

Packing and Covering Properties of Rank Metric Codes

Maximilien Gadouleau and Zhiyuan Yan

Department of Electrical and Computer Engineering

Lehigh University, PA 18015, USA

E-mails: {magc, yan}@lehigh.edu

Abstract

This paper investigates packing and covering properties of codes with the rank metric. First, we investigate asymptotic packing properties of rank metric codes. Then, we study sphere covering properties of rank metric codes, derive bounds on their parameters, and investigate their asymptotic covering properties.

I. INTRODUCTION

Although the rank has long been known to be a metric implicitly and explicitly (see, for example, [1]), the rank metric was first considered for error control codes (ECCs) by Delsarte [2]. The potential applications of rank metric codes to wireless communications [3], [4], public-key cryptosystems [5], and storage equipments [6], [7] have motivated a steady stream of works [2], [6]–[22], described below, that focus on their properties.

The majority [2], [6]–[8], [11], [14]–[16], [18], [20], [21] of previous works focus on rank distance properties, code construction, and efficient decoding of rank metric codes. Some previous works focus on the packing and covering properties of rank metric codes. Both packing and covering properties are significant for ECCs, and packing and covering radii are basic geometric parameters of a code, important in several respects [23]. For instance, the covering radius can be viewed as a measure of performance: if the code is used for error correction, then the covering radius is the maximum weight of a correctable error vector [24]; if the code is used for data compression, then the covering radius is a measure of the maximum distortion [24]. The Hamming packing and covering radii of ECCs have been extensively studied (see, for example, [25]–[27]), whereas the rank packing and covering radii have received relatively

little attention. It was shown that nontrivial perfect rank metric codes do not exist in [9], [10], [19]. In [12], a sphere covering bound for rank metric codes was introduced. Generalizing the concept of rank covering radius, the multi-covering radii of codes with the rank metric were defined in [13]. Bounds on the volume of balls with rank radii were also derived [22].

In this paper, we investigate packing and covering properties of rank metric codes. The main contributions of this paper are:

- In Section III, we establish further properties of elementary linear subspaces (ELS's) [21], and investigate properties of balls with rank radii. In particular, we derive both upper and lower bounds on the volume of balls with given rank radii, and our bounds are tighter than their respective counterpart in [22]. These technical results are used later in our investigation of properties of rank metric codes.
- In Section IV, we study the packing properties of rank metric codes, and also derive the asymptotic maximum code rate for a code with given relative minimum rank distance.
- In Section V, we first derive both upper and lower bounds on the minimal cardinality of a code with given length and rank covering radius. Our new bounds are tighter than the bounds introduced in [12]. We also establish additional sphere covering properties for linear rank metric codes, and prove that some classes of rank metric codes have maximal covering radius. Finally, we establish the asymptotic minimum code rate for a code with given relative covering radius.

We provide the following remarks on our results:

- 1) The concept of elementary linear subspace was introduced in our previous work [21]. It has similar properties to those of a set of coordinates, and as such has served as a useful tool in our derivation of properties of the rank metric (see Section III), covering properties of rank metric codes (see Section V), and properties of Gabidulin codes (see [21]). Although our results may be derived without the concept of ELS, we have adopted it in this paper since it enables readers to easily relate our approach and results to their counterparts for Hamming metric codes.
- 2) Both the matrix form [2], [7] and the vector form [8] for rank metric codes have been considered in the literature. Following [8], in this paper the vector form over $\text{GF}(q^m)$ is used for rank metric codes although their rank weight is defined by their corresponding $m \times n$ code matrices over $\text{GF}(q)$ [8]. The vector form is chosen in this paper since our results and their derivations for rank metric codes can be readily related to their counterparts for Hamming metric codes.

The rest of the paper is organized as follows. Section II gives a brief review of necessary background

to keep this paper self-contained. In Section III, we derive some further properties of ELS's and balls of rank radii. In Sections IV and V, we investigate the packing and covering properties respectively of rank metric codes.

II. PRELIMINARIES

A. Rank metric and elementary linear subspaces

Consider an n -dimensional vector $\mathbf{x} = (x_0, x_1, \dots, x_{n-1}) \in \text{GF}(q^m)^n$. The field $\text{GF}(q^m)$ may be viewed as an m -dimensional vector space over $\text{GF}(q)$. The rank weight of \mathbf{x} , denoted as $\text{rk}(\mathbf{x})$, is defined to be the *maximum* number of coordinates in \mathbf{x} that are linearly independent over $\text{GF}(q)$ [8]. Note that all ranks are with respect to $\text{GF}(q)$ unless otherwise specified in this paper. The coordinates of \mathbf{x} thus span a linear subspace of $\text{GF}(q^m)^n$, denoted as $\mathfrak{S}(\mathbf{x})$, with dimension equal to $\text{rk}(\mathbf{x})$. For all $\mathbf{x}, \mathbf{y} \in \text{GF}(q^m)^n$, it is easily verified that $d_{\text{R}}(\mathbf{x}, \mathbf{y}) \stackrel{\text{def}}{=} \text{rk}(\mathbf{x} - \mathbf{y})$ is a metric over $\text{GF}(q^m)^n$ [8], referred to as the *rank metric* henceforth. The *minimum rank distance* of a code \mathcal{C} , denoted as $d_{\text{R}}(\mathcal{C})$, is simply the minimum rank distance over all possible pairs of distinct codewords. When there is no ambiguity about \mathcal{C} , we denote the minimum rank distance as d_{R} .

In [21], we introduced the concept of elementary linear subspace (ELS). If there exists a basis set B of vectors in $\text{GF}(q)^n$ for a linear subspace $\mathcal{V} \subseteq \text{GF}(q^m)^n$, we say \mathcal{V} is an elementary linear subspace and B is an elementary basis of \mathcal{V} . We denote the set of all ELS's of $\text{GF}(q^m)^n$ with dimension v as $E_v(q^m, n)$. An ELS has properties similar to those for a set of coordinates [21], and they are summarized as follows. A vector has rank $\leq r$ if and only if it belongs to some ELS with dimension r . For any $\mathcal{V} \in E_v(q^m, n)$, there exists $\bar{\mathcal{V}} \in E_{n-v}(q^m, n)$ such that $\mathcal{V} \oplus \bar{\mathcal{V}} = \text{GF}(q^m)^n$, where \oplus denotes the direct sum of two subspaces. For any vector $\mathbf{x} \in \text{GF}(q^m)^n$, we denote the projection of \mathbf{x} on \mathcal{V} along $\bar{\mathcal{V}}$ as $\mathbf{x}_{\mathcal{V}}$, and we remark that $\mathbf{x} = \mathbf{x}_{\mathcal{V}} + \mathbf{x}_{\bar{\mathcal{V}}}$.

B. The Singleton bounds

It can be shown that $d_{\text{R}} \leq d_{\text{H}}$ [8], where d_{H} is the minimum Hamming distance of the same code. Due to the Singleton bound for block codes, the minimum rank distance of an (n, k) block code over $\text{GF}(q^m)$ thus satisfies [8]

$$d_{\text{R}} \leq n - k + 1. \quad (1)$$

An alternative bound on the minimum rank distance is also given in [28]:

$$d_{\text{R}} \leq \frac{m}{n}(n - k) + 1. \quad (2)$$

For $n \leq m$, the bound in (1) is tighter than that in (2). When $n > m$ the bound in (2) is tighter.

When $n \leq m$, a class of vector codes satisfying (1) with equality was first proposed in [8] and then generalized in [16]. Let $\mathbf{g} = (g_0, g_1, \dots, g_{n-1})$ be linearly independent elements of $\text{GF}(q^m)$, then the code defined by the generator matrix

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-1} \\ g_0^{[1]} & g_1^{[1]} & \cdots & g_{n-1}^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_0^{[k-1]} & g_1^{[k-1]} & \cdots & g_{n-1}^{[k-1]} \end{pmatrix}, \quad (3)$$

where $[i] \stackrel{\text{def}}{=} q^{ai}$ with a being an integer prime to m , is called a generalized Gabidulin code generated by $\mathbf{g} = (g_0, g_1, \dots, g_{n-1})$; it has dimension k and minimum rank distance $d_R = n - k + 1$ [16].

A class of codes satisfying (2) with equality was proposed in [28]. It consists of cartesian products of a generalized Gabidulin code with length $n = m$. Let \mathcal{G} be an $(m, k, d_R = m - k + 1)$ generalized Gabidulin code over $\text{GF}(q^m)$, and let $\mathcal{G}^l \stackrel{\text{def}}{=} \mathcal{G} \times \dots \times \mathcal{G}$ be the code obtained by l cartesian products of \mathcal{G} . Thus \mathcal{G}^l is a code over $\text{GF}(q^m)$ with length ml , dimension kl , and minimum rank distance $d_R = m - k + 1$ [28].

C. Covering radius and excess

The covering radius ρ of a code C with length n over $\text{GF}(q^m)$ is defined to be the smallest integer ρ such that all vectors in the space $\text{GF}(q^m)^n$ are within distance ρ of some codeword of C [27]. It is the maximal distance from any vector in $\text{GF}(q^m)^n$ to the code C . That is, $\rho = \max_{\mathbf{x} \in \text{GF}(q^m)^n} \{d(\mathbf{x}, C)\}$. Also, if $C \subset C'$, then the covering radius of C is no less than the minimum distance of C' . Finally, a code C with length n and minimum distance d is called a maximal code if there does not exist any code C' with same length and minimum rank distance such that $C \subset C'$. A maximal code has covering radius $\rho \leq d - 1$.

Van Wee [29], [30] derived several bounds on codes with Hamming covering radii based on the excess of a code, which is determined by the number of codewords covering the same vectors. Below are some key definitions and results in [29], [30]. For all $V \subseteq \text{GF}(q^m)^n$ and a code C with covering radius ρ , the excess on V by C is defined to be

$$E_C(V) \stackrel{\text{def}}{=} \sum_{\mathbf{c} \in C} |B_\rho^H(\mathbf{c}) \cap V| - |V|, \quad (4)$$

where $B_\rho^H(\mathbf{c})$ denotes a ball centered at \mathbf{c} with Hamming radius ρ . The excess on $\text{GF}(q^m)^n$ by C is given by $E_C(\text{GF}(q^m)^n) = |C| \cdot V_\rho^H(q^m, n) - q^{mn}$, where $V_\rho^H(q^m, n)$ denotes the volume of a ball with Hamming

radius ρ . Also, if $\{W_i\}$ is a family of disjoint subsets of $\text{GF}(q^m)^n$, then $E_C(\bigcup_i W_i) = \sum_i E_C(W_i)$. Suppose $Z \stackrel{\text{def}}{=} \{\mathbf{z} \in \text{GF}(q^m)^n | E_C(\{\mathbf{z}\}) > 0\}$, i.e., Z is the set of vectors covered by at least two codewords in C . Note that $\mathbf{z} \in Z$ if and only if $|B_\rho^H(\mathbf{z}) \cap C| \geq 2$. It can be shown that $|Z| \leq E_C(Z) = E_C(\text{GF}(q^m)^n) = |C| \cdot V_\rho^H(q^m, n) - q^{mn}$.

Although the above definitions and properties were developed for the Hamming metric, they are in fact independent of the underlying metric and thus are applicable to the rank metric as well.

