PG}(k-1, q^m).$$

In particular, any code in $(\Psi^{\mathrm{H}} \circ \mathrm{Ext}^{\mathrm{H}} \circ \Phi)([\mathcal{C}])$ is monomially equivalent to the concatenation of $\frac{q^m-1}{q-1}$ copies of the $[\frac{q^{km}-1}{q^m-1}, k, q^{(k-1)m}]_{q^m}$ simplex code in the Hamming metric.

Lemma 4.4 shows how the fundamental parameters of a nondegenerate $[n, k, d]_{q^m/q}$ rank-metric code $\mathcal{C}$ relate to those of an associated Hamming-metric code $\mathcal{C}^{\mathrm{H}}$. The connection can be made even more precise. For example, we can say how the weight distributions of the two codes relate to each other.

Theorem 4.8. Let $\mathcal{C}$ be a nondegenerate $[n, k, d]_{q^m/q}$ rank-metric code with rank-weight distribution $\{A_i^{\mathrm{rk}}(\mathcal{C})\}_i$. Then the Hamming-weight distribution of $\mathcal{C}^{\mathrm{H}}$ is $\{A_j^{\mathrm{H}}(\mathcal{C}^{\mathrm{H}})\}_j$ with

$$A_j^{\mathrm{H}}(\mathcal{C}^{\mathrm{H}}) = \begin{cases} A_i^{\mathrm{rk}}(\mathcal{C}) & \text{if } j = \frac{q^n - q^{n-i}}{q-1}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let G be a generator matrix for $\mathcal{C}$ and denote by $\mathcal{U}$ the $\mathbb{F}_q$-span of its columns. Let G_{Ext} be a generator matrix for $\mathcal{C}^{\mathrm{H}}$ whose columns are the elements of the multiset $(L_{\mathcal{U}}, \mathrm{m}_{\mathcal{U}})$. Doing the same computations as in Lemma 4.4 we obtain that, for every $u \in \mathbb{F}_{q^m}^k \setminus \{0\}$,

$$\mathrm{wt}^{\mathrm{H}}(uG_{\mathrm{Ext}}) = \frac{q^n - 1}{q - 1} - \sum_{P \in \mathrm{PG}(H_u, \mathbb{F}_{q^m})} \frac{q^{\mathrm{wt}_{\mathcal{U}}(P)} - 1}{q - 1} = \frac{q^n - q^{n - \mathrm{rk}(uG)}}{q - 1}, \tag{4.3}$$

where $H_u := \langle u \rangle^{\perp}$. ∎

Remark 4.9. While the connection between the dual of a code $\mathcal{C}$ and the dual of $\mathcal{C}^{\mathrm{H}}$ seems to be difficult to describe explicitly, we remark that their weight distributions (in the rank and Hamming metric, respectively) are linked via the theory of MacWilliams identities; see [30] for a general reference. More precisely, the Hamming weight distribution of $(\mathcal{C}^{\mathrm{H}})^{\perp}$ can be written in terms of the Hamming weight distribution of $\mathcal{C}^{\mathrm{H}}$. By Theorem 4.8, the latter can be written in terms of the rank weight distribution of $\mathcal{C}$ which, in turn, can be expressed in terms of the rank weight distribution of $\mathcal{C}^{\perp}$. We do not go into the details of the computation.

Remark 4.10. Theorem 4.8 generalizes various known results on Hamming-metric codes obtained from linear sets. This is the case of the two-weight Hamming-metric codes arising from maximum scattered linear sets found by Blokhuis and Lavrauw in [9, Section 5], and of the Hamming-metric codes with $h + 1$ weights recently presented by Zini and Zullo in [45, Theorem 7.1].

Finally, one can also prove the following result connecting the generalized weights of $\mathcal{C}$ and $\mathcal{C}^{\mathrm{H}}$ (in the respective metrics). These code invariants can be found in Definition 3.13 and in the Appendix, respectively. Since the argument is very similar to that in the proof of Theorem 4.8, the details are omitted.

Theorem 4.11. Let $\mathcal{C}$ be a nondegenerate $[n, k, d]_{q^m/q}$ rank-metric code with generalized rank-weights $\{d_i^{\mathrm{rk}}(\mathcal{C})\}_i$. Then the generalized Hamming-weights of $\mathcal{C}^{\mathrm{H}}$ are given by $\{d_i^{\mathrm{H}}(\mathcal{C}^{\mathrm{H}})\}_i$, where

$$d_i^{\mathrm{H}}(\mathcal{C}^{\mathrm{H}}) = \frac{q^n - q^{n - d_i^{\mathrm{rk}}(\mathcal{C})}}{q - 1}.$$

4.3 The Total Weight of a Rank-Metric Code

In this subsection we continue comparing codes in the rank and in the Hamming metric. Our focus is on the rank-metric analogue of a fundamental parameter of a Hamming-metric code, namely, its *total weight*. It is well-known that the latter only depends on the field size and on the code's dimension and effective length. More precisely, if $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a Hamming-nondegenerate code, then

$$\sum_{v \in \mathcal{C}} \mathrm{wt}^{\mathrm{H}}(v) = n(q^k - q^{k-1}). \tag{4.4}$$

This simple result, which has numerous applications in classical coding theory (for example, a simple proof of the Plotkin bound for linear codes), does not have an immediate analogue in the rank metric. Indeed, it is easy to find examples of rank-nondegenerate codes having the same parameters (q, m, n, k) but for which the quantity $\sum_{v \in \mathcal{C}} \mathrm{rk}(v)$ is not a constant.

In this section, we argue that, in the "total weight" context, a convenient analogue of $\mathrm{wt}^{\mathrm{H}}(v)$ is $q^{n-\mathrm{rk}(v)}$. We start by recalling the following q-analogue of the Pless identities; see [25].

Notation 4.12. For a prime power q and integers n, m, k, j, r, let

$$f_q(n, m, k, j, r) := \sum_{\nu=j}^{r} q^{m(k-\nu)} \begin{bmatrix} n-j \\ \nu-j \end{bmatrix}_q \begin{bmatrix} r \\ \nu \end{bmatrix}_q \prod_{\ell=0}^{\nu-1} (q^\nu - q^\ell).$$

Theorem 4.13 (Theorem 30 of [17])**.** Let $\mathcal{C}$ be an $[n, k, d]_{q^m/q}$ code. Then for all $0 \leq r \leq n$ we have

$$\sum_{v \in \mathcal{C}} q^{r(n-\mathrm{rk}(v))} = \sum_{j=0}^{r} A_j(\mathcal{C}^\perp)\, f_q(n, m, k, j, r).$$

In analogy with Remark 4.9, we observe that a different statement of Pless-type identities can in principle be obtained by combining the correspondence $\mathcal{C} \to \mathcal{C}^{\mathrm{H}}$ with the classical Pless identities for Hamming-metric codes. For the purposes of this section, Theorem 4.13 is what we will need.

In this paper, we are not only interested in the q-analogue of the total weight of a code, but also in other related quantities. In order to unify their treatment, it is convenient to regard the Hamming/rank weight of the nonzero elements of a code as a discrete random variable, which we simply denote by $\mathcal{C}^*$, $\mathbb{E}^{\mathrm{rk}}$ and $\mathrm{Var}^{\mathrm{rk}}$ for the mean and variance of (a function of) $\mathcal{C}^*$, viewed as a random variable in the sense explained above.

In the sequel, we call a code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ **rank-2-nondegenerate** if $d^{\mathrm{rk}}(\mathcal{C}^\perp) \geq 3$. Codes with this property are the rank-metric analogues of projective codes in the Hamming metric; see page 11. The previous theorem has the following simple consequences.

Corollary 4.14. Let $\mathcal{C}$ be an $[n, k, d]_{q^m/q}$ code. If $\mathcal{C}$ is rank-nondegenerate, then

$$\mathbb{E}^{\mathrm{rk}}[q^{n-\mathcal{C}^*}] = \frac{-q^n + q^{mk} + q^{m(k-1)}(q^n - 1)}{q^{mk} - 1},$$
$$\mathrm{Var}^{\mathrm{rk}}[q^{n-\mathcal{C}^*}] \geq \frac{-q^{2n} + f_q(n, m, k, 0, 2)}{q^{mk} - 1} - \mathbb{E}^{\mathrm{rk}}[q^{n-\mathcal{C}^*}]^2,$$

where the latter lower bound is attained with equality if and only if $\mathcal{C}$ is rank-2-nondegenerate.

Corollary 4.14 establishes the rank-metric analogue of the formula for the total weight of a Hamming-metric code in (4.4). It also shows that, for a rank-2-nondegenerate code $\mathcal{C}$, the variance of the random variable $q^{n-\mathcal{C}^*}$ only depends on a few code's parameters. While the formulas in Corollary 4.14 are quite involved and not immediate to interpret, their asymptotics as $q \to +\infty$ can be explicitly computed. The estimates describe how the variance behaves over large fields.

Proposition 4.15. Let $\mathcal{C}$ be an $[n,k,d]_{q^m/q}$ code. If $\mathcal{C}$ is rank-nondegenerate then $n \le km$ and, as $q \to +\infty$,

$$\mathbb{E}^{\mathrm{rk}}[q^{n-\mathcal{C}^*}] \sim \begin{cases} 1 & \text{if } n \le m-1, \\ q^{n-m} & \text{if } m+1 \le n \le km, \\ 2 & \text{if } n = m. \end{cases}$$

If in addition $\mathcal{C}$ is rank-2-nondegenerate, then $n \le mk/2$ and for $k \ge 3$ and $q \to +\infty$ we have

$$\mathrm{Var}^{\mathrm{rk}}[q^{n-\mathcal{C}^*}] \sim \begin{cases} q^{-m+n+1} & \text{if } k \le n \le m-2 \text{ or } m+2 \le n \le mk/2, \\ 1 & \text{if } n = m-1, \\ q & \text{if } n = m, \\ q^2 & \text{if } n = m+1. \end{cases}$$

Proof. The first part of the statement easily follows from Proposition 3.4 and Corollary 4.14. To prove the second part, we start by applying the rank-metric Singleton bound [18,20] to $\mathcal{C}^\perp$, obtaining $m(n-k) \le n(m - d^{\mathrm{rk}}(\mathcal{C}^\perp) + 1) \le n(m-2)$. This implies $n \le mk/2$, as desired.

