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*— In this paper, we investigate the packing and the covering properties of rank metric codes. We first study the sphere packing problem for rank metric codes, and show that an optimal solution in the sense of Singleton bound can be constructed for any set of parameters. We then investigate the properties of balls with rank radii, and derive several useful results. Using these results, we investigate sphere covering properties for rank metric codes and derive both upper and lower bounds on the minimal cardinality of a code with given length and rank covering radius.**

I. Introduction

Error correction codes (ECCs) with the rank metric [1]–[4] have been receiving steady attention in the literature due to their applications in storage systems [2], public-key cryptosystems [3], and space-time coding [4]. The pioneering works in [1] and [2] have established many important properties of codes with the rank metric. In [1], a Singleton bound on the minimum rank distance of codes was established, and codes that attain this bound were called maximum rank distance (MRD) codes. An explicit construction for a subclass of MRD codes was also proposed in [1], and this construction was extended in [5]. In [2], an equivalent bound and an equivalent construction were proposed, and it was shown that MRD codes are also optimal in the sense of Singleton bound in crisscross weight, a metric considered in [2] for crisscross errors. General properties of rank metric codes are also explored in [6]–[9].

Both packing and covering properties are significant for ECCs, and both packing radius and covering radius are basic geometric parameters of a code, important in several respects. 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; If the code is used for data compression, then the covering radius is a measure of the maximum distortion [10]. The Hamming packing and covering radii of ECCs have been extensively studied (see, for example, [11]–[13]), whereas the rank packing and covering radii have received relatively little attention. It is shown that nontrivial perfect rank metric codes do not exist in [14], [15]. In [6], a sphere-covering bound for rank metric codes is introduced. The concept of rank covering radius is generalized in [7], where the multi-covering radii of codes with the rank metric are defined. In [15], maximal codes for the rank metric are defined and the covering radii of subclasses of MRD codes are determined.

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

- We first study the sphere packing problem for rank metric codes. We show that for all the parameter sets, the optimal solution in the sense of Singleton bound to the sphere packing problem can be constructed.
- We establish further properties of elementary linear subspaces, and these properties parallel those of subsets of coordinates.
- Properties of balls with rank radii are also studied. We first derive an upper bound on the volume of a ball with a rank radius. We then prove some fundamental properties of the intersections of two balls with rank radii, and study some special cases. We finally show that the problem of the intersection of three balls with rank radii is similar to the same problem for the Hamming metric.
- We derive both upper and lower bounds on the minimal cardinality of a code with given length and rank covering radius. Our two lower bounds are tighter than the sphere-covering bound in [6]. Using the sphere-covering bound, we also establish additional sphere covering properties for linear rank metric codes.

The rest of the paper is organized as follows. Section II briefly reviews some backgrounds necessary to make this paper self-contained. We investigate the packing properties of rank metric codes in Section III. Section IV studies the covering properties of rank metric codes. Section IV-A derives some properties of elementary linear subspaces, and Section IV-B investigates the properties of balls with rank radii. Using the results in Sections IV-A and IV-B, we derive both upper and lower bounds on the minimum cardinality of a code with given length and rank covering radius in Section IV-C. Based on these bounds, further covering properties for linear rank metric codes are established in Section IV-D. Some proofs have been omitted due to limited space, and they will be presented at the conference.

II. Preliminaries

A. Rank metric

Consider an n-dimensional vector $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in \mathrm{GF}(q^m)^n$. Assume $\{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$ is a basis set of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$, then for

$j = 0, 1, \ldots, n-1$, x_j can be written as $x_j = \sum_{i=0}^{m-1} x_{i,j}\alpha_i$, where $x_{i,j} \in \mathrm{GF}(q)$ for $i = 0, 1, \ldots, m-1$. Hence, x_j can be expanded to an m-dimensional column vector $(x_{0,j}, x_{1,j}, \ldots, x_{m-1,j})^T$ with respect to the basis set $\{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$. Let $\mathbf{X}$ be the $m \times n$ matrix obtained by expanding all the coordinates of $\mathbf{x}$. That is,

$$\mathbf{X} = \begin{pmatrix} x_{0,0} & x_{0,1} & \ldots & x_{0,n-1} \\ x_{1,0} & x_{1,1} & \ldots & x_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m-1,0} & x_{m-1,1} & \ldots & x_{m-1,n-1} \end{pmatrix},$$

where $x_j = \sum_{i=0}^{m-1} x_{i,j}\alpha_i$. The *rank norm* of the vector $\mathbf{x}$ (over GF(q)), denoted as $\mathrm{rk}(\mathbf{x}|\mathrm{GF}(q))$, is defined to be the rank of the matrix $\mathbf{X}$ over GF(q), i.e., $\mathrm{rk}(\mathbf{x}|\mathrm{GF}(q)) \stackrel{\text{def}}{=} \mathrm{rank}(\mathbf{X})$ [1]. In this paper, all the ranks are over the base field GF(q) unless otherwise specified. To simplify notations, we denote the rank norm of $\mathbf{x}$ as $\mathrm{rk}(\mathbf{x})$ henceforth.