D. Notations

In order to simplify notations, we shall occasionally denote the vector space $\text{GF}(q^m)^n$ as F . We denote the number of vectors of rank u ($0 \leq u \leq \min\{m, n\}$) in $\text{GF}(q^m)^n$ as $N_u(q^m, n)$. It can be shown that $N_u(q^m, n) = \begin{bmatrix} n \\ u \end{bmatrix} \alpha(m, u)$ [8], where $\alpha(m, 0) \stackrel{\text{def}}{=} 1$ and $\alpha(m, u) \stackrel{\text{def}}{=} \prod_{i=0}^{u-1} (q^m - q^i)$ for $u \geq 1$. The $\begin{bmatrix} n \\ u \end{bmatrix}$ term is often referred to as a Gaussian polynomial [31], defined as $\begin{bmatrix} n \\ u \end{bmatrix} \stackrel{\text{def}}{=} \alpha(n, u) / \alpha(u, u)$. Note that $\begin{bmatrix} n \\ u \end{bmatrix}$ is the number of u -dimensional linear subspaces of $\text{GF}(q)^n$. We refer to all vectors in $\text{GF}(q^m)^n$ within rank distance r of $\mathbf{x} \in \text{GF}(q^m)^n$ as a ball of rank radius r centered at \mathbf{x} , and denote it as $B_r(\mathbf{x})$. Its volume, which does not depend on \mathbf{x} , is denoted as $V_r(q^m, n) = \sum_{u=0}^r N_u(q^m, n)$.

III. TECHNICAL RESULTS

A. Further properties of ELS's

Lemma 1: Any vector $\mathbf{x} \in \text{GF}(q^m)^n$ with rank r belongs to a unique ELS $\mathcal{V} \in E_r(q^m, n)$.

Proof: The existence of $\mathcal{V} \in E_r(q^m, n)$ has been proved in [21]. Thus we only prove the uniqueness of \mathcal{V} , with elementary basis $\{\mathbf{v}_i\}_{i=0}^{r-1}$. Suppose \mathbf{x} also belongs to \mathcal{W} , where $\mathcal{W} \in E_r(q^m, n)$ has an elementary basis $\{\mathbf{w}_j\}_{j=0}^{r-1}$. Therefore, $\mathbf{x} = \sum_{i=0}^{r-1} a_i \mathbf{v}_i = \sum_{j=0}^{r-1} b_j \mathbf{w}_j$, where $a_i, b_j \in \text{GF}(q^m)$ for $0 \leq i, j \leq r-1$. By definition, we have $\mathfrak{S}(\mathbf{x}) = \mathfrak{S}(a_0, \dots, a_{r-1}) = \mathfrak{S}(b_0, \dots, b_{r-1})$, therefore b_j 's can be expressed as linear combinations of a_i 's, i.e., $b_j = \sum_{i=0}^{r-1} c_{j,i} a_i$ where $c_{j,i} \in \text{GF}(q)$. Hence

$$\mathbf{x} = \sum_{j=0}^{r-1} b_j \mathbf{w}_j = \sum_{j=0}^{r-1} \sum_{i=0}^{r-1} c_{j,i} a_i \mathbf{w}_j = \sum_{i=0}^{r-1} a_i \mathbf{u}_i, \quad (5)$$

where $\mathbf{u}_i = \sum_{j=0}^{r-1} c_{j,i} \mathbf{w}_j \in \text{GF}(q)^n$. Now consider \mathbf{X} , the matrix obtained by expanding the coordinates of \mathbf{x} with respect to the basis $\{a_i\}_{i=0}^{r-1}$. For $0 \leq i \leq r-1$, the i -th row of \mathbf{X} is given by the vector \mathbf{v}_i by definition and by the vector \mathbf{u}_i from Eq. (5). Therefore $\mathbf{v}_i = \mathbf{u}_i \in \mathcal{W}$, and hence $\mathcal{V} \subseteq \mathcal{W}$. However, $\dim(\mathcal{V}) = \dim(\mathcal{W})$, and thus $\mathcal{V} = \mathcal{W}$. ■

Lemma 1 shows that an ELS is analogous to a subset of coordinates since a vector \mathbf{x} with Hamming weight r belongs to a unique subset of r coordinates, often referred to as the support of \mathbf{x} .

In [21], it was shown that an ELS always has a complementary elementary linear subspace. The following lemma enumerates such complementary ELS's.

Lemma 2: Suppose $\mathcal{V} \in E_v(q^m, n)$ and $\mathcal{A} \subseteq \mathcal{V}$ is an ELS with dimension a , then there are $q^{a(v-a)}$ ELS's \mathcal{B} such that $\mathcal{A} \oplus \mathcal{B} = \mathcal{V}$. Furthermore, there are $q^{a(v-a)} \begin{bmatrix} v \\ a \end{bmatrix}$ such ordered pairs $(\mathcal{A}, \mathcal{B})$.

Proof: First, remark that $\dim(\mathcal{B}) = v - a$. The total number of sets of $v - a$ linearly independent vectors over $\text{GF}(q)$ in $\mathcal{V} \setminus \mathcal{A}$ is given by $N = (q^v - q^a)(q^v - q^{a+1}) \cdots (q^v - q^{v-1}) = q^{a(v-a)} \alpha(v-a, v-a)$. Note that each set of linearly independent vectors over $\text{GF}(q)$ constitutes an elementary basis set. Thus, the number of possible \mathcal{B} is given by N divided by $\alpha(v-a, v-a)$, the number of elementary basis sets for each \mathcal{B} . Therefore, once \mathcal{A} is fixed, there are $q^{a(v-a)}$ choices for \mathcal{B} . Since the number of a -dimensional subspaces \mathcal{A} in \mathcal{V} is $\begin{bmatrix} v \\ a \end{bmatrix}$, the total number of ordered pairs $(\mathcal{A}, \mathcal{B})$ is hence $q^{a(v-a)} \begin{bmatrix} v \\ a \end{bmatrix}$. ■

Puncturing a vector with full Hamming weight results in another vector with full Hamming weight. Lemma 3 below shows that the situation for vectors with full rank is similar.

Lemma 3: Suppose $\mathcal{V} \in E_v(q^m, n)$ and $\mathbf{u} \in \mathcal{V}$ has rank v , then $\text{rk}(\mathbf{u}_{\mathcal{A}}) = a$ and $\text{rk}(\mathbf{u}_{\mathcal{B}}) = v - a$ for any $\mathcal{A} \in E_a(q^m, n)$ and $\mathcal{B} \in E_{v-a}(q^m, n)$ such that $\mathcal{A} \oplus \mathcal{B} = \mathcal{V}$.

Proof: First, $\mathbf{u}_{\mathcal{A}} \in \mathcal{A}$ and hence $\text{rk}(\mathbf{u}_{\mathcal{A}}) \leq a$ by [21, Proposition 2]; similarly, $\text{rk}(\mathbf{u}_{\mathcal{B}}) \leq v - a$. Now suppose $\text{rk}(\mathbf{u}_{\mathcal{A}}) < a$ or $\text{rk}(\mathbf{u}_{\mathcal{B}}) < v - a$, then $v = \text{rk}(\mathbf{u}) \leq \text{rk}(\mathbf{u}_{\mathcal{A}}) + \text{rk}(\mathbf{u}_{\mathcal{B}}) < a + v - a = v$. ■

It was shown in [21] that the projection $\mathbf{u}_{\mathcal{A}}$ of a vector \mathbf{u} on an ELS \mathcal{A} depends on both \mathcal{A} and its complement \mathcal{B} . The following lemma further clarifies the relationship: changing \mathcal{B} always modifies $\mathbf{u}_{\mathcal{A}}$, provided that \mathbf{u} has full rank.

Lemma 4: Suppose $\mathcal{V} \in E_v(q^m, n)$ and $\mathbf{u} \in \mathcal{V}$ has rank v . For any $\mathcal{A} \in E_a(q^m, n)$ and $\mathcal{B} \in E_{v-a}(q^m, n)$ such that $\mathcal{A} \oplus \mathcal{B} = \mathcal{V}$, define the functions $f_{\mathbf{u}}(\mathcal{A}, \mathcal{B}) = \mathbf{u}_{\mathcal{A}}$ and $g_{\mathbf{u}}(\mathcal{A}, \mathcal{B}) = \mathbf{u}_{\mathcal{B}}$. Then both $f_{\mathbf{u}}$ and $g_{\mathbf{u}}$ are injective.

Proof: Consider another pair $(\mathcal{A}', \mathcal{B}')$ with dimensions a and $v - a$ respectively. Suppose $\mathcal{A}' \neq \mathcal{A}$, then $\mathbf{u}_{\mathcal{A}'} \neq \mathbf{u}_{\mathcal{A}}$. Otherwise $\mathbf{u}_{\mathcal{A}}$ belongs to two distinct ELS's with dimension a , which contradicts Lemma 1. Hence $\mathbf{u}_{\mathcal{A}'} \neq \mathbf{u}_{\mathcal{A}}$ and $\mathbf{u}_{\mathcal{B}'} = \mathbf{u} - \mathbf{u}_{\mathcal{A}'} \neq \mathbf{u} - \mathbf{u}_{\mathcal{A}} = \mathbf{u}_{\mathcal{B}}$. The argument is similar if $\mathcal{B}' \neq \mathcal{B}$. ■

B. Properties of balls with rank radii

Lemma 5: For $0 \leq r \leq \min\{n, m\}$,

$$q^{r(m+n-r)} \leq V_r(q^m, n) < q^{r(m+n-r)+\sigma(q)}, \quad (6)$$

where $\sigma(q) \stackrel{\text{def}}{=} \frac{1}{\ln(q)} \sum_{k=1}^{\infty} \frac{1}{k(q^k-1)}$ is a decreasing function of q satisfying $\sigma(q) < 2$ for $q \geq 2$ [21].

Proof: The upper bound in (6) was derived in [21, Lemma 13], and it suffices to prove the lower bound. Without loss of generality, we assume that the center of the ball is $\mathbf{0}$. We associate each $\mathbf{x} \in \text{GF}(q^m)^r$ with one subspace \mathfrak{T} of $\text{GF}(q^m)$ such that $\dim(\mathfrak{T}) = r$ and $\mathfrak{S}(\mathbf{x}) \subseteq \mathfrak{T}$. We consider the vectors $\mathbf{y} \in \text{GF}(q^m)^{n-r}$ such that $\mathfrak{S}(\mathbf{y}) \subseteq \mathfrak{T}$. There are q^{mr} choices for \mathbf{x} and, for a given \mathbf{x} , $q^{r(n-r)}$ choices for \mathbf{y} . Thus the total number of vectors $\mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \text{GF}(q^m)^n$ is $q^{r(m+n-r)}$. Since $\mathfrak{S}(\mathbf{z}) \subseteq \mathfrak{T}$, we have $\text{rk}(\mathbf{z}) \leq r$ and $\mathbf{z} \in B_r(\mathbf{0})$. Thus, $V_r(q^m, n) \geq q^{r(m+n-r)}$. ■

We remark that both bounds in (6) are tighter than their respective counterparts in [22, Proposition 1]. More importantly, the two bounds in (6) differ only by a factor of $q^{\sigma(q)}$, and thus they not only provide a good approximation of $V_r(q^m, n)$, but also accurately describe the asymptotic behavior of $V_r(q^m, n)$.

The diameter of a set is defined to be the maximum distance between any pair of elements in the set [25, p. 172]. For a binary vector space $\text{GF}(2)^n$ and a given diameter $2r < n$, Kleitman [32] proved that balls with Hamming radius r maximize the cardinality of a set with a given diameter. However, when the underlying field for the vector space is not $\text{GF}(2)$, the result is not necessarily valid [27, p. 40]. We show below that balls with rank radii do not necessarily maximize the cardinality of a set with a given diameter.

Proposition 1: For $3 \leq n \leq m$ and $2 \leq 2r < n$, there exists $S \subset \text{GF}(q^m)^n$ with diameter $2r$ such that $|S| > V_r(q^m, n)$.

Proof: The set $S \stackrel{\text{def}}{=} \{(x_0, \dots, x_{n-1}) \in \text{GF}(q^m)^n \mid x_{2r} = \dots = x_{n-1} = 0\}$ has diameter $2r$ and cardinality q^{2mr} . For $r = 1$, we have $V_1(q^m, n) = 1 + \frac{(q^n-1)(q^m-1)}{(q-1)} < q^{2m}$. For $r \geq 2$, we have $V_r(q^m, n) < q^{r(n+m)-r^2-\sigma(q)}$ by Lemma 5. Since $r^2 > 2 > \sigma(q)$, we obtain $V_r(q^m, n) < q^{r(n+m)} \leq |S|$. ■

The intersection of balls with Hamming radii has been studied in [27, Chapter 2], and below we investigate the intersection of balls with rank radii.

