Packing and Covering Properties of Rank Metric Codes

Maximilien Gadouleau, *Student Member, IEEE*, and Zhiyuan Yan, *Senior Member, IEEE*

***Abstract*—This paper investigates packing and covering properties of codes with the rank metric. First, we investigate 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.**

***Index Terms*—Covering radius, error control codes, rank metric codes.**

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 by Delsarte [2]. The potential applications of rank metric codes to wireless communications [3], public-key cryptosystems [4], storage equipments [5], [6], and network coding [7]–[9] have motivated a steady stream of works [2], [5], [6], [10]–[22], described below, that focus on their properties.

The majority [2], [5], [6], [10], [15], [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 error control codes, 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 error control codes have been extensively studied (see, for example, [25] and [26]), 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 [11], [12], and [19]. In [13], a sphere covering bound for rank metric codes was introduced. Generalizing the concept of rank covering radius, the multicovering radii of codes with the rank metric were defined in [14]. 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 as follows.

- In Section III, we investigate 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 IV, we establish further properties of elementary linear subspaces (ELSs) [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 counterparts in [22]. These technical results are used later in our investigation of properties of rank metric codes.
- 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 [13]. 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.

Manuscript received June 21, 2007; revised May 12, 2008. Published August 27, 2008 (projected). This work was supported in part by Thales Communications, Inc. and in part by a Grant from the Commonwealth of Pennsylvania, Department of Community and Economic Development, through the Pennsylvania Infrastructure Technology Alliance (PITA). The material in this paper was presented at IEEE Globecom, Washington, DC, November 2007.

The authors are with the Department of Electrical and Computer Engineering, Lehigh University, Bethlehem, PA 18015 USA (e-mail: magc@lehigh.edu; yan@lehigh.edu).

Communicated by L. M. G. M. Tolhuizen, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2008.928284

II. Preliminaries

A. Rank Metric

Consider an n-dimensional vector $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1}) \in \mathrm{GF}(q^m)^n$. The field $\mathrm{GF}(q^m)$ may be viewed as an m-dimensional vector space over $\mathrm{GF}(q)$. The rank weight of $\boldsymbol{x}$, denoted as $\mathrm{rk}(\boldsymbol{x})$, is defined to be the *maximum* number of coordinates in $\boldsymbol{x}$ that are linearly independent over $\mathrm{GF}(q)$ [10]. Note that all ranks are with respect to $\mathrm{GF}(q)$ unless otherwise specified in this paper. The coordinates of $\boldsymbol{x}$ thus span a linear subspace of $\mathrm{GF}(q^m)$, denoted as $\mathfrak{S}(\boldsymbol{x})$ or $\mathfrak{S}(x_0, x_1, \ldots, x_{n-1})$, with dimension equal to $\mathrm{rk}(\boldsymbol{x})$. For any basis B_m of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$, each coordinate of $\boldsymbol{x}$ can be expanded to an m-dimensional column vector over $\mathrm{GF}(q)$ with respect to B_m. The rank weight of $\boldsymbol{x}$ is hence the rank of the $m \times n$ matrix over $\mathrm{GF}(q)$ obtained by expanding all the coordinates of $\boldsymbol{x}$. For all $\boldsymbol{x}, \boldsymbol{y} \in \mathrm{GF}(q^m)^n$, it is easily verified that $d_{\mathrm{R}}(\boldsymbol{x}, \boldsymbol{y}) \stackrel{\mathrm{def}}{=} \mathrm{rk}(\boldsymbol{x} - \boldsymbol{y})$ is a metric over $\mathrm{GF}(q^m)^n$ [10], referred to as the *rank metric* henceforth. The *minimum rank distance* of a code $\mathcal{C}$, denoted as $d_{\mathrm{R}}(\mathcal{C})$, 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}.

Because the rank weight can be defined from either a matrix perspective or a vector viewpoint, both the matrix form [2], [6] and the vector form [10] for rank metric codes have been considered in the literature. Following [10], in this paper, we use mostly the vector form over GF(q^m) for rank metric codes so that our results and their derivations for rank metric codes can be readily related to their counterparts for Hamming metric codes. The matrix perspective is also used when it either is more convenient or provides more insights.

B. Sphere Packing and Sphere Covering Problems

The sphere packing problem we consider is as follows: given a finite field GF(q^m), length n, and radius r, what is the maximum number of nonintersecting balls with radius r that can be packed into GF$(q^m)^n$? The sphere packing problem is equivalent to finding the maximum cardinality of a code over 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 nonintersecting spheres centered at all codewords cover the *whole* space, the code is called a perfect code.

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 [26]. It is the maximal distance from any vector in GF$(q^m)^n$ to the code C. That is, $\rho = \max_{\boldsymbol{x} \in \mathrm{GF}(q^m)^n} \{d(\boldsymbol{x}, C)\}$. 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 the same length and minimum distance such that $C \subset C'$. A maximal code has covering radius $\rho \leq d-1$. The sphere covering problem for the rank metric can be stated as follows: given an extension field GF(q^m), length n, and radius ρ, we want to determine the minimum number of balls of rank radius ρ, which cover GF$(q^m)^n$ entirely. The sphere covering problem is equivalent to finding the minimum cardinality of a code over GF(q^m) with length n and rank covering radius ρ.

III. Packing Properties of Rank Metric Codes

It can be shown that the cardinality K of a code C over GF(q^m) with length n and minimum rank distance d_{R} satisfies $K \leq \min\{q^{m(n-d_{\mathrm{R}}+1)}, q^{n(m-d_{\mathrm{R}}+1)}\}$. We refer to this bound as the Singleton bound for codes with the rank metric, and refer to codes that attain the Singleton bound as maximum rank distance (MRD) codes. We remark that special cases of this more general Singleton bound were proposed in [10], [6], and [27].

For any given parameter set n, m, and d_{R}, explicit construction for linear or nonlinear MRD codes exists. For $n \leq m$ and $d_{\mathrm{R}} \leq n$, generalized Gabidulin codes [16] can be constructed. For $n > m$ and $d_{\mathrm{R}} \leq m$, an MRD code can be constructed by transposing a generalized Gabidulin code of length m and minimum rank distance d_{R} over GF(q^n), although this code is not necessarily linear over GF(q^m). When $n = lm$ $(l \geq 2)$, linear MRD codes of length n and minimum distance d_{R} can be constructed by a Cartesian product $\mathcal{G}^l$ of an (m, k) generalized Gabidulin code $\mathcal{G}$. Although maximum distance separable 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 GF(q^m). This has significant impact on the packing properties of rank metric codes as explained below.