The rank norm of $\mathbf{x}$ is also the number of coordinates in $\mathbf{x}$ that are linearly independent over GF(q) [1]. The field GF(q^m) may be viewed as an m-dimensional vector space over GF(q). The coordinates of $\mathbf{x}$ thus span a linear subspace of GF(q^m), denoted as $\mathfrak{S}(\mathbf{x})$, and the rank of $\mathbf{x}$ is the dimension of $\mathfrak{S}(\mathbf{x})$.

For all $\mathbf{x}, \mathbf{y} \in \mathrm{GF}(q^m)^n$, it is easily verified that $d_{\mathrm{R}}(\mathbf{x}, \mathbf{y}) \stackrel{\text{def}}{=} \mathrm{rk}(\mathbf{x} - \mathbf{y})$ is a metric over GF$(q^m)^n$, referred to as the *rank metric* henceforth [1]. The *minimum rank distance* of a code, denoted as d_{R}, is simply the minimum rank distance over all possible pairs of distinct codewords.

B. Notations

In order to simplify notations, we shall occasionally denote the vector space GF$(q^m)^n$ as F. We denote the number of vectors of rank u ($0 \leq u \leq \min\{m, n\}$) in GF$(q^m)^n$ as $N_u(q^m, n)$. It can be shown that $N_u(q^m, n) = \begin{bmatrix} n \\ u \end{bmatrix} \alpha(m, u)$, where $\alpha(m, u)$ is defined as follows: $\alpha(m, 0) = 1$ and $\alpha(m, u) = \prod_{i=0}^{u-1}(q^m - q^i)$ for $u \geq 1$. The $\begin{bmatrix} n \\ u \end{bmatrix}$ term is the Gaussian binomial [16], defined as $\begin{bmatrix} n \\ u \end{bmatrix} = \alpha(n, u)/\alpha(u, u)$. Note that $\begin{bmatrix} n \\ u \end{bmatrix}$ is the number of u-dimensional linear subspaces of GF$(q)^n$. We refer to the set of vectors in GF$(q^m)^n$ within rank distance t of $\mathbf{x} \in \mathrm{GF}(q^m)^n$ as the ball of rank radius t centered at $\mathbf{x}$, and denote it as $B_t(\mathbf{x})$. It is easy to verify that its volume does not depend on $\mathbf{x}$. Hence we denote the volume of a ball of rank radius t as $V_t(q^m, n) = \sum_{u=0}^{t} N_u(q^m, n)$.

C. Elementary linear subspaces [17]

If there exists a basis set B of vectors in GF$(q)^n$ for a linear subspace $\mathcal{V} \subseteq \mathrm{GF}(q^m)^n$, we say $\mathcal{V}$ is elementary and B is an elementary basis of $\mathcal{V}$. We denote the set of elementary linear subspaces (ELS) of GF$(q^m)^n$ with dimension v as $E_v(q^m, n)$. Any vector $\mathbf{x} \in \mathrm{GF}(q^m)^n$ with rank r belongs to an ELS in $E_r(q^m, n)$. Also, any vector in an ELS with dimension r has rank no more than 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 $\mathcal{V} \oplus \bar{\mathcal{V}} = \mathrm{GF}(q^m)^n$, where $\oplus$ denotes the direct sum of two subspaces. For any vector $\mathbf{x} \in \mathrm{GF}(q^m)^n$, we denote the projection of $\mathbf{x}$ on $\mathcal{V}$ along $\bar{\mathcal{V}}$ as $\mathbf{x}_{\mathcal{V}}$, and we remark that $\mathbf{x} = \mathbf{x}_{\mathcal{V}} + \mathbf{x}_{\bar{\mathcal{V}}}$.

D. Covering radius and excess

The covering radius ρ of a code C with length n over GF(q^m) is defined to be the smallest integer ρ such that all vectors in the space GF$(q^m)^n$ are within distance ρ of some codeword of C [13]. It is the maximal distance from any vector in GF$(q^m)^n$ to the code C. That is,

$$\rho = \max_{\mathbf{x} \in F}\{d_{\mathrm{R}}(\mathbf{x}, C)\}. \tag{1}$$

The covering radius of an (n, k) linear code is no more than $n - k$ [13].