Lemma 6: If $0 \leq r, s \leq n$ and $\mathbf{c}_1, \mathbf{c}_2 \in \text{GF}(q^m)^n$, then $|B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)|$ depends on \mathbf{c}_1 and \mathbf{c}_2 only through $d_R(\mathbf{c}_1, \mathbf{c}_2)$.

Proof: First, without loss of generality, we assume $\mathbf{c}_1 = \mathbf{0}$, and we denote $\text{rk}(\mathbf{c}_2) = e$. We can express \mathbf{c}_2 as $\mathbf{c}_2 = \mathbf{uB}$, where $\mathbf{u} = (u_0, \dots, u_{e-1}, 0, \dots, 0) \in \text{GF}(q^m)^n$ has rank e and $\mathbf{B} \in \text{GF}(q)^{n \times n}$ has full rank. For any $\mathbf{x} \in B_r(\mathbf{0}) \cap B_s(\mathbf{u})$ we have $\text{rk}(\mathbf{xB}) = \text{rk}(\mathbf{x}) \leq r$ and $\text{rk}(\mathbf{xB} - \mathbf{c}_2) = \text{rk}(\mathbf{x} - \mathbf{u}) \leq s$. Thus there is a bijection between $B_r(\mathbf{0}) \cap B_s(\mathbf{uB})$ and $B_r(\mathbf{0}) \cap B_s(\mathbf{u})$. Hence $|B_r(\mathbf{0}) \cap B_s(\mathbf{uB})| = |B_r(\mathbf{0}) \cap B_s(\mathbf{u})|$, that is, $|B_r(\mathbf{0}) \cap B_s(\mathbf{uB})|$ does not depend on \mathbf{B} .

Since $|B_r(\mathbf{0}) \cap B_s(\mathbf{uB})|$ is independent of \mathbf{B} , we assume $\mathbf{B} = \mathbf{I}_{n \times n}$ without loss of generality henceforth. The nonzero coordinates of \mathbf{u} all belong to a basis set $\{u_i\}_{i=0}^{e-1}$ of $\text{GF}(q^m)$. Let $\mathbf{x} =$

$(x_0, \dots, x_{n-1}) \in B_r(\mathbf{0}) \cap B_s(\mathbf{u})$, then we can express x_j as $x_j = \sum_{i=0}^{m-1} a_{i,j} u_i$ with $a_{i,j} \in \text{GF}(q)$ for $0 \leq j \leq n-1$. Suppose $\mathbf{v} = (v_0, \dots, v_{e-1}, 0, \dots, 0) \in \text{GF}(q^m)^n$ also has rank e , then the nonzero coordinates of \mathbf{v} all belong to a basis set $\{v_i\}_{i=0}^{m-1}$ of $\text{GF}(q^m)$. We define $\bar{\mathbf{x}} = (\bar{x}_0, \dots, \bar{x}_{n-1}) \in \text{GF}(q^m)^n$ such that $\bar{x}_j = \sum_{i=0}^{m-1} a_{i,j} v_i$ for $0 \leq j \leq n-1$. We remark that $\text{rk}(\bar{\mathbf{x}}) = \text{rk}(\mathbf{x}) \leq r$ and $\text{rk}(\bar{\mathbf{x}} - \mathbf{v}) = \text{rk}(\mathbf{x} - \mathbf{u}) \leq s$. Thus there is a bijection between $B_r(\mathbf{0}) \cap B_s(\mathbf{v})$ and $B_r(\mathbf{0}) \cap B_s(\mathbf{u})$. Hence $|B_r(\mathbf{0}) \cap B_s(\mathbf{u})|$ depends on the vector \mathbf{u} only through its rank e . ■

Proposition 2: If $0 \leq r, s \leq n$, $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}'_1, \mathbf{c}'_2 \in \text{GF}(q^m)^n$ and $d_r(\mathbf{c}_1, \mathbf{c}_2) > d_r(\mathbf{c}'_1, \mathbf{c}'_2)$, then

$$|B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)| \leq |B_r(\mathbf{c}'_1) \cap B_s(\mathbf{c}'_2)|. \quad (7)$$

Proof: It suffices to prove (7) when $d_r(\mathbf{c}_1, \mathbf{c}_2) = d_r(\mathbf{c}'_1, \mathbf{c}'_2) + 1 = e + 1$. By Lemma 6, we can assume without loss of generality that $\mathbf{c}_1 = \mathbf{c}'_1 = \mathbf{0}$, $\mathbf{c}'_2 = (0, c_1, \dots, c_e, 0, \dots, 0)$ and $\mathbf{c}_2 = (c_0, c_1, \dots, c_e, 0, \dots, 0)$, where $c_0, \dots, c_e \in \text{GF}(q^m)$ are linearly independent.

We will show that an injective mapping ϕ from $B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)$ to $B_r(\mathbf{c}'_1) \cap B_s(\mathbf{c}'_2)$ can be constructed. We consider vectors $\mathbf{z} = (z_0, z_1, \dots, z_{n-1}) \in B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)$. We thus have $\text{rk}(\mathbf{z}) \leq r$ and $\text{rk}(\mathbf{u}) \leq s$, where $\mathbf{u} = (u_0, u_1, \dots, u_{n-1}) = \mathbf{z} - \mathbf{c}_2 = (z_0 - c_0, z_1 - c_1, \dots, z_{n-1})$. We also define $\bar{\mathbf{z}} = (z_1, \dots, z_{n-1})$ and $\bar{\mathbf{u}} = (u_1, \dots, u_{n-1})$. We consider three cases for the mapping ϕ , depending on $\bar{\mathbf{z}}$ and $\bar{\mathbf{u}}$.

- Case I: $\text{rk}(\bar{\mathbf{u}}) \leq s - 1$. In this case, $\phi(\mathbf{z}) \stackrel{\text{def}}{=} \mathbf{z}$. We remark that $\text{rk}(\mathbf{z} - \mathbf{c}'_2) \leq \text{rk}(\bar{\mathbf{u}}) + 1 \leq s$ and hence $\phi(\mathbf{z}) \in B_r(\mathbf{c}'_1) \cap B_s(\mathbf{c}'_2)$.
- Case II: $\text{rk}(\bar{\mathbf{u}}) = s$ and $\text{rk}(\bar{\mathbf{z}}) \leq r - 1$. In this case, $\phi(\mathbf{z}) \stackrel{\text{def}}{=} (z_0 - c_0, z_1, \dots, z_{n-1})$. We have $\text{rk}(\phi(\mathbf{z})) \leq \text{rk}(\bar{\mathbf{z}}) + 1 \leq r$ and $\text{rk}(\phi(\mathbf{z}) - \mathbf{c}'_2) = \text{rk}(\mathbf{z} - \mathbf{c}_2) \leq s$, and hence $\phi(\mathbf{z}) \in B_r(\mathbf{c}'_1) \cap B_s(\mathbf{c}'_2)$.
- Case III: $\text{rk}(\bar{\mathbf{u}}) = s$ and $\text{rk}(\bar{\mathbf{z}}) = r$. Since $\text{rk}(\mathbf{u}) = s$, we have $z_0 - c_0 \in \mathfrak{S}(\bar{\mathbf{u}})$. Similarly, since $\text{rk}(\mathbf{z}) = r$, we have $z_0 \in \mathfrak{S}(\bar{\mathbf{z}})$. Denote $\dim(\mathfrak{S}(\bar{\mathbf{u}}, \bar{\mathbf{z}}))$ as d ($d \geq s$). For $d > s$, let $\alpha_0, \dots, \alpha_{d-1}$ be a basis of $\mathfrak{S}(\bar{\mathbf{u}}, \bar{\mathbf{z}})$ such that $\alpha_0, \dots, \alpha_{s-1} \in \mathfrak{S}(\bar{\mathbf{u}})$ and $\alpha_s, \dots, \alpha_{d-1} \in \mathfrak{S}(\bar{\mathbf{z}})$. Note that $c_0 \in \mathfrak{S}(\bar{\mathbf{u}}, \bar{\mathbf{z}})$, and may therefore be uniquely expressed as $c_0 = c_u + c_z$, where $c_u \in \mathfrak{S}(\alpha_0, \dots, \alpha_{s-1}) \subseteq \mathfrak{S}(\bar{\mathbf{u}})$ and $c_z \in \mathfrak{S}(\alpha_s, \dots, \alpha_{d-1}) \subseteq \mathfrak{S}(\bar{\mathbf{z}})$. If $d = s$, then $c_z = 0 \in \mathfrak{S}(\bar{\mathbf{z}})$. In this case, $\phi(\mathbf{z}) \stackrel{\text{def}}{=} (z_0 - c_z, z_1, \dots, z_{n-1})$. Remark that $z_0 - c_z \in \mathfrak{S}(\bar{\mathbf{z}})$ and hence $\text{rk}(\phi(\mathbf{z})) = r$. Also, $z_0 - c_z = z_0 - c_0 + c_u \in \mathfrak{S}(\bar{\mathbf{u}})$ and hence $\text{rk}(\phi(\mathbf{z}) - \mathbf{c}'_2) = s$. Therefore $\phi(\mathbf{z}) \in B_r(\mathbf{c}'_1) \cap B_s(\mathbf{c}'_2)$.

We now verify that the mapping ϕ is injective. Suppose there exists \mathbf{z}' such that $\phi(\mathbf{z}') = \phi(\mathbf{z})$. Since $\phi(\mathbf{z})$ only modifies the first coordinate of \mathbf{z} , the last $n - 1$ coordinates of \mathbf{z} and \mathbf{z}' are equal and so are the last $n - 1$ coordinates of $\mathbf{z} - \mathbf{c}_2$ and $\mathbf{z}' - \mathbf{c}_2$. Hence \mathbf{z} and \mathbf{z}' belong to the same case. It can be easily verified that for each case above, ϕ is injective. Hence $\phi(\mathbf{z}') = \phi(\mathbf{z})$ implies that $\mathbf{z}' = \mathbf{z}$. Therefore ϕ is injective, and $|B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)| \leq |B_r(\mathbf{c}'_1) \cap B_s(\mathbf{c}'_2)|$. ■

Corollary 1: If $0 \leq r, s \leq n$, $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}'_1, \mathbf{c}'_2 \in \text{GF}(q^m)^n$ and $d_{\mathbf{R}}(\mathbf{c}_1, \mathbf{c}_2) \geq d_{\mathbf{R}}(\mathbf{c}'_1, \mathbf{c}'_2)$, then

$$|B_r(\mathbf{c}_1) \cup B_s(\mathbf{c}_2)| \geq |B_r(\mathbf{c}'_1) \cup B_s(\mathbf{c}'_2)|. \quad (8)$$

Proof: The result follows from $|B_r(\mathbf{c}_1) \cup B_s(\mathbf{c}_2)| = V_r(q^m, n) + V_s(q^m, n) - |B_r(\mathbf{c}_1) \cap B_s(\mathbf{c}_2)|$. ■

We now quantify the volume of the intersection of two balls with rank radii for some special cases, which will be used in Section V-B.

Proposition 3: If $\mathbf{c}_1, \mathbf{c}_2 \in \text{GF}(q^m)^n$ and $d_{\mathbf{R}}(\mathbf{c}_1, \mathbf{c}_2) = r$, then $|B_r(\mathbf{c}_1) \cap B_1(\mathbf{c}_2)| = 1 + (q^m - q^r) \begin{bmatrix} r \\ 1 \end{bmatrix} + (q^r - 1) \begin{bmatrix} n \\ 1 \end{bmatrix}$.