We now turn to the asymptotic estimates. To simplify the notation, write f_q instead of $f_q(n,m,k,0,2)$. Lengthy computations show that

$$f_q = q^{mk} + q^{m(k-1)}(q^n-1)(q+1) + q^{m(k-2)+1}(q^n-1)(q^{n-1}-1).$$

Therefore

$$f_q(n,m,k,0,2) \sim \begin{cases} q^{mk} & \text{if } n \le m-2, \\ q^{mk+1} & \text{if } n = m, \\ q^{mk+2n-2m} & \text{if } n \ge m+2, \\ 2q^{mk} & \text{if } n = m-1, \\ 2q^{mk+2} & \text{if } n = m+1. \end{cases}$$

From the first part of the statement we also have

$$\mathbb{E}^{\mathrm{rk}}[q^{n-\mathcal{C}^*}]^2 \sim \begin{cases} 1 & \text{if } n \le m-1, \\ q^{2n-2m} & \text{if } n \ge m+1, \\ 4 & \text{if } n = m. \end{cases}$$

Using $k \ge 3$ (needed in the case $n = m+1$), this easily gives the asymptotics of

$$\mathrm{Var}^{\mathrm{rk}}[q^{n-\mathcal{C}^*}] = \frac{-q^{2n} + f_q(n,m,k,0,2)}{q^{mk}-1} - \mathbb{E}^{\mathrm{rk}}[q^{n-\mathcal{C}^*}]^2$$

for $n = m-1$, $n = m$, and $n = m+1$. To compute the asymptotics in the other cases, write

$$\frac{-q^{2n} + f_q(n,m,k,0,2)}{q^{mk}-1} - \mathbb{E}^{\mathrm{rk}}[q^{n-\mathcal{C}^*}]^2 = \frac{A_q - B_q}{(q^{mk}-1)^2},$$

where $A_q = (q^{mk}-1)(-q^{2n}+f_q)$ and $B_q = (-q^n + q^{mk} + q^{m(k-1)}(q^n-1))^2$.

If $n \le m-2$ then $f_q \sim q^{mk} + q^{m(k-1)+n+1}$. Therefore $A_q \sim q^{2mk} + q^{m(2k-1)+n+1}$ and $B_q \sim -q^{2mk} + 2q^{m(2k-1)+n}$, from which the desired asymptotic estimate follows.

If $m+2 \le n \le mk/2$, then $m+2 \le n \le m(k-1)$, because $k \ge 3$. We then have $f_q \sim q^{m(k-2)+2n} + q^{m(k-1)+n+1}$ and thus $A_q \sim q^{m(2k-2)+2n} + q^{m(2k-1)+n+1}$, $B_q \sim q^{2m(k-1)+2n} + 2q^{m(2k-1)+n}$. This again implies the desired asymptotic estimate.

□

5 Minimal Rank-Metric Codes: Geometry and Properties

The next two sections of this paper are devoted to the theory of minimal codes in the rank metric. In this first section we propose a definition of minimal and establish a 1-1 correspondence between $[n,k]_{q^m/q}$ minimal rank-metric codes and $[n,k]_{q^m/q}$ systems. This allows us to investigate the main properties of this new family of codes.

Definition 5.1. Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code. A codeword $v \in \mathcal{C}$ is a **minimal codeword** if, for every $v' \in \mathcal{C}$, $\sigma^{\mathrm{rk}}(v') \subseteq \sigma^{\mathrm{rk}}(v)$ implies $v' = \alpha v$ for some $\alpha \in \mathbb{F}_{q^m}$. We say that $\mathcal{C}$ is **minimal** if all its codewords are minimal.

Lemma 5.2. Let $v \in \mathbb{F}_{q^m}^n$. The following hold.

1. There exists $A \in \mathrm{GL}_n(q)$ such that $\sigma^{\mathrm{rk}}(vA) = \langle e_i \,:\, i \in \sigma^{\mathrm{H}}(vA)\rangle$.
2. Let $I \subseteq \{1,\dots,n\}$. Then, $\sigma^{\mathrm{rk}}(v) \subseteq \langle e_i \,:\, i \in I\rangle$ if and only if $I \supseteq \sigma^{\mathrm{H}}(v)$. In particular,
$$\sigma^{\mathrm{H}}(v) = \arg\min\{|I| \,:\, \sigma^{\mathrm{rk}}(v) \subseteq \mathcal{E}_I\},$$
where $\mathcal{E}_I := \langle e_i \,:\, i \in I\rangle$ and $\sigma^{\mathrm{rk}}(v) \subseteq \langle e_i \,:\, i \in \sigma^{\mathrm{H}}(v)\rangle$.

Proof. 1. Let $r = \dim(\sigma^{\mathrm{rk}}(v))$. By Proposition 2.1, there exist a matrix A and a basis Γ of $\mathbb{F}_{q^m}/\mathbb{F}_q$, such that $\Gamma(vA)$ is in Smith normal form. Hence, $\sigma^{\mathrm{H}}(vA) = \{1,\dots,r\}$ and $\sigma^{\mathrm{rk}}(vA) = \langle e_i \,:\, i \in \{1,\dots,r\}\rangle$.

2. Let $I = \sigma^{\mathrm{H}}(v)$ and fix any basis Γ of $\mathbb{F}_{q^m}/\mathbb{F}_q$. The rows indexed by $\{1,\dots,n\} \setminus I$ in $\Gamma(v)$ are identically zero. Hence, $\sigma^{\mathrm{rk}}(v) \subseteq \langle e_i \,:\, i \in I\rangle$. Vice versa, assume that there exists $t \in \sigma^{\mathrm{H}}(v) \setminus I$. Fix any basis Γ of $\mathbb{F}_{q^m}/\mathbb{F}_q$. Since $t \in \sigma^{\mathrm{H}}(v)$, there exists $j \in [m]$ such that $\Gamma(v_t)_j \neq 0$. Hence, the vector $a = (\Gamma(v_1)_j, \dots, \Gamma(v_n)_j)$ belongs to $\sigma^{\mathrm{rk}}(v)$ and has a nonzero entry in the t-th coordinate. Thus, $\sigma^{\mathrm{rk}}(v) \not\subseteq \langle e_i \,:\, i \in I\rangle$. The second statement immediately follows. □

5.1 Linear Cutting Blocking Sets and the Parameters of Minimal Codes

In this subsection we give a geometric characterization of minimal codes in the rank metric. This will allow us to derive bounds on their parameters.

We start with the q-analogue of the notion of a cutting blocking set.

Definition 5.3. A $[n,k]_{q^m/q}$ system $\mathcal{U}$ is called a **linear cutting blocking set** if for any $\mathbb{F}_{q^m}$-hyperplanes $H, H' \subseteq \mathbb{F}_{q^m}^k$ we have $(\mathcal{U} \cap H) \subseteq (\mathcal{U} \cap H')$ implies $H = H'$. We will say that that $\mathcal{U}$ is a linear cutting $[n,k]_{q^m/q}$ blocking set to emphasize the parameters.

While the term "linear cutting blocking set" might seem not fully consistent with the terminology used so far (since such an object is not a linear set), one can verify that an $[n,k]_{q^m/q}$ system $\mathcal{U}$ is a linear cutting blocking set if and only if its associated linear set $L_{\mathcal{U}}$ is a cutting blocking set in $\mathrm{PG}(k-1,q^m)$. The proof of this fact can be found in Section 5.2; see Theorem 5.13. This explains the choice of the terminology.

We will need the following characterization of linear cutting blocking sets.

Proposition 5.4. A $[n,k]_{q^m/q}$ system $\mathcal{U}$ is a linear cutting blocking set if and only if for every $\mathbb{F}_{q^m}$-hyperplane H we have $\langle H \cap \mathcal{U}\rangle_{\mathbb{F}_{q^m}} = H$.

Proof. ($\Leftarrow$) Let H, H' be two $\mathbb{F}_{q^m}$-hyperplanes of $\mathbb{F}_{q^m}^k$ such that $(\mathcal{U} \cap H) \subseteq (\mathcal{U} \cap H')$. Hence, $H = \langle H \cap \mathcal{U}\rangle_{\mathbb{F}_{q^m}} \subseteq \langle H' \cap \mathcal{U}\rangle_{\mathbb{F}_{q^m}} = H'$. Since H and H' are both hyperplanes, they have to be equal.

($\Rightarrow$) Suppose by contradiction that there exists an $\mathbb{F}_{q^m}$-hyperplane H of $\mathbb{F}_{q^m}^k$ such that $\langle H \cap \mathcal{U}\rangle_{\mathbb{F}_{q^m}} = X \subsetneq H$. Then, for every hyperplane $H' \supset X$ we have $(\mathcal{U} \cap H) \subseteq (\mathcal{U} \cap H')$. Since there are at least q^m such hyperplanes different from H, we obtain that $\mathcal{U}$ is not a linear cutting blocking set. □

Corollary 5.5. If $\mathcal{U}$ is a linear cutting $[n,k]_{q^m/q}$ blocking set, then for every $\mathbb{F}_{q^m}$-hyperplane of $\mathbb{F}_{q^m}^k$ we have $|H \cap \mathcal{U}| \geq q^{k-1}$.

Proof. Let $t := \dim_{\mathbb{F}_q}(H \cap \mathcal{U})$. Then an $\mathbb{F}_q$-basis for $H \cap \mathcal{U}$ is also a set of $\mathbb{F}_{q^m}$-generators for $\langle H \cap \mathcal{U} \rangle_{\mathbb{F}_{q^m}}$. Hence, since $\mathcal{U}$ is a linear cutting blocking set, by Proposition 5.4 we have

$$m(k-1) = \dim_{\mathbb{F}_q}(\langle H \cap \mathcal{U} \rangle_{\mathbb{F}_{q^m}}) \leq mt,$$

which shows that $t \geq k-1$. □

The geometric description of minimal rank-metric codes via linear cutting blocking sets relies on the following characterization of the inclusion of rank supports.

Theorem 5.6. Let G be a generator matrix for a nondegenerate $[n,k]_{q^m/q}$ code, $\mathcal{U}$ be the corresponding $[n,k]_{q^m/q}$ system and $u, v \in \mathbb{F}_{q^m}^k \setminus \{0\}$. Then,

$$\sigma^{\mathrm{rk}}(uG) \subseteq \sigma^{\mathrm{rk}}(vG) \qquad \text{if and only if} \qquad (\langle u \rangle^\perp \cap \mathcal{U}) \supseteq (\langle v \rangle^\perp \cap \mathcal{U}).$$

Proof. ($\Leftarrow$) Let $x_1, \ldots, x_t$ be an $\mathbb{F}_q$-basis of the space $X := (\langle v \rangle^\perp \cap \mathcal{U})$. Let $A \in \mathrm{GL}_n(q)$ be such that

$$GA = (\, x_1 \,|\, \cdots \,|\, x_t \,|\, G' \,),$$

where $G' \in \mathbb{F}_{q^m}^{k \times (n-t)}$. We have $uGA = (0, \ldots, 0 | uG')$ and $vGA = (0, \ldots, 0 | vG')$. Moreover, by (3.5) we have $\mathrm{rk}(vGA) = n - t$ and, by Lemma 5.2, $\sigma^{\mathrm{rk}}(vGA) = \langle e_i \,:\, i = t+1 \ldots, n \rangle$ and $\sigma^{\mathrm{rk}}(uGA) \subseteq \langle e_i \,:\, i = t+1 \ldots, n \rangle$. This means that $\sigma^{\mathrm{rk}}(uGA) \subseteq \sigma^{\mathrm{rk}}(vGA)$. Finally, Proposition 2.1 implies $\sigma^{\mathrm{rk}}(uG) \subseteq \sigma^{\mathrm{rk}}(vG)$.