Van Wee [18], [19] gave several bounds on codes with Hamming covering radii. The approach is 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 [18], [19]. For all $V \subseteq F$, we define the excess on V by C to be

$$E_C(V) \stackrel{\text{def}}{=} \sum_{\mathbf{c} \in C} |B_\rho(\mathbf{c}) \cap V| - |V|. \tag{2}$$

The excess on F by C is given by $E_C(F) = |C| \cdot V_\rho(q^m, n) - q^{mn}$. Also, if $\{W_i\}$ is a family of disjoint subsets of F, then $E_C\left(\bigcup_i W_i\right) = \sum_i E_C(W_i)$. We also define $Z \stackrel{\text{def}}{=} \{\mathbf{z} \in F | E_C(\{\mathbf{z}\}) > 0\}$ [18]. In a nutshell, Z is the set of vectors covered by at least two codewords in C. That is, $\mathbf{z} \in Z$ if and only if $|B_\rho(\mathbf{z}) \cap C| \geq 2$. Finally, we have $|Z| \leq E_C(Z) = E_C(F) = |C| \cdot V_\rho(q^m, n) - q^{mn}$.

We remark that the above definitions and properties are all independent of the underlying metric, and thus are applicable to the rank metric as well.

III. Packing properties of rank metric codes

The most important question about packing properties of rank metric codes is the existence of perfect codes, for which there are balls of equal rank radius centered at the codewords that are disjoint and that completely fill the space. It has been shown that nontrivial perfect rank metric codes do not exist in [14], and the same conclusion was reached from an asymptotic perspective in [15].

Another important question is related to the sphere packing problem: given a finite field 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 GF$(q^m)^n$? The sphere packing problem is equivalent to finding the maximum cardinality $A(q^m, n, d)$ of a code over GF(q^m) with length n and minimum distance $d \geq 2r + 1$. Indeed, the balls of rank radius r centered at the codewords of such a code do not intersect one another. Therefore, the sphere packing problem can be solved by finding a family of optimal codes. For the Hamming metric, an optimal solution to the sphere packing problem is not known for all the parameter sets [11]. In contrast, for rank metric codes we show that an optimal solution in the sense of Singleton bound to the sphere packing problem can be constructed for any set of parameters. First, remark that $A_{\mathrm{R}}(q^m, n, d_{\mathrm{R}}) = 1$ for $d_{\mathrm{R}} > \min\{n, m\}$. Let C be a code over GF(q^m) with length n, cardinality K, and minimum rank distance d_{R}. If $n \leq m$, then the Singleton bound in [1] implies that $K \leq q^{m \cdot (n-d_{\mathrm{R}}+1)}$. For $n \leq m$ and for any $1 \leq d_{\mathrm{R}} \leq n$, MRD codes proposed in [1] satisfy this bound with equality [1], and hence $A_{\mathrm{R}}(q^m, n, d_{\mathrm{R}}) = q^{m \cdot (n-d_{\mathrm{R}}+1)}$. If $n > m$, since the transpose of an MRD code over $\mathrm{GF}(q^n)$ with length m, cardinality K, and minimum rank distance d_{R} is a code[1] over $\mathrm{GF}(q^m)$ with length n, cardinality K, and minimum rank distance d_{R}, $A_{\mathrm{R}}(q^m, n, d_{\mathrm{R}}) = q^{n \cdot (m-d_{\mathrm{R}}+1)}$.

IV. Covering properties of rank metric codes

A. Further properties of ELS's

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

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 [17], 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, there are $q^{a(v-a)}$ ELS's $\mathcal{B}$ such that $\mathcal{A} \oplus \mathcal{B} = \mathcal{V}$.

Corollary 1: There are $q^{a(v-a)} \begin{bmatrix} v \\ a \end{bmatrix}$ such ordered pairs $(\mathcal{A}, \mathcal{B})$.

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

It was shown 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 $\mathcal{B}$ in [17]. 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 $\mathbf{u}$, $\mathcal{V}$, $\mathcal{A}$ and $\mathcal{B}$ are defined as above. For any ordered pair of complementary ELS's $(\mathcal{A}, \mathcal{B})$, 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.

B. Properties of balls with rank radii

An upper bound on the volume of a ball with a rank radius t was derived in [17]. It was shown that $V_t(q^m, n) < q^{t(m+n-t)+\sigma(q)}$, where $\sigma(q) \stackrel{\mathrm{def}}{=} \frac{1}{\ln(q)} \sum_{k=1}^{\infty} \frac{1}{k(q^k-1)} < 2$. We also establish a lower bound on $V_t(q^m, n)$.

Lemma 5: For $0 \leq t \leq \min\{n, m\}$, $V_t(q^m, n) \geq q^{t(m+n-t)}$.

We remark that the lower bound in Lemma 5 and the upper bound in [17, Lemma 13] provide a good approximation of $V_t(q^m, n)$.

The diameter of a set is defined to be the maximum distance between any pair of elements in the set [11, p. 172]. For a given diameter $2r$, Kleitman [20] proved that balls with Hamming radius r maximize the cardinality in a vector space over $\mathrm{GF}(2)$. However, when the field is not $\mathrm{GF}(2)$, the result is not necessarily valid [13, p. 40]. We show below that the situation is similar for the rank metric.

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

We now consider the intersection of balls with rank radii.