Proof: The claim holds for $r = m$ trivially, and we assume $r < m$ henceforth. By Lemma 6, assume $\mathbf{c}_2 = \mathbf{0}$ and hence $\text{rk}(\mathbf{c}_1) = r$ without loss of generality. By Lemma 1, the vector \mathbf{c}_1 belongs to a unique ELS $\mathcal{V} \in E_r(q^m, n)$. First of all, it is easy to check that $\mathbf{y} = \mathbf{0} \in B_r(\mathbf{c}_1) \cap B_1(\mathbf{0})$. We consider a nonzero vector $\mathbf{y} \in B_1(\mathbf{0})$ with rank 1. Firstly, if $\mathbf{y} \in \mathcal{V}$, then $\mathbf{c}_1 - \mathbf{y} \in \mathcal{V}$. We hence have $\text{rk}(\mathbf{c}_1 - \mathbf{y}) \leq r$ and $\mathbf{y} \in B_r(\mathbf{c}_1)$. Note that there are $(q^m - 1) \begin{bmatrix} r \\ 1 \end{bmatrix}$ such vectors. Secondly, if $\mathbf{y} \notin \mathcal{V}$ and $\mathfrak{S}(\mathbf{y}) \subseteq \mathfrak{S}(\mathbf{c}_1)$, then $\mathfrak{S}(\mathbf{c}_1 - \mathbf{y}) \subseteq \mathfrak{S}(\mathbf{c}_1)$. We hence have $\text{rk}(\mathbf{c}_1 - \mathbf{y}) \leq r$ and $\mathbf{y} \in B_r(\mathbf{c}_1)$. Note that there are $(q^r - 1)(\begin{bmatrix} n \\ 1 \end{bmatrix} - \begin{bmatrix} r \\ 1 \end{bmatrix})$ such vectors. Finally, suppose $\mathbf{y} \notin \mathcal{V}$ and $\mathfrak{S}(\mathbf{y}) \not\subseteq \mathfrak{S}(\mathbf{c}_1)$. Denote the linearly independent coordinates of \mathbf{c}_1 as $\alpha_0, \dots, \alpha_{r-1}$ and a nonzero coordinate of \mathbf{y} as $\alpha_r \notin \mathfrak{S}(\mathbf{c}_1)$, where $\{\alpha_i\}_{i=0}^{m-1}$ is a basis set of $\text{GF}(q^m)$. Then the matrix $\mathbf{C}_1 - \mathbf{Y}$ obtained by expanding the coordinates of $\mathbf{c}_1 - \mathbf{y}$ according to the basis $\{\alpha_i\}$ has row rank $r + 1$. Therefore $\text{rk}(\mathbf{c}_1 - \mathbf{y}) = r + 1$, and $\mathbf{y} \notin B_r(\mathbf{c}_1)$. ■

Proposition 4: If $\mathbf{c}_1, \mathbf{c}_2 \in \text{GF}(q^m)^n$ and $d_{\mathbf{R}}(\mathbf{c}_1, \mathbf{c}_2) = r$, then $|B_s(\mathbf{c}_1) \cap B_{r-s}(\mathbf{c}_2)| = q^{s(r-s)} \begin{bmatrix} r \\ s \end{bmatrix}$ for $0 \leq s \leq r$.

Proof: By Lemma 6, we can assume that $\mathbf{c}_1 = \mathbf{0}$, and hence $\text{rk}(\mathbf{c}_2) = r$. By Lemma 1, \mathbf{c}_2 belongs to a unique ELS $\mathcal{V} \in E_r(q^m, n)$. We first prove that all vectors $\mathbf{y} \in B_s(\mathbf{0}) \cap B_{r-s}(\mathbf{c}_2)$ are in \mathcal{V} . Let $\mathbf{y} = \mathbf{y}_{\mathcal{V}} + \mathbf{y}_{\mathcal{W}}$, where $\mathcal{W} \in E_{n-r}(q^m, n)$ such that $\mathcal{V} \oplus \mathcal{W} = \text{GF}(q^m)^n$. We have $\mathbf{y}_{\mathcal{V}} + (\mathbf{c}_2 - \mathbf{y})_{\mathcal{V}} = \mathbf{c}_2$, with $\text{rk}(\mathbf{y}_{\mathcal{V}}) \leq \text{rk}(\mathbf{y}) \leq s$ and $\text{rk}((\mathbf{c}_2 - \mathbf{y})_{\mathcal{V}}) \leq \text{rk}(\mathbf{c}_2 - \mathbf{y}) \leq r - s$. Therefore, $\text{rk}(\mathbf{y}_{\mathcal{V}}) = \text{rk}(\mathbf{y}) = s$, $\text{rk}((\mathbf{c}_2 - \mathbf{y})_{\mathcal{V}}) = \text{rk}(\mathbf{c}_2 - \mathbf{y}) = r - s$, and $\mathfrak{S}(\mathbf{y}_{\mathcal{V}}) \cap \mathfrak{S}((\mathbf{c}_2 - \mathbf{y})_{\mathcal{V}}) = \{0\}$. Since $\text{rk}(\mathbf{y}_{\mathcal{V}}) = \text{rk}(\mathbf{y})$, we have $\mathfrak{S}(\mathbf{y}_{\mathcal{W}}) \subseteq \mathfrak{S}(\mathbf{y}_{\mathcal{V}})$; and similarly $\mathfrak{S}((\mathbf{c}_2 - \mathbf{y})_{\mathcal{W}}) \subseteq \mathfrak{S}((\mathbf{c}_2 - \mathbf{y})_{\mathcal{V}})$. Altogether, we obtain $\mathfrak{S}(\mathbf{y}_{\mathcal{W}}) \cap \mathfrak{S}((\mathbf{c}_2 - \mathbf{y})_{\mathcal{W}}) = \{0\}$. However, $\mathbf{y}_{\mathcal{W}} + (\mathbf{c}_2 - \mathbf{y})_{\mathcal{W}} = \mathbf{0}$, and hence $\mathbf{y}_{\mathcal{W}} = (\mathbf{c}_2 - \mathbf{y})_{\mathcal{W}} = \mathbf{0}$. Therefore, $\mathbf{y} \in \mathcal{V}$.

We now prove that \mathbf{y} is necessarily the projection of \mathbf{c}_2 onto some ELS \mathcal{A} of \mathcal{V} . If $\mathbf{y} \in \mathcal{V}$ satisfies $\text{rk}(\mathbf{y}) = s$ and $\text{rk}(\mathbf{c}_2 - \mathbf{y}) = r - s$, then \mathbf{y} belongs to some ELS \mathcal{A} and $\mathbf{c}_2 - \mathbf{y} \in \mathcal{B}$ such that $\mathcal{A} \oplus \mathcal{B} = \mathcal{V}$. We hence have $\mathbf{y} = \mathbf{c}_{2,\mathcal{A}}$ and $\mathbf{c}_2 - \mathbf{y} = \mathbf{c}_{2,\mathcal{B}}$.

On the other hand, for any $\mathcal{A} \in E_s(q^m, n)$ and $\mathcal{B} \in E_{r-s}(q^m, n)$ such that $\mathcal{A} \oplus \mathcal{B} = \mathcal{V}$, $\mathbf{c}_{2,\mathcal{A}}$ is a vector of rank s with distance $r - s$ from \mathbf{c}_2 by Lemma 3. By Lemma 4, all the $\mathbf{c}_{2,\mathcal{A}}$ vectors are distinct. There are thus as many vectors \mathbf{y} as ordered pairs $(\mathcal{A}, \mathcal{B})$. By Lemma 2, there are $q^{s(r-s)} \begin{bmatrix} r \\ s \end{bmatrix}$ such pairs, and hence $q^{s(r-s)} \begin{bmatrix} r \\ s \end{bmatrix}$ vectors \mathbf{y} . ■

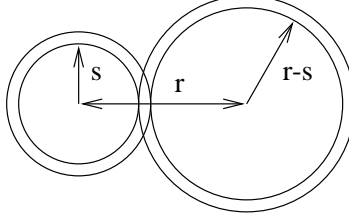


Fig. 1. Illustration of Proposition 4.

As shown in Figure 1, only the outmost layers of two balls of radii s and $r - s$ intersect when the distance between the two centers is r . Proposition 4 quantifies the volume of the intersection in Figure 1.

The problem of the intersection of three balls with rank radii is more complicated since the volume of the intersection of three balls with rank radii is not completely determined by the pairwise distances between the centers. We give a simple example to illustrate this point: consider $\text{GF}(2^2)^3$ and the vectors $\mathbf{c}_1 = \mathbf{c}'_1 = (0, 0, 0)$, $\mathbf{c}_2 = \mathbf{c}'_2 = (1, \alpha, 0)$, $\mathbf{c}_3 = (\alpha, 0, 1)$, and $\mathbf{c}'_3 = (\alpha, \alpha + 1, 0)$, where α is a primitive element of the field. It can be verified that $d_R(\mathbf{c}_1, \mathbf{c}_2) = d_R(\mathbf{c}_2, \mathbf{c}_3) = d_R(\mathbf{c}_3, \mathbf{c}_1) = 2$ and $d_R(\mathbf{c}'_1, \mathbf{c}'_2) = d_R(\mathbf{c}'_2, \mathbf{c}'_3) = d_R(\mathbf{c}'_3, \mathbf{c}'_1) = 2$. However, $B_1(\mathbf{c}_1) \cap B_1(\mathbf{c}_2) \cap B_1(\mathbf{c}_3) = \{(\alpha + 1, 0, 0)\}$, whereas $B_1(\mathbf{c}'_1) \cap B_1(\mathbf{c}'_2) \cap B_1(\mathbf{c}'_3) = \{(1, 0, 0), (0, \alpha + 1, 0), (\alpha, \alpha, 0)\}$. We remark that this is similar to the problem of the intersection of three balls with Hamming radii discussed in [27, p. 58], provided that the underlying field $\text{GF}(q^m)$ is not $\text{GF}(2)$.

IV. PACKING PROPERTIES OF RANK METRIC CODES

Combining (1) and (2) and generalizing slightly to account for nonlinear codes, we can show that the cardinality K of a code C over $\text{GF}(q^m)$ with length n and minimum rank distance d_R satisfies

$$K \leq \min \left\{ q^{m(n-d_R+1)}, q^{n(m-d_R+1)} \right\}. \quad (9)$$

In this paper, we call the bound in (9) the Singleton bound¹ for codes with the rank metric, and refer to codes that attain the Singleton bound as maximum rank distance (MRD) codes.

¹The Singleton bound in [7] has a different form since array codes are defined over base fields.

We refer to MRD codes over $\text{GF}(q^m)$ with length $n \leq m$ and with length $n > m$ as Class-I and Class-II MRD codes respectively. For any given parameter set n , m , and d_R , explicit construction for linear or nonlinear MRD codes exists. For $n \leq m$ and $d_R \leq n$, generalized Gabidulin codes can be constructed, and thus they constitute a *subclass* of linear Class-I MRD codes. For $n > m$ and $d_R \leq m$, a Class-II MRD code can be constructed by transposing a generalized Gabidulin code of length m and minimum rank distance d_R over $\text{GF}(q^n)$, although this code is not necessarily linear over $\text{GF}(q^m)$. When $n = lm$ ($l \geq 2$), linear Class-II MRD codes of length n and minimum distance d_R can be constructed by a cartesian product \mathcal{G}^l of an (m, k) linear Class-I MRD code \mathcal{G} (cf. Section II-B). Although maximum distance separable (MDS) codes, which attain the Singleton bound for the Hamming metric, exist only for limited block length over any given field, MRD codes can be constructed for any block length n and minimum rank distance d_R over arbitrary fields $\text{GF}(q^m)$. This has significant impact on the packing properties of rank metric codes as explained below.

The sphere packing problem we consider is as follows: given a finite field $\text{GF}(q^m)$, length n , and radius r , what is the maximum number of non-intersecting balls with radius r that can be packed into $\text{GF}(q^m)^n$? The sphere packing problem is equivalent to finding the maximum cardinality $A(q^m, n, d)$ of a code over $\text{GF}(q^m)$ with length n and minimum distance $d \geq 2r + 1$: the spheres of radius r centered at the codewords of such a code do not intersect one another. Furthermore, when these non-intersecting spheres centered at all codewords cover the *whole* space, the code is called a perfect code.