($\Rightarrow$) Assume now that $\sigma^{\mathrm{rk}}(uG) \subseteq \sigma^{\mathrm{rk}}(vG)$. Let $r := \mathrm{rk}(vG)$. By the first part of Lemma 5.2 there exists $A \in \mathrm{GL}_n(q)$ such that $\sigma^{\mathrm{rk}}(vGA) = \langle e_1, \ldots, e_r \rangle$. Hence, $\sigma^{\mathrm{rk}}(uGA) \subseteq \sigma^{\mathrm{rk}}(vGA) = \langle e_1, \ldots, e_r \rangle$. Denote by $x_1, \ldots, x_n$ the columns of GA, which also form a basis of $\mathcal{U}$. In this notation we have $\langle v \rangle^\perp \cap \mathcal{U} = \langle x_{r+1}, \ldots, x_n \rangle_{\mathbb{F}_q}$. Moreover, by the second part of Lemma 5.2 we have $\sigma^{\mathrm{H}}(uGA) \subseteq \{1, \ldots, r\}$. This implies that $x_i \in \langle u \rangle^\perp$ for $i = r+1, \ldots, n$. Hence, $(\langle u \rangle^\perp \cap \mathcal{U}) \supseteq (\langle v \rangle^\perp \cap \mathcal{U})$. □

By combining Theorem 5.6 and the correspondence stated in Theorem 3.8 we obtain the following.

Corollary 5.7. The correspondence (Φ, Ψ) defined in Section 3.1 induces a 1-1 correspondence between minimal rank-metric codes and linear cutting blocking sets.

Corollary 5.7 has several consequences in the theory of minimal codes. The first result we drive concerns the construction of new minimal codes from existing ones.

Corollary 5.8. Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ minimal rank-metric code with generator matrix G, and let $v \in \mathbb{F}_{q^m}^k$. Then the $[n+1,k]_{q^m/q}$ code $\bar{\mathcal{C}} = \mathrm{rowsp}(G \mid v^\top)$ is minimal.

Proof. Without loss of generality, we may assume that $\mathcal{C}$ is nondegenerate. Let $\mathcal{U}$ be any $[n,k]_{q^m/q}$ system associated to $[\mathcal{C}]$ and let $\bar{\mathcal{U}} = \langle \mathcal{U}, v \rangle_{\mathbb{F}_q}$. If $v \in \mathcal{U}$, then by Proposition 3.2 the code $\bar{\mathcal{C}}$ is degenerate and it is equivalent to the code $\{(\, c \mid 0 \,) \,:\, c \in \mathcal{C}\}$, which is clearly minimal. Hence, assume that $v \notin \mathcal{U}$. By Proposition 3.2 we have that $\bar{\mathcal{C}}$ is nondegenerate and $\bar{\mathcal{U}}$ is an $[n+1,k]_{q^m/q}$ system associated to $\bar{\mathcal{C}}$. Let H be any $\mathbb{F}_{q^m}$-hyperplane of $\mathbb{F}_{q^m}^k$. Then

$$H \supseteq \langle H \cap \bar{\mathcal{U}} \rangle_{\mathbb{F}_{q^m}} = \langle H \cap (\mathcal{U} + \langle v \rangle_{\mathbb{F}_q}) \rangle_{\mathbb{F}_{q^m}} \supseteq \langle H \cap \mathcal{U} \rangle = H,$$

where the latter equality follows from the fact that, since $\mathcal{C}$ is minimal, $\mathcal{U}$ is a linear cutting blocking set by Theorem 5.7. Therefore $\bar{\mathcal{U}}$ is also a linear cutting blocking set and we conclude using Theorem 5.7 again. □

The following two results are also consequences of Corollary 5.7 and provide information about the parameters of a minimal $[n,k]_{q^m/q}$ code.

Corollary 5.9. Let $\mathcal{C}$ be a minimal $[n,k]_{q^m/q}$ code. Then for every $c \in \mathcal{C}$ we have $\mathrm{rk}(c) \leq \dim_{\mathbb{F}_q}(\sigma^{\mathrm{rk}}(\mathcal{C})) - k + 1$. In particular, $w^{\mathrm{rk}}(\mathcal{C}) \leq \dim_{\mathbb{F}_q}(\sigma^{\mathrm{rk}}(\mathcal{C})) - k + 1 \leq n - k + 1$.

Proof. Let $n' = \dim_{\mathbb{F}_q}(\sigma^{\mathrm{rk}}(\mathcal{C}))$ for ease of notation. As observed in Remark 3.3, we can isometrically embed $\mathcal{C}$ in $\mathbb{F}_{q^m}^{n'}$. Moreover, the resulting code is minimal if and only if $\mathcal{C}$ is minimal. Therefore we can assume without loss of generality that $\mathcal{C}$ is nondegenerate of length $n = \dim_{\mathbb{F}_q}(\sigma^{\mathrm{rk}}(\mathcal{C}))$. Let $\mathcal{U}$ be any $[n,k]_{q^m/q}$ system associated to $\mathcal{C}$. By Corollary 5.7, $\mathcal{U}$ is a linear cutting blocking set. From the proof of Corollary 5.5 we get that $\dim_{\mathbb{F}_q}(H \cap \mathcal{U}) \geq k-1$ for every $\mathbb{F}_{q^m}$-hyperplane of $\mathbb{F}_{q^m}^k$, and we conclude using Lemma 3.7. □

Corollary 5.10. If $\mathcal{C}$ is a minimal $[n,k]_{q^m/q}$ code with $k \geq 2$, then $n \geq k + m - 1$.

Proof. Without loss of generality we shall assume that $\mathcal{C}$ is nondegenerate. Therefore by Proposition 3.11 we have $w^{\mathrm{rk}}(\mathcal{C}) = \min\{m,n\}$. Since $k \geq 2$, by Corollary 5.9 we also have $w^{\mathrm{rk}}(\mathcal{C}) \leq n-k+1 < n$. Therefore $w^{\mathrm{rk}}(\mathcal{C}) = m$ and using again the fact that $w^{\mathrm{rk}}(\mathcal{C}) \leq n-k+1$ we find $n \geq m + k - 1$, as desired. □

5.2 Connections with Hamming-Metric Minimal Codes

It is natural to ask how the notions of minimality in the rank and in the Hamming metric relate to each other. This is the question we address in this subsection. In particular, we prove that a nondegenerate rank-metric code $\mathcal{C}$ is minimal if and only if its associated code(s) $\mathcal{C}^{\mathrm{H}}$ is minimal; see Section 4.2 for the notation.

The following result shows that minimality in the Hamming metric implies minimality in the rank metric. We propose two proofs, one in coding theory parlance and the other in the language of projective systems.

Proposition 5.11. Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code with the property of being Hamming-minimal. Then $\mathcal{C}$ is rank-minimal.

Proof. Suppose that $\mathcal{C}$ is not a minimal rank-metric code. Then there exist two codewords v, v' that are $\mathbb{F}_{q^m}$-linearly independent such that $\sigma^{\mathrm{rk}}(v) \subseteq \sigma^{\mathrm{rk}}(v')$. By Lemma 5.2, we also have that $\sigma^{\mathrm{H}}(v') = \arg\min\{|I| : \sigma^{\mathrm{rk}}(v') \subseteq \mathcal{E}_I\}$, where $\mathcal{E}_I := \langle e_i : i \in I\rangle$. Since $\sigma^{\mathrm{rk}}(v) \subseteq \sigma^{\mathrm{rk}}(v')$, we have $\sigma^{\mathrm{H}}(v) \subseteq \sigma^{\mathrm{H}}(v')$, and therefore $\mathcal{C}$ is not Hamming-minimal. □

Second proof. Without loss of generality, we may assume that $\mathcal{C}$ is nondegenerate. Let G be a generator matrix for $\mathcal{C}$, and let $\mathcal{B}$ be the basis of the associated $[n,k]_{q^m/q}$ system $\mathcal{U}$ formed by the columns of G. Then $\mathcal{M} := \{\langle u\rangle_{q^m} : u \in \mathcal{B}\}$ is a projective $[n,k]_{q^m}$ system in $\mathrm{PG}(k-1,q^m)$. By Hamming-minimality and Theorem 2.11, it is a cutting blocking set. Hence $\langle \mathrm{PG}(H,\mathbb{F}_{q^m}) \cap \mathcal{M}\rangle = \mathrm{PG}(H,\mathbb{F}_{q^m})$ for every $\mathbb{F}_{q^m}$-hyperplane H of $\mathbb{F}_{q^m}^k$. Let H be an $\mathbb{F}_{q^m}$-hyperplane of $\mathbb{F}_{q^m}^k$ and let

$$V := \langle H \cap \mathcal{U}\rangle = \langle H \cap \langle \mathcal{B}\rangle_{\mathbb{F}_q}\rangle.$$

Then

$$\mathrm{PG}(V,\mathbb{F}_{q^m}) = \langle \mathrm{PG}(H,\mathbb{F}_{q^m}) \cap L_{\mathcal{U}}\rangle \supseteq \langle \mathrm{PG}(H,\mathbb{F}_{q^m}) \cap \mathcal{M}\rangle = \mathrm{PG}(H,\mathbb{F}_{q^m}),$$

showing that $V = H$, We conclude by applying Proposition 5.4. □

Remark 5.12. The converse of Proposition 5.11 is false in general. For example, let $(q,m,n) = (2,3,4)$. Write $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, where $\alpha^3 + \alpha + 1 = 0$. The code generated by

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

is rank-minimal but not Hamming-minimal. Moreover, the code $\mathcal{C} \cdot A$ is not Hamming-minimal for any $A \in \mathrm{GL}_3(2)$. Indeed, if this was the case, then there would exist a Hamming-minimal $[4,2]_8$ code, which contradicts [3, Theorem 2.14].

The previous results and examples show that minimality in the rank and in the Hamming metric gives rise to very different concepts. We now show that the correspondence $\mathcal{C} \to \mathcal{C}^{\mathrm{H}}$ is more natural in this context, as it translates rank-minimality precisely into Hamming-minimality.

Theorem 5.13. Let $\mathcal{C}$ be a nondegenerate $[n,k,d]_{q^m/q}$ rank-metric code. Then $\mathcal{C}$ is minimal if and only if $\mathcal{C}^{\mathrm{H}}$ is Hamming-minimal.