Lemma 6: If $0 \leq s, t \leq n$ and $\mathbf{c}_1, \mathbf{c}_2 \in \mathrm{GF}(q^m)^n$, then $|B_s(\mathbf{c}_1) \cap B_t(\mathbf{c}_2)|$ depends on only $r = d_{\mathrm{R}}(\mathbf{c}_1, \mathbf{c}_2)$.

Proof: First, without loss of generality, we assume $\mathbf{c}_1 = \mathbf{0}$, and hence $\mathrm{rk}(\mathbf{c}_2) = r$. We can express $\mathbf{c}_2$ as $\mathbf{c}_2 = \mathbf{uB}$, where $\mathbf{u} = (u_0, \ldots, u_{r-1}, 0, \ldots, 0) \in \mathrm{GF}(q^m)^n$ has rank r and $\mathbf{B} \in \mathrm{GF}(q)^{n \times n}$ has full rank. For any $\mathbf{x} \in B_s(\mathbf{0}) \cap B_t(\mathbf{u})$ we have $\mathrm{rk}(\mathbf{xB}) = \mathrm{rk}(\mathbf{x}) \leq s$ and $\mathrm{rk}(\mathbf{xB} - \mathbf{c}_2) = \mathrm{rk}(\mathbf{x} - \mathbf{u}) \leq t$. Thus $|B_s(\mathbf{0}) \cap B_t(\mathbf{uB})| = |B_s(\mathbf{0}) \cap B_t(\mathbf{u})|$, and hence $|B_s(\mathbf{0}) \cap B_t(\mathbf{c}_2)|$ does not depend on the matrix $\mathbf{B}$.

The coordinates of $\mathbf{u}$ all belong to a basis set $\{u_i\}_{i=0}^{m-1}$ of $\mathrm{GF}(q^m)$. Let $\mathbf{x} = (x_0, \ldots, x_{n-1}) \in B_s(\mathbf{0}) \cap B_t(\mathbf{u})$, then we can express x_j as $x_j = \sum_{j=0}^{m-1} a_{i,j} u_i$ with $a_{i,j} \in \mathrm{GF}(q)$ for $0 \leq j \leq n-1$. Suppose $\mathbf{v} \in \mathrm{GF}(q^m)^r$ has rank r, then the coordinates of $\mathbf{v}$ all belong to a basis set $\{v_i\}_{i=0}^{m-1}$ of $\mathrm{GF}(q^m)$. We define $\bar{\mathbf{x}} = (\bar{x}_0, \ldots, \bar{x}_{n-1}) \in \mathrm{GF}(q^m)^n$ such that $\bar{x}_j = \sum_{j=0}^{m-1} a_{i,j} v_i$. We remark that $\mathrm{rk}(\bar{\mathbf{x}}) = \mathrm{rk}(\mathbf{x}) \leq s$ and $\mathrm{rk}(\bar{\mathbf{x}} - \mathbf{v}) = \mathrm{rk}(\mathbf{x} - \mathbf{u}) \leq t$. Thus $|B_s(\mathbf{0}) \cap B_t(\mathbf{v})| = |B_s(\mathbf{0}) \cap B_t(\mathbf{u})|$ and hence $|B_s(\mathbf{0}) \cap B_t(\mathbf{c}_2)|$ does not depend on the vector $\mathbf{u}$ provided that it has rank r. ■

Proposition 2: If $0 \leq s, t \leq n$, $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}'_1, \mathbf{c}'_2 \in \mathrm{GF}(q^m)^n$ and $d_{\mathrm{R}}(\mathbf{c}_1, \mathbf{c}_2) \geq d_{\mathrm{R}}(\mathbf{c}'_1, \mathbf{c}'_2)$, then

$$|B_s(\mathbf{c}_1) \cap B_t(\mathbf{c}_2)| \leq |B_s(\mathbf{c}'_1) \cap B_t(\mathbf{c}'_2)|. \quad (3)$$

Proof: It is clearly sufficient to prove (3) when $d_{\mathrm{R}}(\mathbf{c}_1, \mathbf{c}_2) = d_{\mathrm{R}}(\mathbf{c}'_1, \mathbf{c}'_2) + 1 = e + 1$. By Lemma 6, we can assume without loss of generality that $\mathbf{c}_1 = \mathbf{c}'_1 = \mathbf{0}$, $\mathbf{c}'_2 = (0, c_1, \ldots, c_e, 0, \ldots, 0)$ and $\mathbf{c}_2 = (c_0, c_1, \ldots, c_e, 0, \ldots, 0)$, where $c_0, \ldots, c_e \in \mathrm{GF}(q^m)$ are linearly independent.