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 [11], [12], 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 GF(q^m) with length n and minimum distance $d_{\mathrm{R}} = 2r+1$ as $A_{\mathrm{R}}(q^m, n, d_{\mathrm{R}})$. Thus, for $d_{\mathrm{R}} > \min\{n, m\}$, $A_{\mathrm{R}}(q^m, n, d_{\mathrm{R}}) = 1$ and for $d_{\mathrm{R}} \leq \min\{n, m\}$, $A_{\mathrm{R}}(q^m, n, d_{\mathrm{R}}) = \min\{q^{m(n-d_{\mathrm{R}}+1)}, q^{n(m-d_{\mathrm{R}}+1)}\}$. 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 $A_{\mathrm{R}}(q^m, n, d_{\mathrm{R}})$ when both block length and minimum rank distance go to infinity. However, this cannot be achieved for finite m because the minimum rank distance is no greater than m. Thus, we consider the case where $\lim_{n\to\infty} \frac{n}{m} = b$, where b is a constant.

Define $\delta \stackrel{\mathrm{def}}{=} \lim_{n\to\infty} \frac{d_{\mathrm{R}}}{n}$ and

$$a(\delta) \stackrel{\mathrm{def}}{=} \lim_{n\to\infty} \sup[\log_{q^{mn}} A_{\mathrm{R}}(q^m, n, \lfloor \delta n \rfloor)]$$

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.

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

IV. Technical Results

To simplify notations, we will 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 $N_u(q^m, n) = \begin{bmatrix} n \\ u \end{bmatrix} \alpha(m, u)$ [10], where $\alpha(m, 0) \stackrel{\mathrm{def}}{=} 1$ and $\alpha(m, u) \stackrel{\mathrm{def}}{=} \prod_{i=0}^{u-1} (q^m - q^i)$ for $u \geq 1$. The $\begin{bmatrix} n \\ u \end{bmatrix}$ term is often referred to as a Gaussian polynomial [28], defined as $\begin{bmatrix} n \\ u \end{bmatrix} \stackrel{\mathrm{def}}{=} \alpha(n, u)/\alpha(u, u)$.

A. Further Properties of Elementary Linear Subspaces

The concept of ELS 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 Gabidulin codes (see [21]). Although our results may be derived without the concept of ELS, we have adopted it in this

paper because it enables readers to easily relate our approach and results to their counterparts for Hamming metric codes.

If there exists a basis set B of vectors in $\mathrm{GF}(q)^n$ for a linear subspace $\mathcal{V} \subseteq \mathrm{GF}(q^m)^n$, we say $\mathcal{V}$ is an ELS and B is an elementary basis of $\mathcal{V}$. We denote the set of all ELSs of $\mathrm{GF}(q^m)^n$ with dimension v as $E_v(q^m, n)$. The properties of an ELS are summarized as follows [21]. 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 $\mathcal{V} \oplus \bar{\mathcal{V}} = \mathrm{GF}(q^m)^n$, where $\oplus$ denotes the direct sum of two subspaces. For any vector $\boldsymbol{x} \in \mathrm{GF}(q^m)^n$, we denote the projection of $\boldsymbol{x}$ on $\mathcal{V}$ along $\bar{\mathcal{V}}$ as $\boldsymbol{x}_{\mathcal{V}}$, and we remark that $\boldsymbol{x} = \boldsymbol{x}_{\mathcal{V}} + \boldsymbol{x}_{\bar{\mathcal{V}}}$. Note that $|E_u(q^m, n)| = \begin{bmatrix} n \\ u \end{bmatrix}$ does not depend on m.

Lemma 1: Any vector $\boldsymbol{x} \in \mathrm{GF}(q^m)^n$ 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 $\{\boldsymbol{v}_i\}_{i=0}^{r-1}$, where $\boldsymbol{v}_i \in \mathrm{GF}(q)^n$ for all i. Suppose $\boldsymbol{x}$ also belongs to $\mathcal{W}$, where $\mathcal{W} \in E_r(q^m, n)$ has an elementary basis $\{\boldsymbol{w}_j\}_{j=0}^{r-1}$, where $\boldsymbol{w}_j \in \mathrm{GF}(q)^n$ for all j. Therefore, $\boldsymbol{x} = \sum_{i=0}^{r-1} a_i \boldsymbol{v}_i = \sum_{j=0}^{r-1} b_j \boldsymbol{w}_j$, where $a_i, b_j \in \mathrm{GF}(q^m)$ for $0 \leq i, j \leq r-1$. By definition, we have $\mathfrak{S}(\boldsymbol{x}) = \mathfrak{S}(a_0, \ldots, a_{r-1}) = \mathfrak{S}(b_0, \ldots, b_{r-1})$, 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 $c_{j,i} \in \mathrm{GF}(q)$. Hence, $\boldsymbol{x} = \sum_{i=0}^{r-1} a_i \boldsymbol{u}_i$, where $\boldsymbol{u}_i = \sum_{j=0}^{r-1} c_{j,i} \boldsymbol{w}_j$ for $0 \leq i \leq r-1$ form an elementary basis of $\mathcal{W}$. Considering the matrix obtained by expanding the coordinates of $\boldsymbol{x}$ with respect to the basis $\{a_i\}_{i=0}^{m-1}$, we obtain $\boldsymbol{v}_i = \boldsymbol{u}_i$, and hence, $\mathcal{V} = \mathcal{W}$. □

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

In [21], it was shown that an ELS always has a complementary ELS. The following lemma enumerates such complementary ELSs.