Proof. By Corollary 5.7, $\mathcal{C}$ is minimal if and only if any $[n,k]_{q^m/q}$ system $\mathcal{U}$ associated with $\mathcal{C}$ is a linear cutting blocking set. Now, consider the linear set $L_{\mathcal{U}}$. We show that $\mathcal{U}$ is a linear cutting blocking set if and only if $L_{\mathcal{U}}$ is a cutting blocking set in $\mathrm{PG}(k-1,q^m)$. Let H be an $\mathbb{F}_{q^m}$-hyperplane of $\mathbb{F}_{q^m}^k$, then $L_{\mathcal{U}} \cap \mathrm{PG}(H, \mathbb{F}_{q^m}) = L_{\mathcal{U}} \cap L_H = L_{\mathcal{U} \cap H}$, and hence

$$\langle L_{\mathcal{U}} \cap \mathrm{PG}(H, \mathbb{F}_{q^m}) \rangle = \langle L_{\mathcal{U}} \cap L_H \rangle = \langle L_{\mathcal{U} \cap H} \rangle.$$

Moreover, for every subset $S \subseteq \mathbb{F}_{q^m}^k$, one has $L_{\langle S \rangle_{\mathbb{F}_{q^m}}} = \langle L_S \rangle$. This implies that $L_{\mathcal{U}}$ is a cutting blocking set in $\mathrm{PG}(k-1,q^m)$ if and only if for every $\mathbb{F}_{q^m}$-hyperplane H of $\mathbb{F}_{q^m}^k$ we have $L_{\langle \mathcal{U} \cap H \rangle_{\mathbb{F}_{q^m}}} = L_H$. Since H and $\langle \mathcal{U} \cap H \rangle_{\mathbb{F}_{q^m}}$ are both $\mathbb{F}_{q^m}$-linear, the linear set that they define coincide with the respective projective subspaces. Therefore $L_{\mathcal{U}}$ is a cutting blocking set in $\mathrm{PG}(k-1,q^m)$ if and only if $\langle H \cap \mathcal{U} \rangle_{\mathbb{F}_{q^m}} = H$ for every $\mathbb{F}_{q^m}$-hyperplane H in $\mathbb{F}_{q^m}^k$, as claimed. We conclude using Theorem 2.11 – which states that a linear code is Hamming-minimal if and only if the associated projective system is a cutting blocking set – and observing that, by definition, $L_{\mathcal{U}}$ is the projective system associated to $\mathcal{C}^{\mathrm{H}}$. □

Theorem 5.13 allows us to transfer results known for minimal codes in the Hamming metric to the rank metric setting. For example, the following is the rank-metric analogue of the characterization in [24, Theorem 11].

Theorem 5.14. Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code. Then $\mathcal{C}$ is minimal if and only if

$$\sum_{\lambda \in \mathbb{F}_{q^m} \setminus \{0\}} q^{-\mathrm{rk}(c+\lambda c')} \neq (q^m-1) \cdot q^{-\mathrm{rk}(c)} - q^{-\mathrm{rk}(c')} + 1$$

for all linearly independent $c, c' \in \mathcal{C}$.

Proof. By Theorem 5.13, $\mathcal{C}$ is rank-minimal if and only if any associated-Hamming metric code $\mathcal{C}^{\mathrm{H}}$ is Hamming-minimal. We can now conclude by using [24, Theorem 11] and (4.3). □

Remark 5.15. It is natural to ask if the best known criterion for Hamming-minimality, namely the *Ashikhmin-Barg condition* of [4, Lemma 2.1], can be transferred to the rank-metric context. The mentioned result states that every $[n,k,d]_{q^m}$ code satisfying $w_{\max}(q^m-1) < q^m d$ is Hamming-minimal, where $w_{\max}$ denotes the maximum Hamming weight of a codeword.

One may naturally try to use Ashikhmin-Barg condition together with Theorem 5.13 and Theorem 4.8 to obtain a sufficient condition rank-minimality. This can be done as follows.

Let $\mathcal{C}$ be a nondegenerate $[n,k,d]_{q^m/q}$ code. By Corollary 5.10, we may assume without loss of generality that $n \geq m$. By Proposition 3.11, the maximum rank of a codeword in $\mathcal{C}$ is m. Now consider the associated Hamming-metric code $\mathcal{C}^{\mathrm{H}}$. Using Theorem 4.8 we see that the minimum distance of $\mathcal{C}^{\mathrm{H}}$ is $(q^n - q^{n-d})(q-1)^{-1}$ and that the maximum Hamming weight of a codeword in $\mathcal{C}^{\mathrm{H}}$ is $(q^n - q^{n-m})(q-1)^{-1}$. Therefore imposing the Ashikhmin-Barg condition yields the following: A nondegenerate $[n,k,d]_{q^m/q}$ code is rank-minimal if

$$(q^n - q^{n-m})(q^m-1) < q^m(q^n - q^{n-d}). \tag{5.1}$$

However, it is not difficult to see that (5.1) is only satisfied when $d = m$, that is, when $\mathcal{C}$ is the $[km, k, m]_{q^m/q}$ simplex code; see Proposition 3.16. In other words, the rank metric analogue of the Ashikhmin-Barg condition is trivial.

6 Minimal Rank-Metric Codes: Existence and Constructions

In this second section on minimal rank-metric codes we turn to their existence and constructions. In particular, in the light of the geometric characterization of Corollary 5.7 and of the lower bound of Corollary 5.10, we investigate the existence of short minimal codes. We start by showing some simple examples of minimal codes. Then we construct a family of 3-dimensional minimal codes using scattered linear sets, and establish the existence of minimal rank-metric codes for all $n \geq 2k + m - 2$ using a counting argument. The last part of this section is devoted to a new parameter of rank-metric codes, which we call the *linearity index* and use to investigate further the structure of minimal codes.

6.1 First Examples of Minimal Rank-Metric Codes

A natural question is whether a simplex rank-metric code is minimal or not. Indeed, in the Hamming-metric simplex codes are among the simplest and best known minimal codes.

Theorem 6.1. Let $\mathcal{C}$ be a $[km, k, m]_{q^m/q}$ simplex rank-metric code. Then $\mathcal{C}$ is minimal.

Proof. By the definition, any $[km, k]_{q^m/q}$ system associated to $\mathcal{C}$ is $\mathbb{F}_{q^m}^k$; see Proposition 3.16. The latter is clearly a linear cutting blocking set, since $H \cap \mathbb{F}_{q^m}^k = H$ for each $\mathbb{F}_{q^m}$-hyperplane H of $\mathbb{F}_{q^m}^k$. □

The following criterion is a sufficiency result to have a minimal rank-metric code.

Proposition 6.2. Let $\mathcal{C}$ be a nondegenerate $[n, k]_{q^m/q}$ code with $n \geq (k-1)m + 1$. Then $\mathcal{C}$ is minimal.

Proof. Let $\mathcal{U}$ be any $[n, k]_{q^m/q}$ system corresponding to $\mathcal{C}$ (up to equivalence) and let H be an $\mathbb{F}_{q^m}$-hyperplane of $\mathbb{F}_{q^m}^k$. By Proposition 5.4, we need to show that $\langle H \cap \mathcal{U} \rangle_{\mathbb{F}_{q^m}} = H$. Since H is also an $\mathbb{F}_q$-space, we can compute the $\mathbb{F}_q$-dimension of $H \cap \mathcal{U}$ as follows:

$$\begin{aligned}
\dim_{\mathbb{F}_q}(H \cap \mathcal{U}) &= \dim_{\mathbb{F}_q}(H) + \dim_{\mathbb{F}_q}(\mathcal{U}) - \dim_{\mathbb{F}_q}(H + \mathcal{U}) \\
&= (k-1)m + n - \dim_{\mathbb{F}_q}(H + \mathcal{U}) \\
&\geq (k-1)m + (k-1)m + 1 - km \\
&= (k-2)m + 1.
\end{aligned}$$

This implies that $\langle H \cap \mathcal{U} \rangle_{\mathbb{F}_{q^m}}$ has $\mathbb{F}_{q^m}$-dimension strictly greater than $k-2$ and since it is contained in H, it has to be equal to H. □

Proposition 6.2 shows that every nondegenerate $[n, 2]_{q^m/q}$ code with $n = m + 1$ is minimal. This means that the bound of Corollary 5.10 is sharp for $k = 2$. It is natural to ask if the bound is sharp for other values of k. We will show in Section 6.2 that this happens also for $k = 3$.

6.2 Three-Dimensional Minimal Rank-Metric Codes

In this section we study minimal $[n,3]_{q^m/q}$ codes. In particular we prove that they exist for every $n \geq m+2$ under the assumption that $m \geq 4$. This also implies that for $k=3$ and $m \geq 4$ the bound of Corollary 5.10 is sharp.

The first result that we provide links the existence of scattered linear sets with 3-dimensional minimal rank-metric codes.

Theorem 6.3. Let $\mathcal{C}$ be a nondegenerate $[n,3]_{q^m/q}$ code with $n \geq m+2$ and let $\mathcal{U}$ be any $[n,3]_{q^m/q}$ system corresponding to $\mathcal{C}$. If $L_{\mathcal{U}}$ is a scattered linear set, then $\mathcal{C}$ is a minimal rank-metric code.

Proof. Let $\mathcal{C}^{\mathrm{H}} \in (\Psi^{\mathrm{H}} \circ \mathrm{Ext}^{\mathrm{H}} \circ \Phi)([\mathcal{C}])$ be any Hamming-metric code associated with $\mathcal{C}$. By Theorem 5.13, $\mathcal{C}$ is rank-minimal if and only if $\mathcal{C}^{\mathrm{H}}$ is Hamming-minimal, which is in turn equivalent to the fact that $L_{\mathcal{U}}$ is a cutting blocking set in $\mathrm{PG}(2,q^m)$. Consider now the multiplicity function associated to $L_{\mathcal{U}}$ in the projective $[\frac{q^n-1}{q-1},k]_{q^m}$ system $\mathrm{Ext}^{\mathrm{H}}(\mathcal{U})$. Since $L_{\mathcal{U}}$ is scattered, this means that every point of $L_{\mathcal{U}}$ has multiplicity 1. Let G be any generator matrix of $\mathcal{C}^{\mathrm{H}}$, and let $v \in \mathbb{F}_{q^m}^3 \setminus \{0\}$. Since by Proposition 3.11 the maximum rank of a codeword in $\mathcal{C}$ is m, using Theorem 4.8 we get

$$\mathrm{wt}^{\mathrm{H}}(vG) \leq \frac{q^n - q^{n-m}}{q-1}.$$

Thus,

$$|L_{\mathcal{U}} \cap \langle v \rangle^{\perp}| = \frac{q^n-1}{q-1} - \mathrm{wt}^{\mathrm{H}}(vG) \geq \frac{q^{n-m}-1}{q-1} \geq q+1.$$

In particular, $L_{\mathcal{U}}$ is a $(q+1)$-fold blocking set, and in $\mathrm{PG}(2,q^m)$ this also implies that $L_{\mathcal{U}}$ is cutting. □

Thanks to Theorem 6.3, the existence of certain minimal rank-metric codes reduces to the existence of certain scattered linear sets. There is a well known upper bound on the parameters of these objects, due to Blokhuis and Lavrauw; see [9]. If $\mathcal{U}$ is a $[n,k]_{q^m/q}$ system such that $L_{\mathcal{U}}$ is scattered, then

$$n \leq \frac{km}{2}. \tag{6.1}$$

In this context, much progress has been made in the study of *maximum scattered linear sets*, which are linear sets whose parameters meet the bound in (6.1) with equality. A construction of such linear sets was first provided by Blokhuis and Lavrauw for k even; see [9]. When instead k is odd and m is even, a construction of linear sets meeting (6.1) for infinitely many parameters was given by Bartoli, Giulietti, Marino and Polverino in [7, Theorem 1.2]. The picture was then completed by Csajbók, Marino, Polverino and Zullo; see [15].