For the Hamming metric, although nontrivial perfect codes do exist, the optimal solution to the sphere packing problem is not known for all the parameter sets [25]. In contrast, for rank metric codes, although nontrivial perfect rank metric codes do not exist [9], [10], MRD codes provide an optimal solution to the sphere packing problem for any set of parameters. For given n , m , and r , let us denote the maximum cardinality among rank metric codes over $\text{GF}(q^m)$ with length n and minimum distance $d_R = 2r + 1$ as $A_R(q^m, n, d_R)$. For $d_R > \min\{n, m\}$, $A_R(q^m, n, d_R) = 1$. For $d_R \leq \min\{n, m\}$, $A_R(q^m, n, d_R) = \min\{q^{m(n-d_R+1)}, q^{n(m-d_R+1)}\}$. Note that the maximal cardinality is achieved by MRD codes for all parameter sets. Hence, MRD codes admit the optimal solutions to the sphere packing problem for rank metric codes.

The performance of Hamming metric codes of large block length can be studied in terms of asymptotic bounds on the relative minimum distance in the limit of infinite block length. Next, we derive the asymptotic form of $A_R(q^m, n, d_R)$ when both block length and minimum rank distance go to infinity. However, this cannot be achieved for finite m since the minimum rank distance is no greater than m . Thus, we consider the case where $\lim_{n \rightarrow \infty} \frac{n}{m} = b$, where b is a constant.

Define $\delta \stackrel{\text{def}}{=} \lim_{n \rightarrow \infty} \frac{d_R}{n}$ and $a(\delta) \stackrel{\text{def}}{=} \lim_{n \rightarrow \infty} \sup \left[\frac{\log_{q^m} A_R(q^m, n, \lfloor \delta n \rfloor)}{n} \right]$, where $a(\delta)$ represents the maximum possible code rate of a code which has relative minimum distance δ as its length goes to infinity. We can thus determine the maximum possible code rate $a(\delta)$ of a code based on (9).

Proposition 5: For $0 \leq \delta \leq \min\{1, b^{-1}\}$, the existence of MRD codes for all parameter sets implies that

$$a(\delta) = \min\{1 - \delta, 1 - b\delta\}. \quad (10)$$

V. COVERING PROPERTIES OF RANK METRIC CODES

A. The sphere covering problem

In this section, we are interested in the sphere covering problem for the rank metric. This problem can be stated as follows: given an extension field $\text{GF}(q^m)$, length n , and radius ρ , we want to determine the minimum number of balls of rank radius ρ which cover $\text{GF}(q^m)^n$ entirely. The sphere covering problem is equivalent to finding the minimum cardinality $K_R(q^m, n, \rho)$ of a code over $\text{GF}(q^m)$ with length n and rank covering radius ρ .

We remark that if C is a code over $\text{GF}(q^m)$ with length n and covering radius ρ , then its transpose code C^T is a code over $\text{GF}(q^n)$ with length m and the same covering radius. Therefore, $K_R(q^m, n, \rho) = K_R(q^n, m, \rho)$, and without loss of generality we shall assume $n \leq m$ henceforth in this section. Also note that $K_R(q^m, n, 0) = q^{mn}$ and $K_R(q^m, n, n) = 1$ for all m and n . Hence we assume $0 < \rho < n$ throughout this section.

Two bounds on $K_R(q^m, n, \rho)$ can be easily derived.

Proposition 6: For a code over $\text{GF}(q^m)$ with length n and covering radius $0 < \rho < n$, we have

$$\left\lfloor \frac{q^{mn}}{V_\rho(q^m, n)} \right\rfloor + 1 \leq K_R(q^m, n, \rho) \leq q^{m(n-\rho)}. \quad (11)$$

Proof: The lower bound is a straightforward generalization of the bound given in [12]. Note that the only codes with cardinality $\frac{q^{mn}}{V_\rho(q^m, n)}$ are perfect codes. However, there are no nontrivial perfect codes for the rank metric [9]. Therefore, $K_R(q^m, n, \rho) > \frac{q^{mn}}{V_\rho(q^m, n)}$. The upper bound follows from $\rho \leq n - k$ for any (n, k) linear code [27], and hence any linear code with covering radius ρ has cardinality $\leq q^{m(n-\rho)}$. ■

We refer to the lower bound in (11) as the sphere covering bound.

For a code over $\text{GF}(q^m)$ with length n and covering radius $0 < \rho < n$, we have $K_R(q^m, n, \rho) \leq K_H(q^m, n, \rho)$, where $K_H(q^m, n, \rho)$ is the minimum cardinality of a (linear or nonlinear) code over $\text{GF}(q^m)$ with length n and Hamming covering radius ρ . This is because any code with Hamming covering radius

ρ has rank covering radius $\leq \rho$. Since $K_H(q^m, n, \rho) \leq q^{m(n-\rho)}$, this provides a tighter bound than the one given in Proposition 6.

Lemma 7: For all $m > 0$ and nonnegative n, n', ρ , and ρ' , we have

$$K_R(q^m, n + n', \rho + \rho') \leq K_R(q^m, n, \rho) K_R(q^m, n', \rho'). \quad (12)$$

In particular, we have

$$K_R(q^m, n + 1, \rho + 1) \leq K_R(q^m, n, \rho), \quad (13)$$

$$K_R(q^m, n + 1, \rho) \leq q^m K_R(q^m, n, \rho). \quad (14)$$

Proof: (12) follows directly from [12, Proposition 4]. In particular, when $(n', \rho') = (1, 1)$ and $(n', \rho') = (1, 0)$, we obtain (13) and (14) respectively. ■

B. Lower bounds for the sphere covering problem

We will derive two nontrivial lower bounds on $K_R(q^m, n, \rho)$. First, we adapt the bound given in [33, Theorem 1].

Proposition 7: For all q^m, n , and $0 < \rho < n$, we have

$$K_R(q^m, n, \rho) \geq \left\lceil \frac{q^{mn} - A_R(q^m, n, 2\rho + 1)q^{\rho^2 \left\lceil \frac{2\rho}{\rho} \right\rceil}}{V_\rho(q^m, n) - q^{\rho^2 \left\lceil \frac{2\rho}{\rho} \right\rceil}} \right\rceil, \quad (15)$$

provided that the denominator on the right hand side (RHS) is positive.

Proof: Suppose C is a code over $\text{GF}(q^m)$ with length n and rank covering radius ρ , and let C_0 be a maximal subcode of C with minimum rank distance $d' \geq 2\rho + 1$. If $d' > n$, we choose C_0 to be a single codeword. C_0 thus covers $|C_0|V_\rho(q^m, n)$ vectors. Define $C_1 = C \setminus C_0$, (C_1 is not empty, otherwise C would be a nontrivial perfect code) and for any $\mathbf{c}_1 \in C_1$, let $f(\mathbf{c}_1)$ denote the number of vectors covered by \mathbf{c}_1 which are not covered by C_0 . Since C_0 is maximal, there exists at least one codeword $\mathbf{c}_0 \in C_0$ such that $d_R(\mathbf{c}_0, \mathbf{c}_1) \leq 2\rho$. We have $f(\mathbf{c}_1) \leq V_\rho(q^m, n) - q^{\rho^2 \left\lceil \frac{2\rho}{\rho} \right\rceil}$, where the equality corresponds to when there is only one such \mathbf{c}_0 and $d_R(\mathbf{c}_0, \mathbf{c}_1) = 2\rho$ by Proposition 2. In that case, Proposition 4 implies that there are $q^{\rho^2 \left\lceil \frac{2\rho}{\rho} \right\rceil}$ vectors covered by both \mathbf{c}_0 and \mathbf{c}_1 . Thus, we have

$$\begin{aligned} q^{mn} &\leq |C_0|V_\rho(q^m, n) + \sum_{\mathbf{c}_1 \in C_1} f(\mathbf{c}_1) \\ &\leq |C_0|V_\rho(q^m, n) + (|C| - |C_0|) \left(V_\rho(q^m, n) - q^{\rho^2 \left\lceil \frac{2\rho}{\rho} \right\rceil} \right) \\ &= |C| \left(V_\rho(q^m, n) - q^{\rho^2 \left\lceil \frac{2\rho}{\rho} \right\rceil} \right) + |C_0|q^{\rho^2 \left\lceil \frac{2\rho}{\rho} \right\rceil}. \end{aligned}$$

We have $|C_0| \leq A_R(q^m, n, d') \leq A_R(q^m, n, 2\rho + 1)$, and the result follows. ■

We remark that $A_R(q^m, n, 2\rho + 1)$ is $q^{m(n-2\rho)}$ if $2\rho + 1 \leq n$, or 1 otherwise. Next, we obtain both sufficient and necessary conditions under which the bound is nontrivial, i.e., when the denominator on the RHS of (15) is positive.

Lemma 8: The denominator on the RHS of (15) is positive if $\rho(m + n - 3\rho) \geq \sigma(q)$. Also, the denominator in (15) is positive only if $m + n \geq 3\rho$.

Proof: We first prove the sufficient condition. We need to show $V_\rho(q^m, n) > q^{\rho^2} \binom{2\rho}{\rho}$. By Lemma 5, $V_\rho(q^m, n) \geq q^{\rho(m+n-\rho)}$. By [21, Lemma 1], we have $\binom{2\rho}{\rho} < q^{\rho^2+\sigma(q)}$. Therefore, the denominator in (15) is positive if $\rho(m + n - \rho) \geq 2\rho^2 + \sigma(q)$.

We now prove the necessary condition. Note that $\alpha(n, \rho) \leq q^{n\rho}$ and $\alpha(2\rho, \rho) \geq q^{2\rho^2-\tau(q)}$, where $\tau(q) = \log_q \left(\frac{q^2}{q^2-1} \right)$ [21, Lemma 2]. Now suppose $\rho(m + n - 3\rho) < -\tau(q)$, then $q^{\rho(m+n-3\rho)+\tau(q)} < 1$. This implies $\frac{\alpha(n, \rho)}{\alpha(2\rho, \rho)} q^{\rho(m-\rho)} < 1$, and hence $\binom{n}{\rho} q^{m\rho} < \binom{2\rho}{\rho} q^{\rho^2}$. By [21, Lemma 13], we obtain $V_\rho(q^m, n) \leq \binom{n}{\rho} q^{m\rho} < q^{\rho^2} \binom{2\rho}{\rho}$. Therefore, $V_\rho(q^m, n) - q^{\rho^2} \binom{2\rho}{\rho} > 0$ only if $\rho(m + n - 3\rho) \geq -\tau(q)$. Finally, $0 < \tau(q) < 1$ for $q \geq 2$ and hence $\rho(m + n - 3\rho) \geq 0$. ■

Before deriving the second nontrivial lower bound, we need the following adaptation of [30, Lemma 8]. Let C be a code with length n and rank covering radius ρ over $\text{GF}(q^m)$. We define $A \stackrel{\text{def}}{=} \{\mathbf{x} \in \text{GF}(q^m)^n | d_R(\mathbf{x}, C) = \rho\}$.