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 $q^{a(v-a)}$ ELSs $\mathcal{B}$ 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 $\mathrm{GF}(q)$ in $\mathcal{V} \backslash \mathcal{A}$ 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 $\mathrm{GF}(q)$ 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 $\mathcal{B}$. Because 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 $\boldsymbol{u} \in \mathcal{V}$ has rank v, then $\mathrm{rk}(\boldsymbol{u}_{\mathcal{A}}) = a$ and $\mathrm{rk}(\boldsymbol{u}_{\mathcal{B}}) = v - a$ 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, $\boldsymbol{u}_{\mathcal{A}} \in \mathcal{A}$ and hence $\mathrm{rk}(\boldsymbol{u}_{\mathcal{A}}) \leq a$ by [21, Prop. 2]; similarly, $\mathrm{rk}(\boldsymbol{u}_{\mathcal{B}}) \leq v - a$. Now suppose $\mathrm{rk}(\boldsymbol{u}_{\mathcal{A}}) < a$ or $\mathrm{rk}(\boldsymbol{u}_{\mathcal{B}}) < v - a$, then $v = \mathrm{rk}(\boldsymbol{u}) \leq \mathrm{rk}(\boldsymbol{u}_{\mathcal{A}}) + \mathrm{rk}(\boldsymbol{u}_{\mathcal{B}}) < a + v - a = v$. □

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

Lemma 4: Suppose $\mathcal{V} \in E_v(q^m, n)$ and $\boldsymbol{u} \in \mathcal{V}$ 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 $f_{\boldsymbol{u}}(\mathcal{A}, \mathcal{B}) = \boldsymbol{u}_{\mathcal{A}}$ and $g_{\boldsymbol{u}}(\mathcal{A}, \mathcal{B}) = \boldsymbol{u}_{\mathcal{B}}$. Then, both $f_{\boldsymbol{u}}$ and $g_{\boldsymbol{u}}$ are injective.

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

B. Properties of Balls With Rank Radii

We refer to all vectors in $\mathrm{GF}(q^m)^n$ within rank distance r of $\boldsymbol{x} \in \mathrm{GF}(q^m)^n$ as a ball of rank radius r centered at $\boldsymbol{x}$, and denote it as $B_r(\boldsymbol{x})$. Its volume, which does not depend on $\boldsymbol{x}$, is denoted as $V_r(q^m, n) = \sum_{u=0}^{r} N_u(q^m, n)$. When there is no ambiguity about the vector space, we denote $V_r(q^m, n)$ as $v(r)$.

Lemma 5: For $0 \leq r \leq \min\{n, m\}$, $q^{r(m+n-r)} \leq V_r(q^m, n) < K_q^{-1} q^{r(m+n-r)}$, where $K_q \stackrel{\mathrm{def}}{=} \prod_{j=1}^{\infty}(1 - q^{-j})$ [21].

Proof: The upper bound 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 $\boldsymbol{0}$. We now prove the lower bound by constructing $q^{r(m+n-r)}$ vectors $\boldsymbol{z} \in \mathrm{GF}(q^m)^n$ of rank at most r. Let $\boldsymbol{x} \in \mathrm{GF}(q^m)^r$ be a subspace $\mathfrak{T}$ of $\mathrm{GF}(q^m)$ such that $\dim(\mathfrak{T}) = r$ and $\mathfrak{S}(\boldsymbol{x}) \subseteq \mathfrak{T}$. We consider the vectors $\boldsymbol{y} \in \mathrm{GF}(q^m)^{n-r}$ such that $\mathfrak{S}(\boldsymbol{y}) \subseteq \mathfrak{T}$. There are q^{mr} choices for $\boldsymbol{x}$ and, for a given $\boldsymbol{x}$, $q^{r(n-r)}$, choices for $\boldsymbol{y}$. Thus, the total number of vectors $\boldsymbol{z} = (\boldsymbol{x}, \boldsymbol{y}) \in \mathrm{GF}(q^m)^n$ is $q^{r(m+n-r)}$, and because $\mathfrak{S}(\boldsymbol{z}) \subseteq \mathfrak{T}$, we have $\mathrm{rk}(\boldsymbol{z}) \leq r$. □

We remark that both bounds in Lemma 5 are tighter than their respective counterparts in [21, Prop. 1]. More importantly, the two bounds in Lemma 5 differ only by a factor of K_q, and thus, they not only provide a good approximation of $V_r(q^m, n)$, but also accurately describe the asymptotic behavior of $V_r(q^m, n)$. This will enable us to determine the asymptotic behavior of the solution to sphere covering problem in Section V-G.

The diameter of a set is defined to be the maximum distance between any pair of elements in the set [26, p. 172]. For a binary vector space $\mathrm{GF}(2)^n$ and a given diameter $2r < n$, Kleitman [29] 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 $\mathrm{GF}(2)$, the result is not necessarily valid [26, p. 40]. We show below that balls with

rank radii do not maximize the cardinality of a set with a given diameter.

Proposition 2: For $2 \le 2r \le n \le m$, any $S \in E_{2r}(q^m, n)$ has diameter $2r$ and cardinality $|S| > V_r(q^m, n)$.

Proof: Any $S \in E_{2r}(q^m, n)$ 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 $r \ge 2$, we have $V_r(q^m, n) < K_q^{-1} q^{r(n+m)-r^2}$ by Lemma 5. Because $r^2 > 2 > -\log_q K_q$, we obtain $V_r(q^m, n) < q^{r(n+m)} \le |S|$. □

The intersection of balls with Hamming radii has been studied in [26, ch. 2], and below we investigate the intersection of balls with rank radii.

Lemma 6: If $0 \le r, s \le n$ and $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathrm{GF}(q^m)^n$, then $|B_r(\boldsymbol{c}_1) \cap B_s(\boldsymbol{c}_2)|$ depends on $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ only through $d_{\mathrm{R}}(\boldsymbol{c}_1, \boldsymbol{c}_2)$.

Proof: This follows from the fact that matrices in $\mathrm{GF}(q)^{m \times n}$ together with the rank metric form an association scheme [2], [30]. □

Proposition 3: If $0 \le r, s \le n, \boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}'_1, \boldsymbol{c}'_2 \in \mathrm{GF}(q^m)^n$ and $d_{\mathrm{R}}(\boldsymbol{c}_1, \boldsymbol{c}_2) > d_{\mathrm{R}}(\boldsymbol{c}'_1, \boldsymbol{c}'_2)$, then $|B_r(\boldsymbol{c}_1) \cap B_s(\boldsymbol{c}_2)| \le |B_r(\boldsymbol{c}'_1) \cap B_s(\boldsymbol{c}'_2)|$.