Theorem 6.4 (see [15, Theorem 2.4])**.** Assume that km is even. Then there exists a $[\frac{km}{2},k]_{q^m/q}$ system such that $L_{\mathcal{U}}$ is scattered.

When km is odd, not much is known yet. One of the few existence results on the maximum rank of a scattered linear set is the following, due to Blokhuis and Lavrauw.

Theorem 6.5 (see [9, Theorem 4.4])**.** Let k,m be positive integers and q be a prime power. There exists an $[ab,k]_{q^m/q}$ system such that $L_{\mathcal{U}}$ is scattered, whenever a divides k, $\gcd(a,m)=1$ and

$$ab < \begin{cases} \frac{km-k+3}{2} & \text{if } q=2 \text{ and } a=1, \\ \frac{km-k+a+3}{2} & \text{otherwise.} \end{cases}$$

In contrast with the most common line of research in the theory of scattered linear set, in this paper we are primarily interested in short nondegenerate minimal codes, and thus in

linear sets with small rank. For this reason, we state the following simple lemma, whose proof is omitted.

Lemma 6.6. Let $\mathcal{U}$ be an $[n,k]_{q^m/q}$ system such that $L_{\mathcal{U}}$ is a scattered linear set. If $n > k$, then there exists an $[n-1,k]_{q^m/q}$ system $\mathcal{V} \subseteq \mathcal{U}$ such that $L_{\mathcal{V}}$ is scattered.

We conclude this subsection by combining the previous three results with each other. This yields the following existence theorem for 3-dimensional minimal rank-metric codes.

Theorem 6.7. Suppose that $m \not\equiv 3,5 \mod 6$ and $m \geq 4$. Then there exists a (nondegenerate) minimal $[m+2,3]_{q^m/q}$ code.

Proof. Observe that by Theorem 6.3 it is enough to prove that there exists an $[m+2,3]_{q^m/q}$ system $\mathcal{U}$ such that $L_{\mathcal{U}}$ is scattered.

First, assume that m is even. Then, by Theorem 6.4, we have that there exists a $[\frac{3m}{2},3]_{q^m/q}$ system such that $L_{\mathcal{U}}$ is scattered. Then, since $m+2 \leq \frac{3m}{2}$ whenever $m \geq 4$, using Lemma 6.6 we obtain the desired $[m+2,3]_{q^m/q}$ system.

Now assume that m is odd and $m \not\equiv 0 \mod 3$. Write $m = 3s+i$. We use Theorem 6.5 with $a = 3$ and $b = s+1$, which shows the existence of an $[\frac{m+3-i}{2},3]_{q^m/q}$ system $\mathcal{U}$ such that $L_{\mathcal{U}}$ is scattered. If $m \equiv 1 \mod 3$, we get the desired result. □

Remark 6.8. In the remaining cases, finding scattered linear sets of rank $m+2$ in $\mathrm{PG}(2,q^m)$ seems in general a difficult task. For instance, when $m = 5$, the existence of a $[7,3]_{q^5/q}$ system $\mathcal{U}$ defining a scattered linear set was recently shown in [6, Theorem 5.1], but only in characteristic 2, 3 and 5 and under some restriction on the field size.

We illustrate the construction of minimal codes based on Theorem 6.3 with an explicit example.

Example 6.9. We describe a construction of a $[6,3]_{q^4/q}$ system $\mathcal{U}$ such that $L_{\mathcal{U}}$ is a scattered linear set, which was proposed in [5]. First, consider the finite field $\mathbb{F}_{q^{12}} = \mathbb{F}_{q^4}(\delta) = \mathbb{F}_q(\eta)$ and identify it with $\mathbb{F}_{q^4}^3$ by fixing the $\mathbb{F}_{q^4}$-basis $\{1,\delta,\delta^2\}$. Choose $\alpha,\beta \in \mathbb{F}_{q^{12}}$ such that

$$\begin{cases} \beta^{q^7+q^4-q^3+q} \neq -(\beta^{q^3} - \beta^{q^6+q^3+1})^{q-1}, \\ \alpha^{q^3+1} = \beta^{q^3} - \beta^{q^6+q^3+1} \neq 0, \\ \beta^{q^9+q^6+q^3+1} = 1. \end{cases}$$

Then the set

$$\mathcal{U} = \left\{ \gamma \in \mathbb{F}_{q^{12}} \,:\, \gamma^{q^6} + \alpha\gamma^3 + \beta = 0 \right\}$$

is a $[6,3]_{q^4/q}$ system $\mathcal{U}$ such that $L_{\mathcal{U}}$ is a scattered linear set.

More concretely, take $q = 2$ and η such that $\eta^{12} + \eta^7 + \eta^6 + \eta^5 + \eta^3 + \eta + 1 = 0$. One can check that $\alpha = \eta^{64}$ and $\beta = \eta^7$ satisfy the properties above. We then have

$$\mathcal{U} = \left\{ \gamma \in \mathbb{F}_{2^{12}} \,:\, \gamma^{64} + \alpha\gamma^3 + \beta = 0 \right\} = \langle \eta^6, \eta^{22}, \eta^{63}, \eta^{89}, \eta^{166}, \eta^{289} \rangle_{\mathbb{F}_2}.$$

If we write $\mathbb{F}_{2^{12}} = \mathbb{F}_{16}(\eta)$ and $\mathbb{F}_{16} = \{0\} \cup \{\lambda^i \,:\, 0 \leq i \leq 14\}$, where $\lambda = \eta^{273}$ satisfies $\lambda^4 + \lambda + 1 = 0$, then we can express the generators of $\mathcal{U}$ above in coordinates with respect to the $\mathbb{F}_{16}$-basis $\{1,\eta,\eta^2\}$ of $\mathbb{F}_{2^{12}}$. One of the $[6,3]_{16/2}$ codes in $\Phi([\mathcal{U}])$ is generated by the matrix

$$G = \begin{pmatrix} \lambda^4 & \lambda^{10} & \lambda^8 & \lambda^3 & \lambda^9 & \lambda^7 \\ \lambda^{14} & \lambda^8 & \lambda & \lambda^8 & 0 & \lambda^8 \\ \lambda^{10} & 0 & \lambda^6 & \lambda^5 & \lambda^{11} & \lambda^3 \end{pmatrix}.$$

By Theorem 6.3, this code is minimal.

6.3 Existence Results for Minimal Rank-Metric Codes

In this subsection we establish a general existence result for minimal rank-metric codes. We prove that minimal rank-metric codes exist for all parameter sets (n, m, k) with $m \geq 2$ and $n \geq 2k + m - 2$ (and any q). Combining this with previous results, we then give parameter intervals for which nondegenerate minimal codes exist and do not exist.

Lemma 6.10. Let m, n, k be positive integers and suppose $n \geq k \geq 2$. If

$$\frac{(q^{mn}-1)(q^{m(n-1)}-1)}{(q^{mk}-1)(q^{m(k-1)}-1)} - \frac{1}{2}\sum_{i=2}^{m} \frac{1}{q^m-1}\binom{m}{i}_q \prod_{j=0}^{i-1}(q^n-q^j)\left(\frac{q^{mi}-1}{q^m-1}-1\right) \tag{6.2}$$

is positive, then there exists a minimal $[n,k]_{q^m/q}$ code.

Proof. We use an argument inspired by the methods of [23] but which is simpler and avoids the graph theory language. Form a set of representatives for the equivalence classes of nonzero vectors in $\mathbb{F}_{q^m}^n$. Call this set $\mathcal{Q}$ and let

$$\mathcal{P} = \{P = \{x, y\} \subseteq \mathcal{Q} \,:\, x \neq y,\, \sigma^{\mathrm{rk}}(x) \subseteq \sigma^{\mathrm{rk}}(y) \text{ or } \sigma^{\mathrm{rk}}(y) \subseteq \sigma^{\mathrm{rk}}(x)\}.$$

The $[n,k]_{q^m/q}$ non-minimal codes are the k-dimensional subspaces $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ such that $P \subseteq \mathcal{C}$ for some $P \in \mathcal{P}$. Their number is at most

$$\sum_{P\in\mathcal{P}} |\{\mathcal{C} \subseteq \mathbb{F}_{q^m}^n \,:\, \mathcal{C} \supseteq P\}| = |\mathcal{P}|\binom{n-2}{k-2}_q.$$

Therefore, the minimal $[n,k]_{q^m/q}$ codes are at least

$$\binom{n}{k}_{q^m} - |\mathcal{P}|\binom{n-2}{k-2}_{q^m} = \binom{n-2}{k-2}_{q^m}\left(\frac{(q^{mn}-1)(q^{m(n-1)}-1)}{(q^{mk}-1)(q^{m(k-1)}-1)} - |\mathcal{P}|\right).$$

In particular, a minimal $[n,k]_{q^m/q}$ code exists if

$$\frac{(q^{mn}-1)(q^{m(n-1)}-1)}{(q^{mk}-1)(q^{m(k-1)}-1)} - |\mathcal{P}| > 0. \tag{6.3}$$

Finally, we count the elements of $\mathcal{P}$ as

$$\begin{aligned}
2|\mathcal{P}| &= \sum_{i=1}^{m} |\{(x,y) \in \mathcal{Q}^2 \,:\, x \neq y,\, \mathrm{rk}(y) = i,\, \sigma^{\mathrm{rk}}(x) \subseteq \sigma^{\mathrm{rk}}(y)\}| \\
&= \sum_{i=1}^{m} \sum_{\substack{y\in\mathcal{Q} \\ \mathrm{rk}(y)=i}} |\{x \in \mathcal{Q} \,:\, x \neq y,\, \sigma^{\mathrm{rk}}(x) \subseteq \sigma^{\mathrm{rk}}(y)\}| \\
&= \sum_{i=1}^{m} \frac{1}{q^m-1}\binom{m}{i}_q \prod_{j=0}^{i-1}(q^n-q^j)\left(\frac{q^{mi}-1}{q^m-1}-1\right) \\
&= \sum_{i=2}^{m} \frac{1}{q^m-1}\binom{m}{i}_q \prod_{j=0}^{i-1}(q^n-q^j)\left(\frac{q^{mi}-1}{q^m-1}-1\right).
\end{aligned}$$

Combining this with (6.3) concludes the proof. ∎

We now give a sufficient condition under which the assumption in Lemma 6.10 is satisfied. This gives us parameter ranges for which minimal codes exist. Note that, in line with what we

observed in the Introduction of this paper, the next result does not depend on the field size q. This behaviour of minimal rank-metric codes is in sharp contrast with analogous results for minimal codes in the Hamming metric; see e.g. [3, Theorem 2.14].

Corollary 6.11. For every $m, k \geq 2$, there exists a minimal $[2k+m-2, k]_{q^m/q}$ code.