Lemma 9: For $\mathbf{x} \in A \setminus Z$ and $0 < \rho < n$, we have

$$E_C(B_1(\mathbf{x})) \geq \epsilon, \quad (16)$$

where

$$\epsilon \stackrel{\text{def}}{=} \left\lceil \frac{(q^m - q^\rho) \left(\binom{n}{1} - \binom{\rho}{1} \right)}{q^\rho \binom{\rho+1}{1}} \right\rceil q^\rho \binom{\rho+1}{1} + (q^m - q^\rho) \left(\binom{\rho}{1} - \binom{n}{1} \right).$$

Proof: Since $\mathbf{x} \notin Z$, there is a unique $\mathbf{c}_0 \in C$ such that $d_R(\mathbf{x}, \mathbf{c}_0) = \rho$. By Proposition 3 we have $|B_\rho(\mathbf{c}_0) \cap B_1(\mathbf{x})| = 1 + (q^m - q^\rho) \binom{\rho}{1} + (q^\rho - 1) \binom{n}{1}$. For any codeword $\mathbf{c}_1 \in C$ satisfying $d_R(\mathbf{x}, \mathbf{c}_1) = \rho + 1$, by Proposition 4 we have $|B_\rho(\mathbf{c}_1) \cap B_1(\mathbf{x})| = q^\rho \binom{\rho+1}{1}$. Finally, for all other codewords $\mathbf{c}_2 \in C$ at distance $> \rho + 1$ from \mathbf{x} , we have $|B_\rho(\mathbf{c}_2) \cap B_1(\mathbf{x})| = 0$. Denoting $N \stackrel{\text{def}}{=} |\{\mathbf{c}_1 \in C | d_R(\mathbf{x}, \mathbf{c}_1) = \rho + 1\}|$, we obtain

$$\begin{aligned} E_C(B_1(\mathbf{x})) &= \sum_{\mathbf{c} \in C} |B_\rho(\mathbf{c}) \cap B_1(\mathbf{x})| - |B_1(\mathbf{x})| \\ &= (q^m - q^\rho) \binom{\rho}{1} + N q^\rho \binom{\rho+1}{1} - \binom{n}{1} (q^m - q^\rho) \\ &\equiv (q^m - q^\rho) \left(\binom{\rho}{1} - \binom{n}{1} \right) \pmod{q^\rho \binom{\rho+1}{1}}. \end{aligned}$$

The proof is completed by realizing that $(q^m - q^\rho) \left(\binom{\rho}{1} - \binom{n}{1} \right) < 0$, while $E_C(B_1(\mathbf{x}))$ is a non-negative integer. ■

Proposition 8: If $\epsilon > 0$, then

$$K_R(q^m, n, \rho) \geq \left\lceil \frac{q^{mn}}{V_\rho(q^m, n) - \frac{\epsilon}{\delta} N_\rho(q^m, n)} \right\rceil, \quad (17)$$

where $\delta \stackrel{\text{def}}{=} V_1(q^m, n) - q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix} - 1 + 2\epsilon$.

The proof of Proposition 8, provided in Appendix A, uses the approach in the proof of [30, Theorem 6] and is based on the concept of excess reviewed in Section II-C. We remark that, unlike the bound given in Proposition 7, the bound in Proposition 8 is always applicable. The lower bounds in (15) and (17), when applicable, are at least as tight as the sphere covering bound given in (11).

C. Upper bounds for the sphere covering problem

From the perspective of covering, the following lemma gives a characterization of MRD codes in terms of ELS's.

Lemma 10: Let \mathcal{C} be an (n, k) linear code over $\text{GF}(q^m)$ ($n \leq m$). \mathcal{C} is an MRD code if and only if $\mathcal{C} \oplus \mathcal{V} = \text{GF}(q^m)^n$ for all $\mathcal{V} \in E_{n-k}(q^m, n)$.

Proof: Suppose \mathcal{C} is an $(n, k, n - k + 1)$ Class-I MRD code. It is clear that $\mathcal{C} \cap \mathcal{V} = \{\mathbf{0}\}$ and hence $\mathcal{C} \oplus \mathcal{V} = \text{GF}(q^m)^n$ for all $\mathcal{V} \in E_{n-k}(q^m, n)$. Conversely, suppose $\mathcal{C} \oplus \mathcal{V} = \text{GF}(q^m)^n$ for all $\mathcal{V} \in E_{n-k}(q^m, n)$. Then \mathcal{C} does not contain any nonzero codeword of weight $\leq n - k$, and hence its minimum distance is $n - k + 1$. ■

For $1 \leq u \leq \rho$, let $\alpha_0 = 1, \alpha_1, \dots, \alpha_{m+u-1} \in \text{GF}(q^{m+u})$ be a basis set of $\text{GF}(q^{m+u})$ over $\text{GF}(q)$, and let $\beta_0 = 1, \beta_1, \dots, \beta_{m-1}$ be a basis of $\text{GF}(q^m)$ over $\text{GF}(q)$. We define the *linear* mapping f between two vector spaces $\text{GF}(q^m)$ and $\mathfrak{S}_m \stackrel{\text{def}}{=} \mathfrak{S}(\alpha_0, \alpha_1, \dots, \alpha_{m-1})$ given by $f(\beta_i) = \alpha_i$ for $0 \leq i \leq m - 1$. This can be generalized to n -dimensional vectors, by applying f componentwise. We thus define $\bar{f} : \text{GF}(q^m)^n \rightarrow \text{GF}(q^{m+u})^n$ such that for any $\mathbf{v} = (v_0, \dots, v_{n-1})$, $\bar{f}(\mathbf{v}) = (f(v_0), \dots, f(v_{n-1}))$. Note that $\bar{f}(\cdot)$ depends on u , but we omit this dependence for simplicity of notation. This function \bar{f} is a linear bijection from $\text{GF}(q^m)^n$ to its image \mathfrak{S}_m^n , and \bar{f} preserves the rank. The rank-preserving property of \bar{f} can be shown as follows. Suppose $\mathbf{u} \in \text{GF}(q^m)^n$. Let us denote the matrix formed after extending the coordinates of \mathbf{u} with respect to the basis $\{\beta_i\}$ as \mathbf{U} . The extension of $\bar{f}(\mathbf{u})$ with respect to the basis $\{\alpha_i\}$ is given by $\bar{\mathbf{U}} = \begin{pmatrix} \mathbf{U} \\ \mathbf{0} \end{pmatrix}$. We thus have $\text{rk}(\bar{\mathbf{U}}) = \text{rk}(\mathbf{U})$, and $\text{rk}(\bar{f}(\mathbf{u})) = \text{rk}(\mathbf{u})$.

\bar{f} also introduces a connection between ELS's as shown below.

Lemma 11: For $1 \leq u \leq \rho$, $r \leq n$, and any $\mathcal{V} \in E_r(q^m, n)$, $\bar{f}(\mathcal{V}) \subset \mathcal{W}$, where $\mathcal{W} \in E_r(q^{m+u}, n)$. Furthermore, $\bar{f}(\cdot)$ induces a bijection between $E_r(q^m, n)$ and $E_r(q^{m+u}, n)$.

Proof: Let $B = \{\mathbf{b}_i\}$ be an elementary basis of $\mathcal{V} \in E_r(q^m, n)$. Then, $\mathbf{b}_i \in \text{GF}(q)^n$ and $\mathbf{b}_i = \bar{f}(\mathbf{b}_i)$. Thus, $\{\bar{f}(\mathbf{b}_i)\}$ form an elementary basis, and hence $\bar{f}(\mathcal{V}) \subset \mathcal{W}$, where $\mathcal{W} \in E_r(q^{m+u}, n)$ with $\{\bar{f}(\mathbf{b}_i)\}$ as a basis. It is easy to verify that $\bar{f}(\cdot)$ induces a bijection between $E_r(q^m, n)$ and $E_r(q^{m+u}, n)$. ■

Proposition 9: Let \mathcal{C} be an $(n, n - \rho, \rho + 1)$ MRD code over $\text{GF}(q^m)$ ($n \leq m$) with covering radius ρ . For $0 \leq u \leq \rho$, the code $\bar{f}(\mathcal{C})$, where \bar{f} is as defined above, is a code of length n over $\text{GF}(q^{m+u})$ with cardinality $q^{m(n-\rho)}$ and covering radius ρ .

Proof: The other parameters for the code are obvious, and it suffices to establish the covering radius. Let \mathfrak{T}_u be a subspace of $\text{GF}(q^{m+u})$ with dimension u such that $\mathfrak{S}_m \oplus \mathfrak{T}_u = \text{GF}(q^{m+u})$. Any $\mathbf{u} \in \text{GF}(q^{m+u})^n$ can be expressed as $\mathbf{u} = \mathbf{v} + \mathbf{w}$, where $\mathbf{v} \in \mathfrak{S}_m^n$ and $\mathbf{w} \in \mathfrak{T}_u^n$. Hence $\text{rk}(\mathbf{w}) \leq u$, and $\mathbf{w} \in \mathcal{W}$ for some $\mathcal{W} \in E_\rho(q^{m+u}, n)$ by Lemma 1. By Lemmas 10 and 11, we can express \mathbf{v} as $\mathbf{v} = \bar{f}(\mathbf{c} + \mathbf{e}) = \bar{f}(\mathbf{c}) + \bar{f}(\mathbf{e})$, where $\mathbf{c} \in \mathcal{C}$ and $\mathbf{e} \in \mathcal{V}$, such that $\bar{f}(\mathcal{V}) \subset \mathcal{W}$. Eventually, we have $\mathbf{u} = \bar{f}(\mathbf{c}) + \bar{f}(\mathbf{e}) + \mathbf{w}$, where $\bar{f}(\mathbf{e}) + \mathbf{w} \in \mathcal{W}$, and thus $d(\mathbf{u}, \bar{f}(\mathbf{c})) \leq \rho$. Thus $\bar{f}(\mathcal{C})$ has covering radius $\leq \rho$. Finally, it is easy to verify that the covering radius of $\bar{f}(\mathcal{C})$ is exactly ρ . ■

Corollary 2: We have

$$K_R(q^m, n, \rho) \leq q^{\max\{m-\rho, n\}(n-\rho)}. \quad (18)$$

Proof: We can construct an $(n, n - \rho)$ MRD code \mathcal{C} over $\text{GF}(q^\mu)$ with covering radius ρ , where $\mu = \max\{m - \rho, n\}$ and $m - \mu \leq \rho$. By Proposition 9, $\hat{f}(\mathcal{C}) \subset \text{GF}(q^m)^n$, where \hat{f} is a rank-preserving mapping from $\text{GF}(q^\mu)^n$ to a subset of $\text{GF}(q^m)^n$ similar to \bar{f} above, has covering radius $\leq \rho$. Thus, $K_R(q^m, n, \rho) \leq |\hat{f}(\mathcal{C})| = |\mathcal{C}| = q^{\mu(n-\rho)}$. ■

We can use the properties of $K_R(q^m, n, \rho)$ in Lemma 7 in order to obtain two tighter bounds when $\rho \geq m - n$.

Proposition 10: Given fixed m, n , and ρ , for any $n \geq l > 0$ and (n_i, ρ_i) for $0 \leq i \leq l - 1$ so that $0 < n_i \leq n$, $0 \leq \rho_i \leq n_i$, and $n_i + \rho_i \leq m$ for all i , and $\sum_{i=0}^{l-1} n_i = n$ and $\sum_{i=0}^{l-1} \rho_i = \rho$, we have

$$K_R(q^m, n, \rho) \leq \min_{\{(n_i, \rho_i): 0 \leq i \leq l-1\}} \left\{ q^{m(n-\rho) - \sum_i \rho_i (n_i - \rho_i)} \right\}. \quad (19)$$

Proof: By Lemma 7, we have $K_R(q^m, n, \rho) \leq \prod_i K_R(q^m, n_i, \rho_i)$ for all possible sequences $\{\rho_i\}$ and $\{n_i\}$. For all i , we have $K_R(q^m, n_i, \rho_i) \leq q^{(m-\rho_i)(n_i-\rho_i)}$ by Corollary 2, and hence $K_R(q^m, n, \rho) \leq q^{\sum_i (m-\rho_i)(n_i-\rho_i)} = q^{m(n-\rho) - \sum_i \rho_i (n_i - \rho_i)}$. ■

It is clear that the upper bound in (19) is tighter than the upper bound in (11). It can also be shown that it is tighter than the bound in (18).

The following upper bound is an adaptation of [27, Theorem 12.1.2].