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

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

- Case I: $\mathrm{rk}(\bar{\boldsymbol{u}}) \le s-1$. In this case, $\phi(\boldsymbol{z}) \stackrel{\mathrm{def}}{=} \boldsymbol{z}$. We remark that $\mathrm{rk}(\boldsymbol{z} - \boldsymbol{c}'_2) \le \mathrm{rk}(\bar{\boldsymbol{u}}) + 1 \le s$, and hence, $\phi(\boldsymbol{z}) \in B_r(\boldsymbol{c}'_1) \cap B_s(\boldsymbol{c}'_2)$.
- Case II: $\mathrm{rk}(\bar{\boldsymbol{u}}) = s$ and $\mathrm{rk}(\bar{\boldsymbol{z}}) \le r-1$. In this case, $\phi(\boldsymbol{z}) \stackrel{\mathrm{def}}{=} (z_0 - c_0, z_1, \ldots, z_{n-1})$. We have $\mathrm{rk}(\phi(\boldsymbol{z})) \le \mathrm{rk}(\bar{\boldsymbol{z}}) + 1 \le r$ and $\mathrm{rk}(\phi(\boldsymbol{z}) - \boldsymbol{c}'_2) = \mathrm{rk}(\boldsymbol{z} - \boldsymbol{c}_2) \le s$, and hence, $\phi(\boldsymbol{z}) \in B_r(\boldsymbol{c}'_1) \cap B_s(\boldsymbol{c}'_2)$.
- Case III: $\mathrm{rk}(\bar{\boldsymbol{u}}) = s$ and $\mathrm{rk}(\bar{\boldsymbol{z}}) = r$. Because $\mathrm{rk}(\boldsymbol{u}) = s$, we have $z_0 - c_0 \in \mathfrak{S}(\bar{\boldsymbol{u}})$. Similarly, because $\mathrm{rk}(\boldsymbol{z}) = r$, we have $z_0 \in \mathfrak{S}(\bar{\boldsymbol{z}})$. Denote $\dim(\mathfrak{S}(\bar{\boldsymbol{u}}, \bar{\boldsymbol{z}}))$ as d ($d \ge s$). For $d > s$, let $\alpha_0, \ldots, \alpha_{d-1}$ be a basis of $\mathfrak{S}(\bar{\boldsymbol{u}}, \bar{\boldsymbol{z}})$ such that $\alpha_0, \ldots, \alpha_{s-1} \in \mathfrak{S}(\bar{\boldsymbol{u}})$ and $\alpha_s, \ldots, \alpha_{d-1} \in \mathfrak{S}(\bar{\boldsymbol{z}})$. This basis is fixed for all vectors $\boldsymbol{z}$ having the same $\bar{\boldsymbol{z}}$, i.e., it is fixed for all values of z_0. Note that $c_0 \in \mathfrak{S}(\bar{\boldsymbol{u}}, \bar{\boldsymbol{z}})$, and may, therefore, be uniquely expressed as $c_0 = c_u + c_z$, where $c_u \in \mathfrak{S}(\alpha_0, \ldots, \alpha_{s-1}) = \mathfrak{S}(\bar{\boldsymbol{u}})$ and $c_z \in \mathfrak{S}(\alpha_s, \ldots, \alpha_{d-1}) \subseteq \mathfrak{S}(\bar{\boldsymbol{z}})$. If $d = s$, then $c_z = 0 \in \mathfrak{S}(\bar{\boldsymbol{z}})$. In this case, $\phi(\boldsymbol{z}) \stackrel{\mathrm{def}}{=} (z_0 - c_z, z_1, \ldots, z_{n-1})$. Remark that $z_0 - c_z \in \mathfrak{S}(\bar{\boldsymbol{z}})$, and hence, $\mathrm{rk}(\phi(\boldsymbol{z})) = r$. Also, $z_0 - c_z = z_0 - c_0 + c_u \in \mathfrak{S}(\bar{\boldsymbol{u}})$, and hence, $\mathrm{rk}(\phi(\boldsymbol{z}) - \boldsymbol{c}'_2) = s$. Therefore, $\phi(\boldsymbol{z}) \in B_r(\boldsymbol{c}'_1) \cap B_s(\boldsymbol{c}'_2)$.

It can be easily verified that ϕ is injective, hence $|B_r(\boldsymbol{c}_1) \cap B_s(\boldsymbol{c}_2)| \le |B_r(\boldsymbol{c}'_1) \cap B_s(\boldsymbol{c}'_2)|$. □

Corollary 1: If $0 \le r, s \le n, \boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}'_1, \boldsymbol{c}'_2 \in \mathrm{GF}(q^m)^n$ and $d_{\mathrm{R}}(\boldsymbol{c}_1, \boldsymbol{c}_2) \ge d_{\mathrm{R}}(\boldsymbol{c}'_1, \boldsymbol{c}'_2)$, then $|B_r(\boldsymbol{c}_1) \cup B_s(\boldsymbol{c}_2)| \ge |B_r(\boldsymbol{c}'_1) \cup B_s(\boldsymbol{c}'_2)|$.

Proof: The result follows from $|B_r(\boldsymbol{c}_1) \cup B_s(\boldsymbol{c}_2)| = v(r) + v(s) - |B_r(\boldsymbol{c}_1) \cap B_s(\boldsymbol{c}_2)|$. □

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

Proof: By Lemma 6, we assume without loss of generality that $\boldsymbol{c}_2 = \boldsymbol{0}$ and $\mathrm{rk}(\boldsymbol{c}_1) = r$. By Lemma 1, the vector $\boldsymbol{c}_1$ belongs to a unique ELS $\mathcal{V} \in E_r(q^m, n)$. First, it is easy to check that $\boldsymbol{y} = \boldsymbol{0} \in B_r(\boldsymbol{c}_1) \cap B_1(\boldsymbol{0})$. We now consider a nonzero vector $\boldsymbol{y} \in B_1(\boldsymbol{0})$ with rank 1. We have $d_{\mathrm{R}}(\boldsymbol{y}, \boldsymbol{c}_1) = r+1$ if and only if $\boldsymbol{y} \notin \mathcal{V}$ and $\mathfrak{S}(\boldsymbol{y}) \subseteq \mathfrak{S}(\boldsymbol{c}_1)$. There are $\frac{(q^n-q^r)(q^m-q^r)}{q-1}$ such vectors. Thus, $|B_r(\boldsymbol{c}_1) \cap B_1(\boldsymbol{c}_2)| = 1 + N_1(q^m, n) - \frac{(q^n-q^r)(q^m-q^r)}{q-1} = 1 + (q^m - q^r) \begin{bmatrix} r \\ 1 \end{bmatrix} + (q^r - 1) \begin{bmatrix} n \\ 1 \end{bmatrix}$. □

Proposition 5: If $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathrm{GF}(q^m)^n$ and $d_{\mathrm{R}}(\boldsymbol{c}_1, \boldsymbol{c}_2) = r$, then $|B_s(\boldsymbol{c}_1) \cap B_{r-s}(\boldsymbol{c}_2)| = q^{s(r-s)} \begin{bmatrix} r \\ s \end{bmatrix}$ for $0 \le s \le r$.