Proof. Fix an integer $n \geq k$ and observe that

$$\frac{(q^{mn}-1)(q^{m(n-1)}-1)}{(q^{mk}-1)(q^{m(k-1)}-1)} \geq q^{mn+m(n-1)-mk-m(k-1)} = q^{2m(n-k)}.$$

Therefore the quantity in (6.2) can be bounded from below as follows:

$$\begin{aligned}
(6.2) &\geq q^{2m(n-k)} - \frac{1}{2(q^m-1)^2} \sum_{i=2}^{m} \binom{m}{i}_q \cdot q^{\binom{i}{2}} \cdot (q^{mi}-q^m) \prod_{j=0}^{i-1}(q^{n-j}-1) \\
&> q^{2m(n-k)} - \frac{1}{2(q^m-1)^2} \sum_{i=2}^{m} \binom{m}{i}_q \cdot q^{\binom{i}{2}} \cdot q^{mi} \prod_{j=0}^{i-1} q^{n-j} \\
&= q^{2m(n-k)} - \frac{1}{2(q^m-1)^2} \sum_{i=2}^{m} \binom{m}{i}_q \cdot q^{i(m+n)} =: t_q(m,n,k).
\end{aligned}$$

Define the function

$$f(q) := \prod_{i=1}^{\infty} \frac{q^i}{q^i-1}.$$

In the sequel, we will use the following estimates:

$$\binom{a}{b}_q < f(q)\, q^{b(a-b)}, \qquad \text{for } a, b \in \mathbb{N}, \tag{6.4}$$

$$q^{e_1} + \ldots + q^{e_r} \leq \frac{q}{q-1} q^{e_r}, \qquad \text{for } e_i \in \mathbb{Z},\ 0 \leq e_1 < \ldots < e_r. \tag{6.5}$$

We have

$$\begin{aligned}
2(q^m-1)^2 t_q(m,n,k) &= 2(q^m-1)^2 q^{2m(n-k)} - q^{m(m+n)} - \sum_{i=2}^{m-1} \binom{m}{i}_q q^{i(m+n)} \\
&\overset{(6.4)}{>} 2(q^m-1)^2 q^{2m(n-k)} - q^{m(m+n)} - f(q) \sum_{i=2}^{m-1} q^{i(2m+n-i)} \\
&\overset{(6.5)}{>} 2(q^m-1)^2 q^{2m(n-k)} - q^{m(m+n)} - \frac{q f(q)}{q-1} q^{(m-1)(m+n-1)}. \\
&> 2(q^m-1)^2 q^{2m(n-k)} - q^{m(m+n)} - q^{(m-1)(m+n-1)+3},
\end{aligned} \tag{6.6}$$

where the last inequality follows from the fact that $f(q) < 4$ for every prime power q.

We now specialize the argument to $n = 2k+m-2$, proving that $t_q(m, 2k+m-2, k) > 0$ for every $m, k \geq 2$ and prime power q. Using (6.6) we find

$$\begin{aligned}
2(q^m-1)^2 t_q(m, 2k+m-2, k) &> 2(q^m-1)^2 q^{2m(m+k-2)} - q^{2m(m+k-1)} - q^{(m-1)(2m+2k-3)+3} \\
&= 2(q^m-1)^2 q^{2m(m+k-2)} - (1+q^{-3m-2k+6}) q^{2m(m+k-1)} \\
&\geq 2(q^m-1)^2 q^{2m(m+k-2)} - (1+q^{-4}) q^{2m(m+k-1)} \\
&= q^{2m(m+k-2)-4} \left(2(q^m-1)^2 q^4 - (q^4+1) q^{2m}\right)
\end{aligned}$$

Hence $t_q(m, 2k+m-2, k) > 0$ whenever $q^{2m+4} - 4q^{m+4} - q^{2m} + 2q^4 \geq 0$, which holds for every $m \geq 2$ and every prime power q. Therefore there exists a minimal $[2k+m-2, k]_{q^m/q}$ code by Lemma 6.10. □

Remark 6.12. Fix integers $k, m \geq 2$. Then Corollary 5.10 tells us that for any length value $n < k+m-1$ an $[n, k]_{q^m/q}$ minimal code cannot exist, for any field size q. On the other hand, by Corollary 6.11 for $n \geq 2k+m-2$ there exist $[n, k]_{q^m/q}$ minimal codes for every field size q. Therefore the existence of $[n, k]_{q^m/q}$ minimal codes remains in general an open question only for $k+m-1 \leq n \leq 2k+m-3$.

6.4 The Linearity Index of a q-System

Given an $[n, k]_{q^m/q}$ system $\mathcal{U}$, one could be interested in understanding how $\mathcal{U}$ is related to $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}^k$ and not only to $\mathbb{F}_{q^m}$-hyperplanes. This indeed could reveal some additional information on its parameters and whether it can be a linear cutting blocking set or not. In this subsection we define and analyze a new parameter of projective system and with its aid we generalize the lower bound in Corollary 5.10 for the length of minimal codes.

Let $\mathcal{U}$ be a $[n, k]_{q^m/q}$ system. We introduce a measure for the "linearity" of $\mathcal{U}$ over $\mathbb{F}_{q^m}$. More precisely, we define the **linearity index** of $\mathcal{U}$ as

$$\ell(\mathcal{U}) = \max\{\dim_{\mathbb{F}_{q^m}}(H) \,:\, H \subseteq \mathbb{F}_{q^m}^k \text{ is an } \mathbb{F}_{q^m}\text{-subspace, } H \subseteq \mathcal{U}\}.$$

Observe that the value of $\ell(\mathcal{U})$ is invariant under equivalence of $[n, k]_{q^m/q}$ systems. In particular, it is a well-defined structural parameter of the corresponding equivalence class $[\mathcal{U}]$. The following result relates $\ell(\mathcal{U})$ to the generalized rank weight of a code that gives rise to the q-system $\mathcal{U}$.

Lemma 6.13. Let $\mathcal{C}$ be a nondegenerate $[n, k]_{q^m/q}$ code, and let $\mathcal{U}$ be any corresponding $[n, k]_{q^m/q}$ system. Then

$$\ell(\mathcal{U}) = k - \min\{r \,:\, d_r^{\mathrm{rk}}(\mathcal{C}) = n - (k-r)m\}.$$

Proof. First of all, note that the set $\{r \,:\, d_r^{\mathrm{rk}}(\mathcal{C}) = n-(k-r)m\}$ is nonempty, since $d_k^{\mathrm{rk}}(\mathcal{C}) = n$. By Theorem 3.14,

$$d_r^{\mathrm{rk}}(\mathcal{C}) = n - \max\left\{\dim_{\mathbb{F}_q}(\mathcal{U} \cap H) \,:\, H \text{ is an } \mathbb{F}_{q^m}\text{-subspace of codimension } r \text{ in } \mathbb{F}_{q^m}^k\right\},$$

which is equal to $n-(k-r)m$ if and only if there exists $H \subseteq \mathbb{F}_{q^m}^k$ of codimension r contained in $\mathcal{U}$. □

Lemma 6.13 shows that the parameter ℓ is well-defined in the correspondence of Theorem 3.8. Hence, it is also a well-defined parameter of a nondegenerate code $\mathcal{C}$. Therefore, we will also refer to the **linearity index of a code** $\mathcal{C}$, and denote it by $\ell(\mathcal{C})$.

Lemma 6.14. Let $\mathcal{C}$ be a nondegenerate $[n, k]_{q^m/q}$ code with linearity index ℓ. Then, $d_{i+1}^{\mathrm{rk}}(\mathcal{C}) - d_i^{\mathrm{rk}}(\mathcal{C}) = m$ if and only if $i \geq k - \ell(\mathcal{C})$.

Proof. ($\Leftarrow$) This implication follows from the definition of $\ell(\mathcal{C})$.

($\Rightarrow$) Let $\mathcal{U}$ be any $[n, k]_{q^m/q}$ system associated to $\mathcal{C}$. Let $H \subseteq \mathbb{F}_{q^m}^k$ be the space of codimension i such that $d_i^{\mathrm{rk}}(\mathcal{C}) = n - \dim_{\mathbb{F}_q}(H \cap \mathcal{U})$ and let $t := \dim_{\mathbb{F}_q}(H \cap \mathcal{U})$. Let $\mathcal{V} := H \cap \mathcal{U}$ and observe that $|H' \cap (\mathcal{V} \setminus \{0\})| = (q^{t-m} - 1)$ for any hyperplane H' in H. Let Λ be the set of all hyperplanes in H, then by Lemma 3.6, we have

$$\sum_{H' \in \Lambda} |H' \cap (\mathcal{V} \setminus \{0\})| = \begin{bmatrix} k-i \\ 1 \end{bmatrix}_{q^m} (q^{t-m} - 1).$$

Moreover, observe that every nonzero element of $\mathcal{V}$ belongs to exactly $\begin{bmatrix} k-i-1 \\ 1 \end{bmatrix}_{q^m}$ hyperplanes in H. Hence,

$$\sum_{H' \in \Lambda} |H' \cap (\mathcal{V} \setminus \{0\})| = \sum_{v \in \mathcal{V} \setminus \{0\}} |\{H' : v \in H'\}| = \begin{bmatrix} k-i-1 \\ 1 \end{bmatrix}_{q^m} (q^t - 1).$$

By a double counting argument, we then have that

$$(q^{(k-i)m} - 1)(q^{t-m} - 1) = (q^t - 1)(q^{(k-i-1)m} - 1).$$

By Lemma 3.15, it follows that $t = (k-i)m$. In particular, $\mathcal{V}$ is an $[km, k]_{q^m/q}$ system associated to a simplex code. We conclude then that $H \subseteq \mathcal{V}$ and then $H \subseteq \mathcal{U}$, which implies that $\ell(\mathcal{C}) \geq k - i$.

□

Proposition 6.15. Let $\mathcal{C}$ be a nondegenerate $[n, k]_{q^m/q}$ code. Then

$$\ell(\mathcal{C}) \geq n - k(m-1).$$

Proof. Observe that $\sum_{i=0}^{k-1} d_{i+1}^{\mathrm{rk}}(\mathcal{C}) - d_i^{\mathrm{rk}}(\mathcal{C}) = d_k^{\mathrm{rk}}(\mathcal{C}) - d_0^{\mathrm{rk}}(\mathcal{C}) = n$. Moreover, by applying Lemma 6.14, we have that

$$\begin{aligned} \sum_{i=0}^{k-1} d_{i+1}^{\mathrm{rk}}(\mathcal{C}) - d_i^{\mathrm{rk}}(\mathcal{C}) &= \sum_{i=0}^{k-\ell(\mathcal{C})-1} d_{i+1}^{\mathrm{rk}}(\mathcal{C}) - d_i^{\mathrm{rk}}(\mathcal{C}) + \sum_{i=k-\ell(\mathcal{C})}^{k-1} d_{i+1}^{\mathrm{rk}}(\mathcal{C}) - d_i^{\mathrm{rk}}(\mathcal{C}) \\ &\leq (m-1)(\ell(\mathcal{C}) - 1) + m\ell(\mathcal{C}) = m(k-1) + \ell(\mathcal{C}) - m. \end{aligned}$$

□

The linearity index of a code can help in characterizing and finding improved bounds on the other parameters of a minimal $[n, k]_{q^m/q}$ code.