Proposition 11: For any $m, n \leq m$, and $\rho < n$, there exists a code over $\text{GF}(q^m)$ of length n and

covering radius ρ with cardinality

$$K_R(q^m, n, \rho) \leq \left\lfloor \frac{1}{1 - \log_{q^{mn}}(q^{mn} - V_\rho(q^m, n))} \right\rfloor + 1. \quad (20)$$

Our proof, given in Appendix B, adopts the approach used to prove [27, Theorem 12.1.2].

Proposition 12: For all $m, n \leq m, \rho < n$, we have

$$K_R(q^m, n, \rho) \leq \frac{q^{mn}}{V_\rho(q^m, n)} [1 + \ln(V_\rho(q^m, n))]. \quad (21)$$

Proof: Consider the square 0-1 matrix \mathbf{A} of order q^{mn} , where each row (or column) corresponds to a different vector in $\text{GF}(q^m)^n$. Set $a_{i,j} = 1$ if and only if the sphere with rank radius ρ centered at vector i covers vector j . There are thus exactly $V_\rho(q^m, n)$ ones in each row and each column of \mathbf{A} . Note that any $q^{mn} \times K$ submatrix \mathbf{C} of \mathbf{A} with no all-zeros rows represents a code with cardinality K and covering radius ρ . Applying the Johnston-Stein-Lovász theorem [27, Theorem 12.2.1] to \mathbf{A} , we can find such a submatrix with $K \leq \frac{1}{V_\rho(q^m, n)} [q^{mn} + q^{mn} \ln(V_\rho(q^m, n))]$. ■

The tightest bounds on $K_R(q^m, n, \rho)$ known so far are given in Table I for $q = 2, 2 \leq m \leq 7, 2 \leq n \leq m$, and $1 \leq \rho \leq 6$.

D. Covering properties of linear rank metric codes

For a linear code with given covering radius, the sphere covering bound also implies a lower bound on its dimension.

Proposition 13: An (n, k) linear code over $\text{GF}(q^m)$ with rank covering radius ρ satisfies

$$\left\lfloor n - \rho - \frac{\rho(n - \rho) + \sigma(q)}{m} \right\rfloor + 1 \leq k \leq n - \rho. \quad (22)$$

Proof: The upper bound directly follows the upper bound in (11). We now prove the lower bound. By the sphere covering bound, we have $q^{mk} > \frac{q^{mn}}{V_\rho(q^m, n)}$. However, by Lemma 5 we have $V_\rho(q^m, n) < q^{\rho(m+n-\rho)+\sigma(q)}$ and hence $q^{mk} > q^{mn-\rho(m+n-\rho)-\sigma(q)}$. ■

We do not adapt the bounds in (15) and (17) as their advantage over the lower bound in (22) is not significant. Next, we show that the dimension of a linear code with given covering radius can be completely determined under some conditions.

Proposition 14: Let \mathcal{C} be an (n, k) linear code over $\text{GF}(q^m)$ ($n \leq m$) with rank covering radius ρ . Then $k = n - \rho$ if $\rho \in \{0, 1, n - 1, n\}$ or $\rho(n - \rho) \leq m - \sigma(q)$, or if \mathcal{C} is a generalized Gabidulin code or an ELS.

Proof: The cases $\rho \in \{0, n - 1, n\}$ are straightforward. In all other cases, since $k \leq n - \rho$ by Proposition 13, it suffices to prove that $k \geq n - \rho$. First, suppose $\rho = 1$, then k satisfies $q^{mk} > \frac{q^{mn}}{V_1(q^m, n)}$ by the sphere covering bound. However, $V_1(q^m, n) < q^{m+n} \leq q^{2m}$, and hence $k > n - 2$. Second, if

$\rho(n - \rho) \leq m - \sigma(q)$, then $0 < \frac{1}{m}(\rho(n - \rho) + \sigma(q)) \leq 1$ and $k \geq n - \rho$ by Proposition 13. Third, if \mathcal{C} is an $(n, k, n - k + 1)$ generalized Gabidulin code with $k < n$, then there exists an $(n, k + 1, n - k)$ generalized Gabidulin code \mathcal{C}' such that $\mathcal{C} \subset \mathcal{C}'$. We have $\rho \geq d_R(\mathcal{C}') = n - k$, as noted in Section II-C, and hence $k \geq n - \rho$. The case $k = n$ is straightforward. Finally, if \mathcal{C} is an ELS of dimension k , then for all \mathbf{x} with rank n and for any $\mathbf{c} \in \mathcal{C}$, $d_R(\mathbf{x}, \mathbf{c}) \geq \text{rk}(\mathbf{x}) - \text{rk}(\mathbf{c}) \geq n - k$. ■

A similar argument can be used to bound the covering radius of the cartesian products of generalized Gabidulin codes.

Corollary 3: Let \mathcal{G} be an (n, k, d_R) generalized Gabidulin code ($n \leq m$), and let \mathcal{G}^l be the code obtained by l cartesian products of \mathcal{G} for $l \geq 1$. Then the rank covering radius of \mathcal{G}^l satisfies $\rho(\mathcal{G}^l) \geq d_R - 1$.

Note that when $n = m$, \mathcal{G}^l is a maximal code, and hence Corollary 3 can be further strengthened.

Corollary 4: Let \mathcal{G} be an (m, k, d_R) generalized Gabidulin code over $\text{GF}(q^m)$, and let \mathcal{G}^l be the code obtained by l cartesian products of \mathcal{G} . Then $\rho(\mathcal{G}^l) = d_R - 1$.

The tightest bounds known so far for the dimension of a linear code with given covering radius are given in Table II for $q = 2$, $4 \leq m \leq 8$, $4 \leq n \leq m$, and $2 \leq \rho \leq 6$.

E. Asymptotic covering properties

Table I provides solutions to the sphere covering problem for only small values of m , n , and ρ . Next, we study the asymptotic covering properties when both block length and minimum rank distance go to infinity. As in Section IV, we consider the case where $\lim_{n \rightarrow \infty} \frac{n}{m} = b$, where b is a constant. In other words, these asymptotic covering properties provide insights on the covering properties of long rank metric codes over large fields.

The asymptotic form of the bounds in (6) are given in the lemma below.

Lemma 12: For $0 \leq \delta \leq \min\{1, b^{-1}\}$, $v(\delta) \stackrel{\text{def}}{=} \lim_{n \rightarrow \infty} \left\lfloor \frac{\log_{q^m} V_{\lfloor \delta n \rfloor}(q^m, n)}{n} \right\rfloor = \delta(1 + b - b\delta)$.

Proof: By Lemma 5, we have $q^{d_R(m+n-d_R)} \leq V_{d_R}(q^m, n) < q^{d_R(m+n-d_R)+\sigma(q)}$. Taking the logarithm and dividing by n , this becomes $\delta(1 + b - b\delta) \leq \log_{q^m}(V_{\lfloor \delta n \rfloor}(q^m, n))/n < \delta(1 + b - b\delta) + \frac{\sigma(q)}{mn}$. The proof is concluded by taking the limit when n tends to infinity. ■

Define $r \stackrel{\text{def}}{=} \frac{\rho}{n}$ and $k(r) = \lim_{n \rightarrow \infty} \inf \left\lfloor \frac{\log_{q^m} K_R(q^m, n, \rho)}{n} \right\rfloor$. The bounds in (11) and (21) together solve the asymptotic sphere covering problem.

Theorem 1: For all b and r , we have

$$k(r) = (1 - r)(1 - br). \quad (23)$$

Proof: By Lemma 12 the sphere covering bound in (11) asymptotically becomes $k(r) \geq (1-r)(1-br)$. Also, from the bound in (21), we have

$$\begin{aligned} K_R(q^m, n, \rho) &\leq \frac{q^{mn}}{V_\rho(q^m, n)} [1 + \ln(V_n(q^m, n))] \\ &\leq \frac{q^{mn}}{V_\rho(q^m, n)} [1 + mn \ln(q)] \\ \log_{q^{mn}} K_R(q^m, n, \rho) &\leq \log_{q^{mn}} \frac{q^{mn}}{V_\rho(q^m, n)} + O((mn)^{-1} \ln(mn)). \end{aligned}$$

By Lemma 12, this asymptotically becomes $k(r) \leq (1-r)(1-br)$. Note that although we assume $n \leq m$ above for convenience, both bounds in (11) and (21) hold for any values of m and n . ■

VI. CONCLUSIONS

In this paper, we investigate the packing and covering properties of rank metric codes. We show that MRD codes not only are optimal in the sense of the Singleton bound, but also provide the optimal solution to the sphere packing problem. We also derive bounds for the sphere covering problem and establish the asymptotic minimum code rate for a code with given relative covering radius.

APPENDIX

The proofs in this section use some well-known properties of Gaussian polynomials [31]:

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix} \quad (24)$$

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k \end{bmatrix} + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} \quad (25)$$

$$= q^k \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} \quad (26)$$

$$= \frac{q^n - 1}{q^{n-k} - 1} \begin{bmatrix} n-1 \\ k \end{bmatrix} \quad (27)$$

$$= \frac{q^{n-k+1} - 1}{q^k - 1} \begin{bmatrix} n \\ k-1 \end{bmatrix} \quad (28)$$

$$\begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} k \\ l \end{bmatrix} = \begin{bmatrix} n \\ l \end{bmatrix} \begin{bmatrix} n-l \\ n-k \end{bmatrix}. \quad (29)$$

A. Proof of Proposition 8

We first establish a key lemma.

Lemma 13: If $\mathbf{z} \in Z$ and $0 < \rho < n$, then

$$|A \cap B_1(\mathbf{z})| \leq V_1(q^m, n) - q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix}. \quad (30)$$

Proof: By definition of ρ , there exists $\mathbf{c} \in C$ such that $d_R(\mathbf{z}, \mathbf{c}) \leq \rho$. By Proposition 2, $|B_1(\mathbf{z}) \cap B_{\rho-1}(\mathbf{c})|$ gets its minimal value for $d_R(\mathbf{z}, \mathbf{c}) = \rho$, which is $q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix}$ by Proposition 4. A vector at distance $\leq \rho - 1$ from any codeword does not belong to A . Therefore, $B_1(\mathbf{z}) \cap B_{\rho-1}(\mathbf{c}) \subseteq B_1(\mathbf{z}) \setminus A$, and hence $|A \cap B_1(\mathbf{z})| = |B_1(\mathbf{z})| - |B_1(\mathbf{z}) \setminus A| \leq V_1(q^m, n) - |B_1(\mathbf{z}) \cap B_{\rho-1}(\mathbf{c})|$. ■

We now give a proof of Proposition 8.