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

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

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 $\mathcal{A} \oplus \mathcal{B} = \mathcal{V}, \boldsymbol{c}_{2,\mathcal{A}}$ is a vector of rank s with distance $r - s$ from $\boldsymbol{c}_2$ by Lemma 3. By Lemma 4, all the $\boldsymbol{c}_{2,\mathcal{A}}$ vectors are distinct. There are thus as many vectors $\boldsymbol{y}$ 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 $\boldsymbol{y}$. □

The problem of the intersection of three balls with rank radii is more complicated because 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 $\mathrm{GF}(2^2)^3$ and the vectors $\boldsymbol{c}_1 = \boldsymbol{c}'_1 = (0,0,0), \boldsymbol{c}_2 = \boldsymbol{c}'_2 = (1, \alpha, 0), \boldsymbol{c}_3 = (\alpha, 0, 1)$, and $\boldsymbol{c}'_3 = (\alpha, \alpha+1, 0)$, where α is a primitive element of the field. It can be verified that $d_{\mathrm{R}}(\boldsymbol{c}_1, \boldsymbol{c}_2) = d_{\mathrm{R}}(\boldsymbol{c}_2, \boldsymbol{c}_3) = d_{\mathrm{R}}(\boldsymbol{c}_3, \boldsymbol{c}_1) = 2$ and $d_{\mathrm{R}}(\boldsymbol{c}'_1, \boldsymbol{c}'_2) = d_{\mathrm{R}}(\boldsymbol{c}'_2, \boldsymbol{c}'_3) = d_{\mathrm{R}}(\boldsymbol{c}'_3, \boldsymbol{c}'_1) = 2$. However, $B_1(\boldsymbol{c}_1) \cap B_1(\boldsymbol{c}_2) \cap B_1(\boldsymbol{c}_3) = \{(\alpha+1, 0, 0)\}$, whereas

$B_1(\boldsymbol{c}'_1) \cap B_1(\boldsymbol{c}'_2) \cap B_1(\boldsymbol{c}'_3) = \{(1,0,0),(0,\alpha+1,0),(\alpha,\alpha,0)\}$. We remark that this is similar to the problem of the intersection of three balls with Hamming radii discussed in [26, p. 58], provided that the underlying field is not GF(2).

V. Covering Properties of Rank Metric Codes

A. The Sphere Covering Problem

We denote the *minimum* cardinality of a code of length n and rank covering radius ρ as $K_{\mathrm{R}}(q^m,n,\rho)$. We remark that if C is a code over GF(q^m) with length n and covering radius ρ, then its transpose code C^T is a code over GF(q^n) with length m and the same covering radius. Therefore, $K_{\mathrm{R}}(q^m,n,\rho) = K_{\mathrm{R}}(q^n,m,\rho)$, and without loss of generality, we will assume $n \leq m$ henceforth in this section. Also note that $K_{\mathrm{R}}(q^m,n,0) = q^{mn}$ and $K_{\mathrm{R}}(q^m,n,n) = 1$ for all m and n. Hence, we assume $0 < \rho < n$ throughout this section. Two bounds on $K_{\mathrm{R}}(q^m,n,\rho)$ can be easily derived.

Proposition 6: For $0 < \rho < n \leq m$, $\frac{q^{mn}}{v(\rho)} < K_{\mathrm{R}}(q^m,n,\rho) \leq q^{m(n-\rho)}$.

Proof: The lower bound is a straightforward generalization of the bound given in [13]. Note that only the codes with cardinality $\frac{q^{mn}}{v(\rho)}$ are perfect codes. However, there are no nontrivial perfect codes for the rank metric [11]. Therefore, $K_{\mathrm{R}}(q^m,n,\rho) > \frac{q^{mn}}{v(\rho)}$.

Let $\mathcal{C}$ be an (n,k) linear code over GF(q^m) and without loss of generality assume $(\boldsymbol{I}_k \,|\, \boldsymbol{R})$ is its generator matrix. For any $\boldsymbol{x} = (x_0,x_1,\ldots,x_{n-1}) \in \mathrm{GF}(q^m)^n$, there exists $\boldsymbol{c} = (x_0,x_1,\ldots,x_{k-1},c_k,\ldots,c_{n-1}) \in \mathcal{C}$ such that $\mathrm{rk}(\boldsymbol{c}-\boldsymbol{x}) \leq n-k$, and hence, the covering radius ρ of $\mathcal{C}$ satisfies $\rho \leq n-k$. That is, $|\mathcal{C}| \leq q^{m(n-\rho)}$. By definition, $K_{\mathrm{R}}(q^m,n,\rho) \leq |\mathcal{C}|$, which leads to the upper bound. □

We refer to the lower bound in Proposition 6 as the sphere covering bound.

For a code over GF(q^m) with length n and covering radius $0 < \rho < n$, we have $K_{\mathrm{R}}(q^m,n,\rho) \leq K_{\mathrm{H}}(q^m,n,\rho)$, where $K_{\mathrm{H}}(q^m,n,\rho)$ is the minimum cardinality of a (linear or nonlinear) code over GF(q^m) with length n and Hamming covering radius ρ. This holds because any code with Hamming covering radius ρ has rank covering radius $\leq \rho$. Because $K_{\mathrm{H}}(q^m,n,\rho) \leq q^{m(n-\rho)}$ [26], this provides a tighter bound than the one given in Proposition 6.

Proposition 7: For $0 < \rho < n \leq m, K_{\mathrm{R}}(q^m,n,\rho) \geq 3$.

Proof: Suppose there exists a code C of cardinality 2 and length n over GF(q^m) with covering radius $\rho < n$. Without loss of generality, we assume $C = \{\boldsymbol{0},\boldsymbol{c}\}$. Because $|B_\rho(\boldsymbol{0}) \cup B_\rho(\boldsymbol{c})|$ is a nondecreasing function of $\mathrm{rk}(\boldsymbol{c})$ by Corollary 1, we assume $\mathrm{rk}(\boldsymbol{c}) = n$. The code $\mathcal{G} = \langle \boldsymbol{c} \rangle$ is hence an $(n,1,n)$ linear MRD code over GF(q^m). Therefore, any codeword in $\mathcal{G} \backslash C$ is at distance n from C. Thus, $\rho = n$, which contradicts our assumption. □

Lemma 7: $K_{\mathrm{R}}(q^m,n+n',\rho+\rho') \leq K_{\mathrm{R}}(q^m,n,\rho) K_{\mathrm{R}}(q^m,n',\rho')$ for all $m > 0$ and nonnegative n,n',ρ, and ρ'. In particular, $K_{\mathrm{R}}(q^m,n+1,\rho+1) \leq K_{\mathrm{R}}(q^m,n,\rho)$ and $K_{\mathrm{R}}(q^m,n+1,\rho) \leq q^m K_{\mathrm{R}}(q^m,n,\rho)$.