Lemma 6.16. Let $\mathcal{U}$ be a linear cutting $[n, k]_{q^m/q}$ blocking set. Suppose that there exists an ℓ-dimensional $\mathbb{F}_{q^m}$-subspace T of $\mathbb{F}_{q^m}^k$ such that $T \subseteq \mathcal{U}$. Then $\mathcal{U}/T$ is isomorphic to a linear cutting $[n - \ell m, k - \ell]_{q^m/q}$ blocking set.

Proof. By Proposition 5.4, we need to show that for every $\mathbb{F}_{q^m}$-hyperplane $\bar{H}$ of $\mathbb{F}_{q^m}^k/T$ we have $\langle \bar{H} \cap \mathcal{U}/T \rangle_{\mathbb{F}_{q^m}} = \bar{H}$. The $\mathbb{F}_{q^m}$-hyperplanes of $\mathbb{F}_{q^m}^k/T$ correspond to the $\mathbb{F}_{q^m}$-hyperplanes of $\mathbb{F}_{q^m}^k$ that contain T. Let $\bar{H}$ be an $\mathbb{F}_{q^m}$-hyperplane of $\mathbb{F}_{q^m}^k/T$. Then there exists an $\mathbb{F}_{q^m}$-hyperplane H of $\mathbb{F}_{q^m}^k$ such that $\bar{H} = H/T$. Hence,

$$\langle \bar{H} \cap \mathcal{U}/T \rangle_{\mathbb{F}_{q^m}} = \langle (H \cap \mathcal{U})/T \rangle_{\mathbb{F}_{q^m}} = \langle H \cap \mathcal{U} \rangle_{\mathbb{F}_{q^m}}/T = H/T = \bar{H},$$

where the second last equality follows from the fact that $\mathcal{U}$ is a linear cutting $[n, k]_{q^m/q}$ blocking set and by Proposition 5.4. □

The following result is a generalization of Corollary 5.10.

Proposition 6.17. Let $\mathcal{U}$ be a linear cutting $[n, k]_{q^m/q}$ blocking set and let ℓ be its linearity index. If $k - \ell \geq 2$, then

$$n - k \geq (\ell + 1)(m - 1).$$

In particular, for every $1 \leq r \leq k - \lfloor \frac{n-k+1}{m-1} \rfloor - 1$, we have $d_r^{\mathrm{rk}}(\mathcal{C}) > n - rm$, where $\mathcal{C}$ is the nondegnerate $[n, k]_{q^m/q}$ code associated to $\mathcal{U}$.

Proof. Let $T \subseteq \mathbb{F}_{q^m}^k$ be an ℓ-dimensional $\mathbb{F}_{q^m}$-subspace contained in $\mathcal{U}$. By Lemma 6.16 we have that $\mathcal{U}/T$ is isomorphic to a linear cutting $[n-\ell m, k-\ell]_{q^m/q}$ blocking set. Therefore, by Corollary 5.10, we obtain

$$n - \ell m \geq k - \ell + m - 1,$$

from which we derive the desired inequality.
For the second part, if ℓ does not satisfy the above inequality, i.e. if $\ell \geq \lfloor \frac{n-k+1}{m-1} \rfloor + 1$, then $\mathcal{U}$ cannot contain any ℓ-dimensional $\mathbb{F}_{q^m}$-subspace. This is equivalent to say that $d_{k-\ell}^{\mathrm{rk}}(\mathcal{C}) > n - (k-\ell)m$. □

Remark 6.18. As a consequence of 6.17, it can be immediately seen that in order to construct short minimal rank-metric code, one has to try to construct linear cutting blocking sets not containing $\mathbb{F}_{q^m}$-subspaces. This is also consistent with the construction of minimal $[m+2, 3]_{q^m/q}$ codes provided in Section 6.2. Indeed, if a $[n,k]_{q^m/q}$ system $\mathcal{U}$ contains a $\mathbb{F}_{q^m}$-subspace H, then in the associated linear set $L_{\mathcal{U}}$ one has $\mathrm{wt}_{\mathcal{U}}(P) = m$ for every $P \in \mathrm{PG}(H, \mathbb{F}_{q^m})$. In particular, the associated linear set is far from being scattered.

Proposition 6.17 allows to characterize nondegenerate $[(k-1)m, k]_{q^m/q}$ minimal codes.

Corollary 6.19. Let $k \geq 2$ and $\mathcal{C}$ be a nondegenerate $[(k-1)m, k]_{q^m/q}$ code with linearity index $\ell = \ell(\mathcal{C})$. The following are equivalent.

1. $\mathcal{C}$ is minimal.
2. $\ell < k-2$.
3. $d_2^{\mathrm{rk}}(\mathcal{C}) > m$.

Proof. (1) ⇒ (2): First observe that ℓ can not be equal to $k-1$. Indeed, if $\ell = k-1$, then the code $\mathcal{C}$ is not k-dimensional. Hence, $k - \ell \geq 2$ and since $\mathcal{C}$ is minimal, then by Proposition 6.17 it holds

$$(k-1)m - k + 1 > (\ell+1)(m-1),$$

from which we deduce $\ell < k-2$.

(2) ⇒ (1): Suppose $\mathcal{C}$ is not minimal and let $\mathcal{U}$ be any associated $[(k-1)m, k]_{q^m/q}$ system. By Proposition 5.4, there exists an $\mathbb{F}_{q^m}$-hyperplane of $\mathbb{F}_{q^m}^k$ such that $\langle H \cap \mathcal{U} \rangle_{\mathbb{F}_{q^m}} =: H'$, with $\dim_{\mathbb{F}_{q^m}}(H') \leq k-2$. Hence, we obtain

$$\begin{aligned}(k-2)m &\geq \dim_{\mathbb{F}_q}(H') \geq \dim_{\mathbb{F}_q}(H \cap \mathcal{U}) \\ &= \dim_{\mathbb{F}_q}(H) + \dim_{\mathbb{F}_q}(\mathcal{U}) - \dim_{\mathbb{F}_q}(\mathcal{U} + H) \\ &\geq (k-1)m + (k-1)m - km = (k-2)m.\end{aligned}$$

Hence, all the inequalities above are equalities and $H' = H \cap \mathcal{U}$. This implies that $\mathcal{U}$ contains the $(k-2)$-dimensional $\mathbb{F}_{q^m}$-subspace H' and $\ell \geq k-2$.

(2) ⇔ (3): Observe that $\ell \leq k-2$ and $d_2^{\mathrm{rk}}(\mathcal{C}) \geq m$. Then, the statement directly follows from Lemma 6.13. □

Corollary 6.20. Let $k \geq 3$ be an integer. A nondegenerate $[(k-1)m, k]_{q^m/q}$ minimal code exists if and only if $m \geq 3$.

Proof. Suppose that $m \geq 3$ and construct the $[(k-3)m + 3(m-1), k]_{q^m/q}$ system $\mathcal{U}'$ as follows. Take $\mathcal{V}' = \langle \alpha^i e_j \ : \ 0 \leq i \leq m-2, k-2 \leq j \leq k \rangle$, where $\alpha \in \mathbb{F}_{q^m}$ is such that $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Then, consider $\mathcal{U}' = \{(\, v \mid 0,0,0) \ : \ v \in \mathbb{F}_{q^m}^{k-3}\} \oplus \mathcal{V}'$. By construction $\ell(\mathcal{U}') = k-3$. Moreover, since $m \geq 3$ then $(k-3)m + 3(m-1) \geq (k-1)m$, and we can take any $(k-1)m$-dimensional $\mathbb{F}_q$-subspace $\mathcal{U}$ of $\mathcal{U}'$, which has $\ell(\mathcal{U}) \leq k-3$ and by Corollary 6.19 is minimal.

Assume now $m \leq 2$, and let $\mathcal{C}$ be a nondegenerate a $[(k-1)m, k]_{q^m/q}$ code. Then by Proposition 6.15, we have $\ell(\mathcal{C}) \geq k - m \geq k-2$. Hence, By Corollary 6.19, $\mathcal{C}$ is not minimal. □

Acknowledgements

The authors of this paper would like to thank John Sheekey and Ferdinando Zullo for fruitful discussions and comments.

References

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Network information flow. *IEEE Trans. Inform. Theory*, 46(4):1204–1216, 2000.

[2] G. N. Alfarano, M. Borello, and A. Neri. A geometric characterization of minimal codes and their asymptotic performance. *Adv. Math. Commun.*, 2020.

[3] G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani. Three combinatorial perspectives on minimal codes. *arXiv preprint arXiv:2010.16339*, 2020.

[4] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Trans. Inform. Theory*, 44(5):2010–2017, 1998.

[5] S. Ball, A. Blokhuis, and M. Lavrauw. Linear $(q+1)$-fold blocking sets in $\mathrm{PG}(2, q^4)$. *Finite Fields Appl.*, 6(4):294–301, 2000.

[6] D. Bartoli, B. Csajbók, G. Marino, and R. Trombetti. Evasive subspaces. *arXiv preprint arXiv:2005.08401*, 2020.

[7] D. Bartoli, M. Giulietti, G. Marino, and O. Polverino. Maximum scattered linear sets and complete caps in Galois spaces. *Combinatorica*, 38(2):255–278, 2018.

[8] T. P. Berger. Isometries for rank distance and permutation group of Gabidulin codes. *IEEE Trans. Inform. Theory*, 49(11):3016–3019, 2003.

[9] A. Blokhuis and M. Lavrauw. Scattered spaces with respect to a spread in $\mathrm{PG}(n, q)$. *Geom. Dedicata*, 81(1-3):231–243, 2000.

[10] M. Bonini and M. Borello. Minimal linear codes arising from blocking sets. *J. Algebraic Combin.*, 53(2):327–341, 2021.

[11] A. Bonisoli. Every equidistant linear code is a sequence of dual Hamming codes. *Ars Combin.*, 18:181–186, 1984.

[12] A. E. Brouwer and H. A. Wilbrink. Blocking sets in translation planes. *J. Geom.*, 19(2):200, 1982.

[13] A. A. Bruen, J. A. Thas, and A. Blokhuis. On M.D.S. codes, arcs in $\mathrm{PG}(n, q)$ with q even, and a solution of three fundamental problems of B. Segre. *Invent. Math.*, 92(3):441–459, 1988.

[14] R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bull. London Math. Soc.*, 18(2):97–122, 1986.

[15] B. Csajbók, G. Marino, O. Polverino, and F. Zullo. Maximum scattered linear sets and MRD-codes. *J. Algebraic Combin.*, 46(3-4):517–531, 2017.

[16] A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco. Linear nonbinary covering codes and saturating sets in projective spaces. *Adv. Math. Commun.*, 5(1):119–147, 2011.

[17] J. de la Cruz, E. Gorla, H. H. López, and A. Ravagnani. Weight distribution of rank-metric codes. *Des. Codes Cryptogr.*, 86(1):1–16, 2018.

[18] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *J. Combin. Theory Ser. A*, 25(3):226–241, 1978.

[19] S. Fancsali and P. Sziklai. Lines in higgledy-piggledy arrangement. *Electron. J. Comb.*, 21(2), 2014.