We will define an injective mapping ϕ from $B_s(\mathbf{c}_1) \cap B_t(\mathbf{c}_2)$ to $B_s(\mathbf{c}'_1) \cap B_t(\mathbf{c}'_2)$. We consider vectors $\mathbf{z} = (z_0, z_1, \ldots, z_{n-1}) \in B_s(\mathbf{c}_1) \cap B_t(\mathbf{c}_2)$. We thus have $\mathrm{rk}(\mathbf{z}) \leq s$ and $\mathrm{rk}(\mathbf{u}) \leq t$, where $\mathbf{u} = \mathbf{z} - \mathbf{c}_2$. We also define $\bar{\mathbf{z}} = (z_1, \ldots, z_{n-1})$ and $\bar{\mathbf{u}} = (u_1, \ldots, u_{n-1})$.

We need to consider three cases, depending on $\bar{\mathbf{z}}$ and $\bar{\mathbf{u}}$. Firstly, suppose that $\mathrm{rk}(\bar{\mathbf{u}}) \leq t - 1$. We define $\phi(\mathbf{z}) = \mathbf{z}$. We remark that $\mathrm{rk}(\mathbf{z} - \mathbf{c}'_2) \leq \mathrm{rk}(\bar{\mathbf{u}}) + 1 \leq t$ and hence $\phi(\mathbf{z}) \in B_s(\mathbf{c}'_1) \cap B_t(\mathbf{c}'_2)$. Secondly, suppose $\mathrm{rk}(\bar{\mathbf{u}}) = t$ and $\mathrm{rk}(\bar{\mathbf{z}}) \leq s - 1$. We define $\phi(\mathbf{z}) = (z_0 - c_0, z_1, \ldots, z_{n-1})$. We have $\mathrm{rk}(\phi(\mathbf{z})) \leq \mathrm{rk}(\bar{\mathbf{z}}) + 1 \leq s$, $\phi(\mathbf{z}) - \mathbf{c}'_2 = \mathbf{z} - \mathbf{c}_2$, and hence $\phi(\mathbf{z}) \in B_s(\mathbf{c}'_1) \cap B_t(\mathbf{c}'_2)$. Finally, suppose $\mathrm{rk}(\bar{\mathbf{u}}) = t$ and $\mathrm{rk}(\bar{\mathbf{z}}) = s$. Since $\mathrm{rk}(\mathbf{u}) = t$, we have $z_0 - c_0 \in \mathfrak{S}(\bar{\mathbf{u}})$. Similarly, since $\mathrm{rk}(\mathbf{z}) = s$, we have $z_0 \in \mathfrak{S}(\bar{\mathbf{z}})$. Note that $c_0 \in \mathfrak{S}(\bar{\mathbf{u}}) \cup \mathfrak{S}(\bar{\mathbf{z}})$, and may therefore be expressed as $c_0 = c_u + c_z$, where $c_u \in \mathfrak{S}(\bar{\mathbf{u}})$ and $c_z \in \mathfrak{S}(\bar{\mathbf{z}}) \backslash \mathfrak{S}(\bar{\mathbf{u}})$. We define $\phi(\mathbf{z}) = (z_0 - c_z, z_1, \ldots, z_{n-1})$. Remark that $z_0 - c_z \in \mathfrak{S}(\bar{\mathbf{z}})$ and hence $\mathrm{rk}(\phi(\mathbf{z})) = s$. Also, $z_0 - c_z = z_0 - c_0 + c_u \in \mathfrak{S}(\bar{\mathbf{u}})$ and hence $\mathrm{rk}(\phi(\mathbf{z}) - \mathbf{c}'_2) = t$. Therefore $\phi(\mathbf{z}) \in B_s(\mathbf{c}'_1) \cap B_t(\mathbf{c}'_2)$.

We now verify that the mapping ϕ is injective. Suppose there exists $\mathbf{z}' \neq \mathbf{z}$ such that $\phi(\mathbf{z}') = \phi(\mathbf{z})$. Since $\phi(\mathbf{z})$ only modifies the first coordinate of $\mathbf{z}$, we have $\bar{\mathbf{z}}' = \bar{\mathbf{z}}$ and hence

[1] This code is not necessarily linear although the corresponding MRD code is linear.

$\bar{\mathbf{u}}' = \bar{\mathbf{u}}$. Therefore, $\mathbf{z}$ and $\mathbf{z}'$ belong to the same case. It can be easily verified that for each case, the restriction of ϕ is injective, and hence $\mathbf{z}' = \mathbf{z}$. ■

Corollary 2: If $0 \leq s, t \leq n$, $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}'_1, \mathbf{c}'_2 \in \mathrm{GF}(q^m)^n$ and $d_{\mathrm{R}}(\mathbf{c}_1, \mathbf{c}_2) \geq d_{\mathrm{R}}(\mathbf{c}'_1, \mathbf{c}'_2)$, then

$$|B_s(\mathbf{c}_1) \cup B_t(\mathbf{c}_2)| \geq |B_s(\mathbf{c}'_1) \cup B_t(\mathbf{c}'_2)|. \tag{4}$$

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

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

Theorem 1: If $\mathbf{c}_1, \mathbf{c}_2 \in \mathrm{GF}(q^m)^n$ and $d_{\mathrm{R}}(\mathbf{c}_1, \mathbf{c}_2) = r$, 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 $\mathrm{rk}(\mathbf{c}_2) = r$. We consider the vectors $\mathbf{y} \in B_s(\mathbf{0}) \cap B_{r-s}(\mathbf{c}_2)$.