Proof: For all $\boldsymbol{x},\boldsymbol{y} \in \mathrm{GF}(q^m)^n$ and $\boldsymbol{x}',\boldsymbol{y}' \in \mathrm{GF}(q^m)^{n'}$, we have $d_{\mathrm{R}}((\boldsymbol{x},\boldsymbol{x}'),(\boldsymbol{y},\boldsymbol{y}')) \leq d_{\mathrm{R}}(\boldsymbol{x},\boldsymbol{y}) + d_{\mathrm{R}}(\boldsymbol{y},\boldsymbol{y}')$. Therefore, for any $C \in \mathrm{GF}(q^m)^n, C' \in \mathrm{GF}(q^m)^{n'}$, we have $\rho(C \oplus C') \leq \rho(C) + \rho(C')$ and the first claim follows. In particular, $(n',\rho') = (1,1)$ and $(n',\rho') = (1,0)$ yield the other two claims, respectively. □

B. Lower Bounds for the Sphere Covering Problem

We now derive two nontrivial lower bounds on $K_{\mathrm{R}}(q^m,n,\rho)$. For $0 \leq d \leq n$, we denote the volume of the intersection of two balls in GF$(q^m)^n$ with rank radii ρ and a distance d between their respective centers d as $I(q^m,n,\rho,d)$. When there is no ambiguity about the vector space considered, we simply denote it as $I(\rho,d)$. $I(\rho,d)$ is well defined by Lemma 6, and obviously $I(\rho,d) = 0$ when $d > 2\rho$.

Proposition 8: For $0 < \rho < n \leq m$ and $0 \leq l \leq \lfloor \log_{q^m} K_{\mathrm{R}}(q^m,n,\rho) \rfloor$,

$$K_{\mathrm{R}}(q^m,n,\rho) \geq \frac{1}{v(\rho) - I(\rho,n-l)} \left[q^{mn} - q^{lm} I(\rho,n-l) + \sum_{a=\max\{1,n-2\rho+1\}}^{l} (q^{am} - q^{(a-1)m}) I(\rho,n-a+1) \right]. \quad (1)$$

Proof: Let us denote $\lfloor \log_{q^m} K_{\mathrm{R}}(q^m,n,\rho) \rfloor$ as λ for convenience. Let $C = \{\boldsymbol{c}_i\}_{i=0}^{K-1}$ be a code of length n and covering radius ρ over GF(q^m). We give below an upper bound on the number of vectors covered by C. Define $C_j \stackrel{\mathrm{def}}{=} \{\boldsymbol{c}_i\}_{i=0}^{j}$ for $0 \leq j \leq K-1$, where the codewords are labeled such that $d_{\mathrm{R}}(\boldsymbol{c}_j, C_{j-1})$ is nonincreasing for $j > 0$. For $1 \leq a \leq \lambda$ and $q^{m(a-1)} \leq j < q^{ma}$, we have $d_{\mathrm{R}}(\boldsymbol{c}_j, C_{j-1}) = \min_{1 \leq i \leq j} \{d_{\mathrm{R}}(\boldsymbol{c}_i, C_{i-1})\} = d_{\mathrm{R}}(C_j) \leq n-a+1$ by the Singleton bound. The codeword $\boldsymbol{c}_j$ hence covers at most $v(\rho) - I(\rho,n-a+1)$ vectors that are not previously covered by C_{j-1}. However, by definition, the number of vectors covered by C is q^{mn}. For $1 \leq l \leq \lambda$, the number of vectors covered by C thus satisfies

$$q^{mn} \leq v(\rho) + \sum_{a=1}^{l} (q^{am} - q^{(a-1)m})[v(\rho) - I(\rho,n-a+1)] + (K - q^{lm})[v(\rho) - I(\rho,n-l)]. \quad (2)$$

Because $I(\rho,n-a+1) = 0$ for $a \leq n-2\rho$, (2) reduces to (1). □

Note that the right-hand side (RHS) of (1) is a nondecreasing function of l, thus the bound is tightest when $l = \lfloor \log_{q^m} K_{\mathrm{R}}(q^m,n,\rho) \rfloor$. Although $K_{\mathrm{R}}(q^m,n,\rho)$ is unknown in general, this bound can be used iteratively: we start with any lower bound on $K_{\mathrm{R}}(q^m,n,\rho)$, and using the largest l, the RHS of (1) results in a new lower bound on $K_{\mathrm{R}}(q^m,n,\rho)$; we repeat this until (1) does not offer any improvement on the value of $\lfloor \log_{q^m} K_{\mathrm{R}}(q^m,n,\rho) \rfloor$. The initial condition could be either any *other* lower bound on $K_{\mathrm{R}}(q^m,n,\rho)$, or $l = 0$ (which actually is a refinement of the lower bound in Proposition 6).

Corollary 2: For $0 < \rho < n \leq m$,

$$K_{\mathrm{R}}(q^m,n,\rho) \geq \frac{q^{mn} - I(\rho,n)}{v(\rho) - I(\rho,n)}.$$

Proof: This is a special case of Proposition 8 for $l = 0$. □

Corollary 3: For all m, n, and $0 < \rho \leq \lfloor n/2 \rfloor$

$$K_{\mathrm{R}}(q^m, n, \rho) \geq \frac{q^{mn} - q^{m(n-2\rho)+\rho^2} \begin{bmatrix} 2\rho \\ \rho \end{bmatrix}}{v(\rho) - q^{\rho^2} \begin{bmatrix} 2\rho \\ \rho \end{bmatrix}}.$$

Proof: Because the balls of rank radius ρ around the codewords of an $(n, n-2\rho, 2\rho+1)$ MRD code do not intersect, $q^{mn} \geq V_\rho(q^m, n) q^{m(n-2\rho)}$. By the sphere covering bound, we obtain $K_{\mathrm{R}}(q^m, n, \rho) \geq q^{m(n-2\rho)}$, and hence, $\log_{q^m} K_{\mathrm{R}}(q^m, n, \rho) \geq n - 2\rho$. Use Proposition 8 for $l = n - 2\rho \geq 0$, and

$$I(\rho, 2\rho) = q^{\rho^2} \begin{bmatrix} 2\rho \\ \rho \end{bmatrix}$$

by Proposition 5. □

The bound in Corollary 3 can be viewed as the counterpart in the rank metric of the bound in [31, Theorem 1].