Proof: For a code C with covering radius ρ and $\epsilon \geq 1$,

$$\gamma \stackrel{\text{def}}{=} \epsilon [q^{mn} - |C|V_{\rho-1}(q^m, n)] - (\epsilon - 1) [|C|V_{\rho}(q^m, n) - q^{mn}] \quad (31)$$

$$\leq \epsilon |A| - (\epsilon - 1) |Z| \quad (32)$$

$$\leq \epsilon |A| - (\epsilon - 1) |A \cap Z|$$

$$= \epsilon |A \setminus Z| + |A \cap Z|,$$

where (32) follows from $|Z| \leq |C|V_{\rho}(q^m, n) - q^{mn}$, given in Section II-C.

$$\begin{aligned} \gamma &\leq \sum_{\mathbf{a} \in A \setminus Z} E_C(B_1(\mathbf{a})) + \sum_{\mathbf{a} \in A \cap Z} E_C(B_1(\mathbf{a})) \\ &= \sum_{\mathbf{a} \in A} E_C(B_1(\mathbf{a})), \end{aligned} \quad (33)$$

where (33) follows from Lemma 9 and $|A \cap Z| \leq E_C(A \cap Z)$.

$$\begin{aligned} \gamma &\leq \sum_{\mathbf{a} \in A} \sum_{\mathbf{x} \in B_1(\mathbf{a}) \cap Z} E_C(\{\mathbf{x}\}) \\ &= \sum_{\mathbf{x} \in Z} \sum_{\mathbf{a} \in B_1(\mathbf{x}) \cap A} E_C(\{\mathbf{x}\}) \\ &= \sum_{\mathbf{x} \in Z} |A \cap B_1(\mathbf{x})| E_C(\{\mathbf{x}\}), \end{aligned} \quad (34)$$

where (34) follows from the fact the second summation is over disjoint sets $\{\mathbf{x}\}$. Using Lemma 13, we obtain

$$\begin{aligned} \gamma &\leq \sum_{\mathbf{x} \in Z} \left(V_1(q^m, n) - q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix} \right) E_C(\{\mathbf{x}\}) \\ &= \left(V_1(q^m, n) - q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix} \right) E_C(Z) \\ &= \left(V_1(q^m, n) - q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix} \right) (|C|V_{\rho}(q^m, n) - q^{mn}). \end{aligned} \quad (35)$$

Combining (35) and (31), we obtain (17). ■

B. Proof of Proposition 11

Given a radius ρ and a code C , denote by $P_\rho(C)$ the set of vectors in $\text{GF}(q^m)^n$ that are at distance $> \rho$ from C . To simplify notations, $Q \stackrel{\text{def}}{=} q^{mn}$ and $p_\rho(C) \stackrel{\text{def}}{=} Q^{-1}|P_\rho(C)|$. Let us denote the set of all codes over $\text{GF}(q^m)$ of length n and cardinality K as S_K . Clearly $|S_K| = \binom{Q}{K}$. Let us calculate the average value of $p_\rho(C)$ for all codes $C \in S_K$:

$$\begin{aligned} \frac{1}{|S_K|} \sum_{C \in S_K} p_\rho(C) &= \frac{1}{|S_K|} Q^{-1} \sum_{C \in S_K} |P_\rho(C)| = \frac{1}{|S_K|} Q^{-1} \sum_{C \in S_K} \sum_{\mathbf{x} \in F | d_R(\mathbf{x}, C) > \rho} 1 \\ &= \frac{1}{|S_K|} Q^{-1} \sum_{\mathbf{x} \in F} \sum_{C \in S_K | d_R(\mathbf{x}, C) > \rho} 1 \\ &= \frac{1}{|S_K|} Q^{-1} \sum_{\mathbf{x} \in F} \binom{Q - V_\rho(q^m, n)}{K} \end{aligned} \quad (36)$$

$$= \binom{Q - V_\rho(q^m, n)}{K} / \binom{Q}{K}. \quad (37)$$

Eq. (36) comes from the fact that there are $\binom{Q - V_\rho(q^m, n)}{K}$ codes with cardinality K that do not cover \mathbf{x} .

For all K , there exists a code $C' \in S_K$ for which $p_\rho(C')$ is no more than the average, that is:

$$\begin{aligned} p_\rho(C') &\leq \binom{Q}{K}^{-1} \binom{Q - V_\rho(q^m, n)}{K} \\ &\leq (1 - Q^{-1} V_\rho(q^m, n))^K. \end{aligned}$$

Let us choose $K = \left\lfloor -\frac{1}{\log_Q(1 - Q^{-1} V_\rho(q^m, n))} \right\rfloor + 1$ so that $K \log_Q(1 - Q^{-1} V_\rho(q^m, n)) < -1$ and hence $p_\rho(C') = (1 - Q^{-1} V_\rho(q^m, n))^K < Q^{-1}$. It follows that $|P_\rho(C')| < 1$, and C' has covering radius at most ρ .

REFERENCES

- [1] L. Hua, "A theorem on matrices over a field and its applications," *Chinese Mathematical Society*, vol. 1, no. 2, pp. 109–163, 1951.
- [2] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory A*, vol. 25, pp. 226–241, 1978.
- [3] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Info. Theory*, vol. 44, pp. 774–765, March 1998.
- [4] P. Lusina, E. M. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Trans. Info. Theory*, vol. 49, pp. 2757–2760, Oct. 2003.
- [5] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a non-commutative ring and their application in cryptology," *LNCS*, vol. 573, pp. 482–489, 1991.

- [6] E. M. Gabidulin, "Optimal codes correcting lattice-pattern errors," *Problems on Information Transmission*, vol. 21, no. 2, pp. 3–11, 1985.
- [7] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Trans. Info. Theory*, vol. 37, no. 2, pp. 328–336, March 1991.
- [8] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems on Information Transmission*, vol. 21, no. 1, pp. 1–12, Jan. 1985.
- [9] N. Suresh Babu, "Studies on rank distance codes," Ph.D Dissertation, IIT Madras, Feb. 1995.
- [10] K. Chen, "On the non-existence of perfect codes with rank distance," *Mathematische Nachrichten*, vol. 182, pp. 89–98, 1996.
- [11] R. M. Roth, "Probabilistic crisscross error correction," *IEEE Trans. Info. Theory*, vol. 43, no. 5, pp. 1425–1438, Sept. 1997.
- [12] W. B. Vasantha and N. Suresh Babu, "On the covering radius of rank-distance codes," *Ganita Sandesh*, vol. 13, pp. 43–48, 1999.
- [13] W. B. Vasantha and R. J. Selvaraj, "Multi-covering radii of codes with rank metric," *Proc. Information Theory Workshop*, p. 215, Oct. 2002.
- [14] G. Richter and S. Plass, "Fast decoding of rank-codes with rank errors and column erasures," *Proceedings of IEEE ISIT 2004*, p. 398, June 2004.
- [15] M. Schwartz and T. Etzion, "Two-dimensional cluster-correcting codes," *IEEE Trans. Info. Theory*, vol. 51, no. 6, pp. 2121–2132, June 2005.
- [16] A. Kshevetskiy and E. M. Gabidulin, "The new construction of rank codes," *Proc. IEEE Int. Symp. on Information Theory*, pp. 2105–2108, Sept. 2005.
- [17] E. M. Gabidulin and P. Loidreau, "On subcodes of codes in the rank metric," *Proc. IEEE Int. Symp. on Information Theory*, pp. 121–123, Sept. 2005.
- [18] P. Loidreau, "A Welch-Berlekamp like algorithm for decoding Gabidulin codes," *Proceedings of the 4th International Workshop on Coding and Cryptography*, 2005.
- [19] M. Gadouleau and Z. Yan, "Properties of codes with the rank metric," *Proceedings of 2006 IEEE Globecom*, pp. 1–5, November 2006.
- [20] —, "Decoder error probability of MRD codes," *Proceedings of IEEE International Theory Workshop*, pp. 264–268, October 2006.
- [21] —, "Error performance analysis of maximum rank distance codes," *Submitted to IEEE Transactions on Information Theory*, available at <http://arxiv.org/pdf/cs.IT/0612051>.
- [22] P. Loidreau, "Properties of codes in rank metric," available at <http://arxiv.org/pdf/cs.DM/0610057>.
- [23] P. Delsarte, "Four fundamental parameters of a code and their combinatorial significance," *Information and Control*, vol. 23, pp. 407–438, 1973.
- [24] T. Berger, *Rate Distortion Theory: A Mathematical Basis for Data Compression*, ser. Information and System Sciences Series, T. Kailath, Ed. Englewood Cliffs, N.J.: Prentice-Hall, 1971.
- [25] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.
- [26] R. Blahut, *Theory and Practice of Error Control Codes*. Addison-Wesley, 1983.
- [27] G. D. Cohen, I. Honkala, S. Litsyn, and A. C. Lobstein, *Covering Codes*. Elsevier, 1997.

- [28] P. Loidreau, “Étude et optimisation de cryptosystèmes à clé publique fondés sur la théorie des codes correcteurs,” Ph.D. Dissertation, École Polytechnique, Paris, France, May 2001.
- [29] G. van Wee, “Improved sphere bounds on the covering radius of codes,” *IEEE Trans. Info. Theory*, vol. 34, pp. 237–245, 1988.
- [30] —, “Bounds on packings and coverings by spheres in q -ary and mixed Hamming spaces,” *Journal of Combinatorial Theory, Series A*, vol. 57, pp. 116–129, 1991.
- [31] G. E. Andrews, *The Theory of Partitions*, ser. Encyclopedia of Mathematics and its Applications, G.-C. Rota, Ed. Reading, MA: Addison-Wesley, 1976, vol. 2.
- [32] D. J. Kleitman, “On a combinatorial conjecture of Erdős,” *Journal of Combinatorial Theory*, vol. 1, pp. 209–214, 1966.
- [33] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, “Further results on the covering radius of codes,” *IEEE Trans. Info. Theory*, vol. 32, pp. 680–694, 1986.

m	n	$\rho = 1$	$\rho = 2$	$\rho = 3$	$\rho = 4$	$\rho = 5$	$\rho = 6$
2	2	b 3-4 A	1				
3	2	b 4 B	1				
	3	b 11-32 C	a 2-4 C	1			
4	2	b 7-8 B	1				
	3	b 40-64 B	b 4-8 C	1			
	4	c 293-1024 C	b 10-64 C	a 2-8 C	1		
5	2	b 12-16 B	1				
	3	b 154-256 B	b 6-8 B	1			
	4	b 2267-4096 B	b 33-256 C	a 3-8 C	1		
	5	b 34894-2 ¹⁷ C	b 233-2979 E	b 10-128 C	a 2-8 C	1	
6	2	b 23-32 B	1				
	3	b 601-1024 B	a 10-16 B	1			
	4	b 17822-2 ¹⁵ B	b 123-256 B	b 6-16 C	1		
	5	b 550395-2 ²⁰ B	b 1770-2 ¹⁴ C	c 31-256 C	a 3-16 C	1	
	6	c 17318410-2 ²⁶ C	c 27065-424990 E	c 214-4299 E	c 9-181 D	a 2-16 C	1
7	2	b 44-64 B	1				
	3	b 2372-4096 B	a 19-32 B	1			
	4	b 141231-2 ¹⁸ B	c 484-1024 B	b 10-16 B	1		
	5	b 8735289-2 ²⁴ B	b 13835-2 ¹⁵ B	b 112-1024 C	a 5-16 C	1	
	6	b 549829402-2 ³⁰ B	c 42229-2 ²² C	b 1584-2 ¹⁵ C	b 31-746 E	a 3-16 C	1
	7	b 34901004402-2 ³⁷ C	c 13205450-244855533 E	b 23978-596534 E	c 203-5890 E	a 8-242 D	a 2-16 C

TABLE I

BOUNDS ON $K_R(q^m, n, \rho)$, FOR $2 \leq m \leq 7$, $2 \leq n \leq m$, AND $1 \leq \rho \leq 6$. FOR EACH SET OF PARAMETERS, THE TIGHTEST LOWER AND UPPER BOUNDS ON $K_R(q^m, n, \rho)$ ARE GIVEN, AND LETTERS ASSOCIATED WITH THE NUMBERS ARE USED TO INDICATE THE TIGHTEST BOUND. THE LOWER CASE LETTERS a–c CORRESPOND TO THE LOWER BOUNDS IN (11), (15), AND (17) RESPECTIVELY. THE UPPER CASE LETTERS A–E DENOTE THE UPPER BOUNDS IN (11), (18), (19), (20), AND (21) RESPECTIVELY.

m	n	$\rho = 2$	$\rho = 3$	$\rho = 4$	$\rho = 5$	$\rho = 6$
4	4	1-2	1	0		
5	4	1-2	1	0		
	5	2-3	1-2	1	0	
6	4	2	1	0		
	5	2-3	1-2	1	0	
	6	3-4	2-3	1-2	1	0
7	4	2	1	0		
	5	2-3	1-2	1	0	
	6	3-4	2-3	1-2	1	0
	7	4-5	3-4	2-3	1-2	1
8	4	2	1	0		
	5	3	2	1	0	
	6	3-4	2-3	1-2	1	0
	7	4-5	3-4	2-3	1-2	1
	8	5-6	3-5	2-4	1-3	1-2

TABLE II

BOUNDS ON k FOR $q = 2$, $4 \leq m \leq 8$, $4 \leq n \leq m$, AND $2 \leq \rho \leq 6$.