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 $\mathbf{y}$ are in $\mathcal{V}$. Let $\mathbf{y} = \mathbf{y}_{\mathcal{V}} + \mathbf{y}_{\mathcal{W}}$, where $\mathcal{V} \oplus \mathcal{W} = \mathrm{GF}(q^m)^n$. We have $\mathbf{y}_{\mathcal{V}} + (\mathbf{c}_2 - \mathbf{y})_{\mathcal{V}} = \mathbf{c}_2$, with $\mathrm{rk}(\mathbf{y}_{\mathcal{V}}) \leq \mathrm{rk}(\mathbf{y}) = s$ and $\mathrm{rk}((\mathbf{c}_2 - \mathbf{y})_{\mathcal{V}}) \leq \mathrm{rk}(\mathbf{c}_2 - \mathbf{y}) = r - s$. Therefore, $\mathrm{rk}(\mathbf{y}_{\mathcal{V}}) = s$, $\mathrm{rk}((\mathbf{c}_2 - \mathbf{y})_{\mathcal{V}}) = r - s$, and $\mathfrak{S}(\mathbf{y}_{\mathcal{V}}) \cap \mathfrak{S}((\mathbf{c}_2 - \mathbf{y})_{\mathcal{V}}) = \{\mathbf{0}\}$. Since $\mathrm{rk}(\mathbf{y}_{\mathcal{V}}) = \mathrm{rk}(\mathbf{y})$, 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 $\mathfrak{S}(\mathbf{y}_{\mathcal{W}}) \cap \mathfrak{S}((\mathbf{c}_2 - \mathbf{y})_{\mathcal{W}}) = \{\mathbf{0}\}$. But $\mathbf{y}_{\mathcal{W}} + (\mathbf{c}_2 - \mathbf{y})_{\mathcal{W}} = \mathbf{0}$, so $\mathbf{y}_{\mathcal{W}} = (\mathbf{c}_2 - \mathbf{y})_{\mathcal{W}} = \mathbf{0}$.

Let $\mathcal{A} \in E_s(q^m, n)$ and $\mathcal{B} \in E_{r-s}(q^m, n)$ such that $\mathcal{A} \oplus \mathcal{B} = \mathcal{V}$. By Lemma 3, $\mathbf{c}_{2,\mathcal{A}}$ is a vector of rank s with distance $r - s$ from $\mathbf{c}_2$. By Corollary 1, there are $q^{s(r-s)}\begin{bmatrix} r \\ s \end{bmatrix}$ ordered pairs $(\mathcal{A}, \mathcal{B})$. Note that by Lemma 4, all the $\mathbf{c}_{2,\mathcal{A}}$ vectors are distinct. Conversely, if $\mathbf{y} \in \mathcal{V}$ satisfies $\mathrm{rk}(\mathbf{y}) = s$ and $\mathrm{rk}(\mathbf{c}_2 - \mathbf{y}) = r - s$, then $\mathbf{y}$ belongs to some ELS $\mathcal{A}$ and $\mathbf{c}_2 - \mathbf{y} \in \mathcal{B}$ such that $\mathcal{A} \oplus \mathcal{B} = \mathcal{V}$. The vector $\mathbf{y}$ is hence equal to $\mathbf{c}_{2,\mathcal{A}}$. There are hence $q^{s(r-s)}\begin{bmatrix} r \\ s \end{bmatrix}$ vectors $\mathbf{y}$. ■

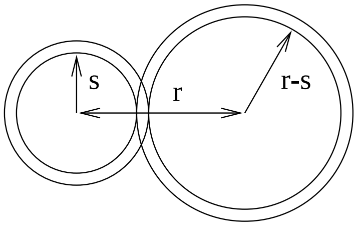

Fig. 1. Illustration of Theorem 1.

As shown in Figure 1, only the outmost layers intersect between two balls of radii s and $r - s$ when the distance between the two centers is r. Theorem 1 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 cardinality of the intersection of three balls with rank radii is not determined by the pairwise distances between the centers. We give a simple example to illustrate this point: consider $\mathrm{GF}(2^2)^3$ 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 $d_{\mathrm{R}}(\mathbf{c}_1, \mathbf{c}_2) = d_{\mathrm{R}}(\mathbf{c}_2, \mathbf{c}_3) = d_{\mathrm{R}}(\mathbf{c}_3, \mathbf{c}_1) = 2$ and $d_{\mathrm{R}}(\mathbf{c}'_1, \mathbf{c}'_2) = d_{\mathrm{R}}(\mathbf{c}'_2, \mathbf{c}'_3) = d_{\mathrm{R}}(\mathbf{c}'_3, \mathbf{c}'_1) = 2$. 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 [13, p. 58], provided that the field $\mathrm{GF}(q^m)$ is not the binary field $\mathrm{GF}(2)$.