Van Wee [32], [33] 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. Although the concepts in [32] and [33] were developed for the Hamming metric, they are in fact independent of the underlying metric and we adapt them to the rank metric. For all $V \subseteq \mathrm{GF}(q^m)^n$ and a code C with covering radius ρ, the excess on V by C is defined to be $E_C(V) \stackrel{\mathrm{def}}{=} \sum_{\boldsymbol{c} \in C} |B_\rho(\boldsymbol{c}) \cap V| - |V|$. If $\{W_i\}$ is a family of disjoint subsets of $\mathrm{GF}(q^m)^n$, then $E_C(\bigcup_i W_i) = \sum_i E_C(W_i)$. We define $Z \stackrel{\mathrm{def}}{=} \{\boldsymbol{z} \in \mathrm{GF}(q^m)^n | E_C(\{\boldsymbol{z}\}) > 0\}$, i.e., Z is the set of vectors covered by at least two codewords in C. Note that $\boldsymbol{z} \in Z$ if and only if $|B_\rho(\boldsymbol{z}) \cap C| \geq 2$. It can be shown that $|Z| \leq E_C(Z) = E_C(\mathrm{GF}(q^m)^n) = |C| V_\rho(q^m, n) - q^{mn}$.

Before deriving the second nontrivial lower bound, we need the following adaptation of [33, Lemma 8]. Let C be a code with length n and rank covering radius ρ over $\mathrm{GF}(q^m)$. We define $A \stackrel{\mathrm{def}}{=} \{\boldsymbol{x} \in \mathrm{GF}(q^m)^n | d_{\mathrm{R}}(\boldsymbol{x}, C) = \rho\}$.

Lemma 8: For $\boldsymbol{x} \in A \backslash Z$ and $0 < \rho < n$, we have that $E_C(B_1(\boldsymbol{x})) \geq \epsilon$, where

$$\epsilon \stackrel{\mathrm{def}}{=} \left\lfloor \frac{(q^m - q^\rho)\left(\begin{bmatrix} n \\ 1 \end{bmatrix} - \begin{bmatrix} \rho \\ 1 \end{bmatrix} \right)}{q^\rho \begin{bmatrix} \rho+1 \\ 1 \end{bmatrix}} \right\rfloor q^\rho \begin{bmatrix} \rho+1 \\ 1 \end{bmatrix} + (q^m - q^\rho)\left(\begin{bmatrix} \rho \\ 1 \end{bmatrix} - \begin{bmatrix} n \\ 1 \end{bmatrix} \right).$$

Proof: Because $\boldsymbol{x} \notin Z$, there is a unique $\boldsymbol{c}_0 \in C$ such that $d_{\mathrm{R}}(\boldsymbol{x}, \boldsymbol{c}_0) = \rho$. By Proposition 5, we have $|B_\rho(\boldsymbol{c}_0) \cap B_1(\boldsymbol{x})| = 1 + (q^m - q^\rho) \begin{bmatrix} \rho \\ 1 \end{bmatrix} + (q^\rho - 1) \begin{bmatrix} n \\ 1 \end{bmatrix}$. For any codeword $\boldsymbol{c}_1 \in C$ satisfying $d_{\mathrm{R}}(\boldsymbol{x}, \boldsymbol{c}_1) = \rho + 1$, by Proposition 5, we have $|B_\rho(\boldsymbol{c}_1) \cap B_1(\boldsymbol{x})| = q^\rho \begin{bmatrix} \rho+1 \\ 1 \end{bmatrix}$. Finally, for all other codewords $\boldsymbol{c}_2 \in C$ at distance $> \rho + 1$ from $\boldsymbol{x}$, we have $|B_\rho(\boldsymbol{c}_2) \cap B_1(\boldsymbol{x})| = 0$. Denoting $N \stackrel{\mathrm{def}}{=} |\{\boldsymbol{c}_1 \in C | d_{\mathrm{R}}(\boldsymbol{x}, \boldsymbol{c}_1) = \rho + 1\}|$, we obtain

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

The proof is completed by realizing that

$$(q^m - q^\rho) \left(\begin{bmatrix} \rho \\ 1 \end{bmatrix} - \begin{bmatrix} n \\ 1 \end{bmatrix} \right) < 0$$

while $E_C(B_1(\boldsymbol{x}))$ is a nonnegative integer. □

For $\rho = n - 1$, Lemma 8 is improved to the following.

Corollary 4: For $\boldsymbol{x} \in A \backslash Z$ and $\rho = n - 1$, $E_C(B_1(\boldsymbol{x})) = \phi$, where

$$\phi \stackrel{\mathrm{def}}{=} q^{n-1} \begin{bmatrix} n \\ 1 \end{bmatrix} |C| - q^{n-1} \left(q^m + \begin{bmatrix} n-1 \\ 1 \end{bmatrix} \right).$$

Proof: The proof calls the same arguments as the proof above, with $N = |C| - 1$ for $\rho = n - 1$. □

Proposition 9: If $\epsilon > 0$, then $K_{\mathrm{R}}(q^m, n, \rho) \geq \frac{q^{mn}}{v(\rho) - \frac{\epsilon}{\delta} N_\rho(q^m, n)}$, where $\delta \stackrel{\mathrm{def}}{=} v(1) - q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix} - 1 + 2\epsilon$.

The Proof of Proposition 9, provided in part A of the Appendix, uses the approach in the proof of [33, Theorem 6] and is based on the concept of excess. The lower bounds in Propositions 8 and 9, when applicable, are at least as tight as the sphere covering bound. For $\rho = n - 1$, Proposition 9 is refined into the following.