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

[21] A. García and H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Invent. Math.*, 121(1):211–222, 1995.

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

[23] A. Gruica and A. Ravagnani. Common complements of linear subspaces and the sparseness of MRD codes. *arXiv:2011.02993*, 2020.

[24] Z. Heng, C. Ding, and Z. Zhou. Minimal linear codes over finite fields. *Finite Fields Appl.*, 54:176–196, 2018.

[25] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[26] R. Jurrius and R. Pellikaan. On defining generalized rank weights. *Adv. Math. Commun.*, 11(1):225–235, 2017.

[27] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inform. Theory*, 54(8):3579–3591, 2008.

[28] S.-Y. R. Li, R. W. Yeung, and N. Cai. Linear network coding. *IEEE Trans. Inform. Theory*, 49(2):371–381, 2003.

[29] G. Lunardon. Normal spreads. *Geom. Dedicata*, 75(3):245–261, 1999.

[30] F. J. MacWilliams and N. J. A. Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977.

[31] U. Martínez-Peñas. On the similarities between generalized rank and Hamming weights and their applications to network coding. *IEEE Trans. Inform. Theory*, 62(7):4081–4095, 2016.

[32] U. Martínez-Peñas. Hamming and simplex codes for the sum-rank metric. *Des. Codes Cryptogr.*, 88(8):1521–1539, 2020.

[33] J. L. Massey. Minimal codewords and secret sharing. In *Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pages 276–279, 1993.

[34] O. Polverino. Linear sets in finite projective spaces. *Discrete Math.*, 310(22):3096–3107, 2010.

[35] O. Polverino and F. Zullo. Connections between scattered linear sets and MRD-codes. *Bulletin of the ICA*, 89:46–74, 2020.

[36] T. H. Randrianarisoa. A geometric approach to rank metric codes and a classification of constant weight codes. *Des. Codes Cryptogr.*, 88(7):1331–1348, 2020.

[37] A. Ravagnani. Generalized weights: an anticode approach. *J. Pure Appl. Algebra*, 220(5):1946–1962, 2016.

[38] A. Ravagnani. Rank-metric codes and their duality theory. *Des. Codes Cryptogr.*, 80(1):197–216, 2016.

[39] J. Sheekey. A new family of linear maximum rank distance codes. *Adv. Math. Commun.*, 10(3):475–488, 2016.

[40] J. Sheekey. (Scattered) Linear Sets are to Rank-Metric Codes as Arcs are to Hamming-Metric Codes. In M. Greferath, C. Hollanti, and J. Rosenthal, editors, *Oberwolfach Report No. 13/2019*, 2019.

[41] J. Sheekey and G. Van de Voorde. Rank-metric codes, linear sets, and their duality. *Des. Codes Cryptogr.*, 88(4):655–675, 2020.

[42] D. Silva, F. R. Kschischang, and R. Kötter. A rank-metric approach to error control in random network coding. *IEEE Trans. Inform. Theory*, 54(9):3951–3967, 2008.

[43] C. Tang, Y. Qiu, Q. Liao, and Z. Zhou. Full characterization of minimal linear codes as cutting blocking sets. *IEEE Trans. Inform. Theory*, 67(6):3690–3700, 2021.

[44] M. A. Tsfasman and S. G. Vlăduţ. *Algebraic-geometric codes*, volume 58 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1991. Translated from the Russian by the authors.

[45] G. Zini and F. Zullo. Scattered subspaces and related codes. *Des. Codes Cryptogr.*, pages 1–21, 2021.

Appendix

Proof of Theorem 3.8. We prove a series of properties separately.

- $\Phi([\mathcal{C}])$ does not depend on the choice of the generator matrix G. Indeed, if G' is another generator matrix for $\mathcal{C}$ then there is an $\mathbb{F}_{q^m}$-linear map φ, such that $\varphi(G) = G'$. The same map sends the $\mathbb{F}_q$-columnspace of G into the $\mathbb{F}_q$-columnspace of G'.
- $\Phi([\mathcal{C}])$ does not depend on $\mathcal{C}$ but only on its equivalence class. To see this, let $\mathcal{C}'$ be a code linearly equivalent to $\mathcal{C}$, then there is a matrix $A \in \mathrm{GL}_n(q)$ such that $\mathcal{C}' = \mathcal{C} \cdot A$. Hence, if G is a generator matrix for $\mathcal{C}$, then GA is a generator matrix for $\mathcal{C}'$ and they have the same $\mathbb{F}_q$-columnspace. Hence, the map Φ does not depend on the choice of the representative.
- $\Phi([\mathcal{C}]) \in \mathcal{U}[n,k,d]_{q^m/q}$. To see this, let $[n',k',d']$ be the parameters of $\Phi([\mathcal{C}])$. We need to show that $(n,k,d) = (n',k',d')$. Since $\mathcal{C}$ has dimension k over $\mathbb{F}_{q^m}$ we have $k = k'$.

  In order to prove that $n = n'$, we use the fact that $\mathcal{C}$ is nondegenerate by assumption. More precisely, let G be a generator matrix for $\mathcal{C}$. Since $\mathcal{C}$ is nondegenerate, by Proposition 3.2, $n = \dim(\sigma^{\mathrm{rk}}(\mathcal{C}))$ is equal to the dimension of the $\mathbb{F}_q$-space of the columns of G, that is n'.

  Finally, denote by G a generator matrix of $\mathcal{C}$. By Lemma 3.7, for all nonzero $v \in \mathbb{F}_{q^m}^k$ we have
  $$\mathrm{rk}(vG) = n - \dim_{\mathbb{F}_q}(\Phi([\mathcal{C}]) \cap \langle v \rangle^{\perp}).$$
  As v ranges over the nonzero vectors in $\mathbb{F}_{q^m}^k$, $\langle v \rangle^{\perp}$ ranges over all $\mathbb{F}_{q^m}$-hyperplanes in $\mathbb{F}_{q^m}^k$. Therefore $d = d'$ by definition of d'.
- $\Psi([\mathcal{U}])$ does not depend on $\mathcal{U}$ but only on its equivalence class. To see this, assume $\mathcal{U}'$ is an $[n,k]_{q^m/q}$ system equivalent to $\mathcal{U}$, hence, there is an $\mathbb{F}_{q^m}$-isomorphism ϕ, such that $\phi(\mathcal{U}) = \mathcal{U}'$. In particular, if $\{g_1, \ldots, g_n\}$ is a basis of $\mathcal{U}$ and $\{g'_1, \ldots, g'_n\}$ is a basis of $\mathcal{U}'$, then $\phi(\{g'_1, \ldots, g'_n\}) = \{g'_1, \ldots, g'_n\}$. In particular, let G be the matrix whose i-th column is given by g_i and G' be the matrix whose i-th column is given by g'_i, then there is a matrix $A \in \mathrm{GL}_n(q)$, such that $G' = GA$. Hence, the rank-metric codes generated by G and G' are linearly equivalent. So, we conclude that Ψ does not depend on the choice of $\mathcal{U}$.
- $\Psi([\mathcal{U}]) \in \mathcal{C}[n,k,d]_{q^m/q}$. To see this, let $\{g_1, \ldots, g_n\}$ be an $\mathbb{F}_q$-basis of $\mathcal{U}$ and let $\mathcal{C}$ be the $[n',k',d']$ code whose generator matrix G has g_i as i-th column. Then, obviously, the length of $\mathcal{C}$ is $n' = n$. The rows of G are linearly independent over $\mathbb{F}_{q^m}$ otherwise there is $x \in \mathbb{F}_{q^m}^k$ such that $xg_i^{\top} = 0$ for all i. Hence, x defines an hyperplane containing $\mathcal{U}$,

which contradicts the fact that $\langle \mathcal{U} \rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^k$. This ensures that the dimension k' of $\mathcal{C}$ is equal to k. For a matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ we denote by G_i the i-th column of G. Now, for the distance, observe that for all $v \in \mathbb{F}_{q^m}^k$,

$$\begin{aligned} d' &= \min\{\omega^{\mathrm{H}}(vGA) \,:\, A \in \mathrm{GL}_n(q)\} \\ &= \min\{n - |\{i \,:\, (GA)_i \in \langle v \rangle^{\perp}\}|\} \\ &= n - \max\{\dim_{\mathbb{F}_q}(\mathcal{U} \cap H) \,:\, H \text{ is an } \mathbb{F}_{q^m}\text{-hyperplane in } \mathbb{F}_{q^m}^k\}, \end{aligned}$$

where the last equality follows from Equation (3.4). Finally, since the g_i's are linearly independent over $\mathbb{F}_q$, $\mathcal{C}$ is nondegenerate by Proposition 3.2.

All of this establishes the desired result. □

Generalized rank weights

In order to prove Theorem 3.14, we first recall the notion of generalized Hamming weight. Given an $[n,k]_{q^m/q}$ nondegenerate code $\mathcal{C}$, for every $r = 1, \dots, k$, the **r-th generalized Hamming weight** of $\mathcal{C}$ is defined as

$$d_r^{\mathrm{H}}(\mathcal{C}) = \min\{|\sigma^{\mathrm{H}}(V)| \,:\, V \subseteq \mathcal{C}, \dim(V) = r\}.$$

It is easy to see that for an $[n,k]_{q^m/q}$ rank-metric code $\mathcal{C}$ one has

$$d_r^{\mathrm{rk}}(\mathcal{C}) = \min\{d_r^{\mathrm{H}}(\mathcal{C} \cdot A) \,:\, A \in \mathrm{GL}_n(q)\}; \tag{6.7}$$

see e.g. [31, Theorem 2]. Recall also the following well-known result.

Lemma (see [44, Theorem 1.1.14])**.** Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code and G be a generator matrix for $\mathcal{C}$. Then

$$d_r^{\mathrm{H}}(\mathcal{C}) = \min\{n - |\{i \,:\, G_i \in H\}| \,:\, H \leq \mathbb{F}_{q^m}^k,\ \dim H \leq k - r\},$$

where G_i denotes the i-th column of G.

Proof of Theorem 3.14. Let G be a generator matrix of $\mathcal{C}$. Then, by the previous Lemma and Equation (6.7) we obtain that

$$d_r^{\mathrm{rk}}(\mathcal{C}) = n - \max\{|\{i \,:\, (GA)_i \in H\}| \,:\, A \in \mathrm{GL}_n(q),\ H \leq \mathbb{F}_{q^m}^k,\ \dim H \leq k - r\}.$$

Let $\mathcal{U}$ be the $\mathbb{F}_q$-span of the columns of G, i.e. $\mathcal{U}$ is an $[n,k]_{q^m/q}$ system corresponding to the equivalence class of $\mathcal{C}$. Note that, by Equation (3.4), for a fixed $H \subseteq \mathbb{F}_{q^m}^k$ with $\dim H \leq k - r$ we have that

$$\max\{|\{i \,:\, (GA)_i \in H\}| \,:\, A \in \mathrm{GL}_n(q)\} = \dim_{\mathbb{F}_q}(\mathcal{U} \cap H).$$

This concludes the proof. □