C. Bounds based on 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 $\mathrm{GF}(q^m)$, length n, and radius ρ, we want to determine the minimum number of balls of rank radius ρ which cover $\mathrm{GF}(q^m)^n$ entirely. Without loss of generality, we assume that $n \leq m$.

Definition 1: For all q^m, n, and $0 \leq \rho \leq n$, we define $K_{\mathrm{R}}(q^m, n, \rho)$ as the minimum cardinality of a (linear or nonlinear) code over $\mathrm{GF}(q^m)$ with length n and rank covering radius ρ.

Note that $K_{\mathrm{R}}(q^m, n, \rho)$ is the cardinality of an optimal covering code. We remark that $K_{\mathrm{R}}(q^m, n, 0) = q^{mn}$ and $K_{\mathrm{R}}(q^m, n, n) = 1$. Two bounds on $K_{\mathrm{R}}(q^m, n, \rho)$ can be easily derived for $0 < \rho < n$.

Proposition 4: For all q^m, n, and $0 < \rho < n$, we have

$$\frac{q^{mn}}{V_\rho(q^m, n)} < K_{\mathrm{R}}(q^m, n, \rho) \leq q^{m(n-\rho)}. \tag{5}$$

We refer to the lower bound in (5) as the sphere-covering bound. An alternative upper bound on $K_{\mathrm{R}}(q^m, n, \rho)$ is given by $K_{\mathrm{H}}(q^m, n, \rho)$, the minimum cardinality of a (linear or nonlinear) code over $\mathrm{GF}(q^m)$ with length n and Hamming covering radius ρ. Indeed, any code with Hamming covering radius ρ has rank covering radius $\leq \rho$. Since $K_{\mathrm{H}}(q^m, n, \rho) \leq q^{m(n-\rho)}$, this upper bound is tighter than the one given in Proposition 4. Unfortunately, the Hamming covering radius of codes has been extensively studied only when $q^m = 2$ or 3 [13], which are irrelevant to our problem.

We will derive two nontrivial lower bounds on $K_{\mathrm{R}}(q^m, n, \rho)$.

Proposition 5: For all q^m, n, and $0 < \rho < n$, we have

$$K_{\mathrm{R}}(q^m, n, \rho) \geq \frac{q^{mn} - A_{\mathrm{R}}(q^m, n, 2\rho+1)q^{\rho^2}\begin{bmatrix} 2\rho \\ \rho \end{bmatrix}}{V_\rho(q^m, n) - q^{\rho^2}\begin{bmatrix} 2\rho \\ \rho \end{bmatrix}}, \tag{6}$$

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

The proof of this bound follows the approach in [21, Theorem 1]. Next, we obtain both sufficient and necessary conditions under which the bound is nontrivial, i.e., when the denominator on the RHS of (6) is positive.

Lemma 7: The denominator on the RHS of (6) is positive if $m + n \geq 5$ for $\rho = 1$ and $m + n \geq 3\rho + 1$ for $\rho \geq 2$.

Lemma 8: The denominator on the RHS of (6) is positive only if $m + n \geq 3\rho$.

We remark that when the bound in (6) is nontrivial, it is at least as tight as the sphere-covering bound given in (5).

Proposition 6: If $\epsilon > 0$, then

$$K_{\mathrm{R}}(q^m, n, \rho) \geq \frac{q^{mn}}{V_\rho(q^m, n) - \frac{\epsilon}{\delta}N_\rho(q^m, n)}, \tag{7}$$

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

$$\begin{aligned}\epsilon &\overset{\text{def}}{=} \left\lceil \frac{(q^m - q^\rho)(\begin{bmatrix}n\\1\end{bmatrix} - \begin{bmatrix}\rho\\1\end{bmatrix})}{q^\rho \begin{bmatrix}\rho+1\\1\end{bmatrix}} \right\rceil q^\rho \begin{bmatrix}\rho+1\\1\end{bmatrix}\\ &- (q^m - q^\rho)\left(\begin{bmatrix}n\\1\end{bmatrix} - \begin{bmatrix}\rho\\1\end{bmatrix}\right). \qquad (8)\end{aligned}$$

The proof for this bound uses the approach in [19] and is based on the concept of excess reviewed in Section II-D. We remark that, unlike the bound given in Proposition 5, the bound in Proposition 6 is always applicable. The lower bound in 6 is always at least as tight as the sphere-covering bound given in (5).

m	n	ρ	(5) lower	(6)	(7)	(5) upper
2	2	1	2	3	2	4
3	2	1	3	4	3	8
	3	1	11	11	11	64
		2	2	-	2	8
4	2	1	6	7	6	16
	3	1	39	40	39	256
		2	3	4	3	16
	4	1	290	291	293	4096
		2	9	10	10	256
		3	2	-	2	16

TABLE I

BOUNDS ON $K_{\text{R}}(2^m, n, \rho)$ FOR $2 \leq m \leq 4$, $2 \leq n \leq m$, AND $0 < \rho < n$.

Table I gives the values of the bounds on $K_{\text{R}}(2^m, n, \rho)$ for $m \leq 4$. The values for all three lower bounds in Table I are obtained by applying the ceiling function to the lower bounds. As seen in Table I, the lower bounds remain far below the upper bound in (5). Also, note that in some cases the bound in (6) is tighter than that in (7), and the bound in (7) is tighter in other cases.

D. Covering properties of linear rank metric codes

The (n, k) linear codes whose rank covering radius ρ have been determined in [15] all satisfy $\rho = n - k$ and hence have maximal rank covering radius. The trivial linear codes with dimension $k = 0$ or $k = n$ for $n \leq m$ also satisfy the equality. In this subsection, we determine other types of linear codes which satisfy $\rho = n - k$ for $n \leq m$.

First, we determine the rank covering radius of ELS's.

Lemma 9: The rank covering radius of $\mathcal{V} \in E_v(q^m, n)$ is $\rho = n - v$.

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

Proposition 7: An (n, k) linear code over $\text{GF}(q^m)$ with rank covering radius ρ satisfies

$$n - \rho - \frac{\rho(n-\rho) + \sigma(q)}{m} < k \leq n - \rho. \qquad (9)$$

Proof: The proof for the upper bound is straightforward, and we now prove the lower bound. By the sphere-covering bound, we have $q^{mk} > \frac{q^{mn}}{V_\rho(q^m,n)}$. However, we have $V_\rho(q^m, n) < q^{\rho(m+n-\rho)+\sigma(q)}$ [17], and hence $q^{mk} > q^{mn-\rho(m+n-\rho)-\sigma(q)}$. ∎

We now show that the bounds in Proposition 7 are tight in some cases.

Corollary 3: An (n, k) linear code over $\text{GF}(q^m)$ $(n \leq m)$ with rank covering radius ρ such that $\rho(n - \rho) \leq m - \sigma(q)$ has dimension $k = n - \rho$.

Next, the linear codes with $\rho = 1$ or $\rho = n - 1$ are shown to also satisfy the equality.

Proposition 8: Let $\mathcal{C}$ be an (n, k) linear code over $\text{GF}(q^m)$ $(n \leq m)$ with rank covering radius ρ. Then $k = n - 1$ if and only if $\rho = 1$, and $k = 1$ if $\rho = n - 1$.

Proof: The case $\rho = n - 1$ is straightforward. Suppose $\rho = 1$, then $k \leq n-1$. By the sphere-covering bound k satisfies $q^{mk} > \frac{q^{mn}}{V_1(q^m,n)}$. However, $V_1(q^m, n) < q^{m+n} \leq q^{2m}$, and hence $k > n - 2$, which concludes the proof. ∎

REFERENCES

[1] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems on Information Transmission*, vol. 21, no. 1, pp. 1–12, Jan. 1985.

[2] 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.

[3] 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.

[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] A. Kshevetskiy and E. M. Gabidulin, "The new construction of rank codes," *Proc. IEEE Int. Symp. on Information Theory*, pp. 2105–2108, Sept. 2005.

[6] W. B. Vasantha and N. Suresh Babu, "On the covering radius of rank-distance codes," *Ganita Sandesh*, vol. 13, pp. 43–48, 1999.

[7] W. B. Vasantha and R. J. Selvaraj, "Multi-covering radii of codes with rank metric," *Proc. Information Theory Workshop*, p. 215, Oct. 2002.

[8] 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.

[9] P. Loidreau, "Properties of codes in rank metric," preprint.

[10] 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.

[11] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[12] R. Blahut, *Theory and Practice of Error Control Codes*. Addison-Wesley, 1983.

[13] G. D. Cohen, I. Honkala, S. Litsyn, and A. C. Lobstein, *Covering Codes*. Elsevier, 1997.

[14] N. Suresh Babu, "Studies on rank distance codes," Ph.D Dissertation, IIT Madras, Feb. 1995.

[15] M. Gadouleau and Z. Yan, "Properties of codes with the rank metric," *Proceedings of 2006 IEEE Globecom*, November 2006.

[16] 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.

[17] M. Gadouleau and Z. Yan, "Error performance analysis of maximum rank distance codes," *Submitted to IEEE Transactions on Information Theory*, http://arxiv.org/pdf/cs.IT/0612051.

[18] G. van Wee, "Improved sphere bounds on the covering radius of codes," *IEEE Trans. Info. Theory*, vol. 34, pp. 237–245, 1988.

[19] ——, "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.

[20] D. J. Kleitman, "On a combinatorial conjecture of Erdös," *Journal of Combinatorial Theory*, vol. 1, pp. 209–214, 1966.

[21] 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.