Corollary 5: Let us denote the coefficients

$$q^{n-1} \begin{bmatrix} n \\ 1 \end{bmatrix} \quad \text{and} \quad q^{n-1} \left(q^m + \begin{bmatrix} n-1 \\ 1 \end{bmatrix} \right)$$

as α and β, respectively. $K_{\mathrm{R}}(q^m, n, n-1)$ satisfies $a K_{\mathrm{R}}(q^m, n, n-1)^2 - b K_{\mathrm{R}}(q^m, n, n-1) + c \geq 0$, where

$$\begin{aligned} a &\stackrel{\mathrm{def}}{=} \alpha[v(n-1) + v(n-2)] \\ b &\stackrel{\mathrm{def}}{=} v(n-1) \left\{ q^{n-2} \begin{bmatrix} n-1 \\ 1 \end{bmatrix} - v(1) + \beta + 1 \right\} \\ &\quad + 2\alpha q^{mn} + \beta v(n-2) \end{aligned}$$

and

$$c \stackrel{\mathrm{def}}{=} q^{mn} \left\{ 2\beta + 1 + q^{n-2} \begin{bmatrix} n-1 \\ 1 \end{bmatrix} - v(1) \right\}.$$

The Proof of Corollary 5 is given in part B of the Appendix.

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 ELSs.

Lemma 9: Let $\mathcal{C}$ be an (n,k) linear code over $\mathrm{GF}(q^m)$ ($n \leq m$). $\mathcal{C}$ is an MRD code if and only if $\mathcal{C} \oplus \mathcal{V} = \mathrm{GF}(q^m)^n$ for all $\mathcal{V} \in E_{n-k}(q^m, n)$.

Proof: Suppose $\mathcal{C}$ is an $(n, k, n-k+1)$ linear MRD code. It is clear that $\mathcal{C} \cap \mathcal{V} = \{\mathbf{0}\}$, and hence, $\mathcal{C} \oplus \mathcal{V} = \mathrm{GF}(q^m)^n$ for all $\mathcal{V} \in E_{n-k}(q^m, n)$. Conversely, suppose $\mathcal{C} \oplus \mathcal{V} = \mathrm{GF}(q^m)^n$ 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 $\alpha_0 = 1, \alpha_1, \ldots, \alpha_{m+u-1} \in \mathrm{GF}(q^{m+u})$ be a basis set of $\mathrm{GF}(q^{m+u})$ over $\mathrm{GF}(q)$, and let $\beta_0 = 1, \beta_1, \ldots, \beta_{m-1}$ be a basis of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$. We define the *linear* mapping f between two vector spaces $\mathrm{GF}(q^m)$ and $\mathfrak{S}_m \stackrel{\mathrm{def}}{=} \mathfrak{S}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$ given by $f(\beta_i) = \alpha_i$ for $0 \leq i \leq m-1$. We remark that $\alpha_0 = \beta_0 = 1$ implies that f maps $\mathrm{GF}(q)$ to itself. This can be generalized to n-dimensional vectors, by applying f componentwise. We thus define $\bar{f} : \mathrm{GF}(q^m)^n \to \mathrm{GF}(q^{m+u})^n$ such that for any $\boldsymbol{v} = (v_0, \ldots, v_{n-1}), \bar{f}(\boldsymbol{v}) = (f(v_0), \ldots, f(v_{n-1}))$. Note that $\bar{f}$ depends on u, but we omit this dependence for simplicity of notation. This function $\bar{f}$ is a linear bijection from $\mathrm{GF}(q^m)^n$ to its image $\mathfrak{S}_m^n$, and hence, $\bar{f}$ preserves the rank. $\bar{f}$ also introduces a connection between ELSs as shown below.

Lemma 10: For $u \geq 1, r \leq n$, 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, $\bar{f}$ induces a bijection between $E_r(q^m, n)$ and $E_r(q^{m+u}, n)$.

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

Proposition 10: Let $\mathcal{C}$ be an $(n, n-\rho, \rho+1)$ MRD code over $\mathrm{GF}(q^m)$ ($n \leq m$) 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 $\mathrm{GF}(q^{m+u})$ 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 $\mathrm{GF}(q^{m+u})$ with dimension u such that $\mathfrak{S}_m \oplus \mathfrak{T}_u = \mathrm{GF}(q^{m+u})$. Any $\boldsymbol{u} \in \mathrm{GF}(q^{m+u})^n$ can be expressed as $\boldsymbol{u} = \boldsymbol{v} + \boldsymbol{w}$, where $\boldsymbol{v} \in \mathfrak{S}_m^n$ and $\boldsymbol{w} \in \mathfrak{T}_u^n$. Hence, $\mathrm{rk}(\boldsymbol{w}) \leq u$, and $\boldsymbol{w} \in \mathcal{W}$ for some $\mathcal{W} \in E_\rho(q^{m+u}, n)$ by Lemma 1. By Lemmas 9 and 10, we can express $\boldsymbol{v}$ as $\boldsymbol{v} = \bar{f}(\boldsymbol{c} + \boldsymbol{e}) = \bar{f}(\boldsymbol{c}) + \bar{f}(\boldsymbol{e})$, where $\boldsymbol{c} \in \mathcal{C}$ and $\boldsymbol{e} \in \mathcal{V}$, such that $\bar{f}(\mathcal{V}) \subset \mathcal{W}$. Eventually, we have $\boldsymbol{u} = \bar{f}(\boldsymbol{c}) + \bar{f}(\boldsymbol{e}) + \boldsymbol{w}$, where $\bar{f}(\boldsymbol{e}) + \boldsymbol{w} \in \mathcal{W}$, and thus, $d(\boldsymbol{u}, \bar{f}(\boldsymbol{c})) \leq \rho$. 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 6: For $0 < \rho < n \leq m$, $K_{\mathrm{R}}(q^m, n, \rho) \leq q^{\max\{m-\rho, n\}(n-\rho)}$.

Proof: We can construct an $(n, n-\rho)$ linear MRD code $\mathcal{C}$ over $\mathrm{GF}(q^\mu)$ with covering radius ρ, where $\mu = \max\{m-\rho, n\}$. By Proposition 10, $\hat{f}(\mathcal{C}) \subset \mathrm{GF}(q^m)^n$, where $\hat{f}$ is a rank-preserving mapping from $\mathrm{GF}(q^\mu)^n$ to a subset of $\mathrm{GF}(q^m)^n$ similar to $\bar{f}$ above, has covering radius $\leq \rho$. Thus, $K_{\mathrm{R}}(q^m, n, \rho) \leq |\hat{f}(\mathcal{C})| = |\mathcal{C}| = q^{\mu(n-\rho)}$. □

We use the properties of $K_{\mathrm{R}}(q^m, n, \rho)$ in Lemma 7 to obtain a tighter upper bound when $\rho > m - n$.

Proposition 11: Given fixed m, n, and ρ, for any $0 < l \leq n$ 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

$$K_{\mathrm{R}}(q^m, n, \rho) \leq \min_{\{(n_i, \rho_i): 0 \leq i \leq l-1\}} \left\{ q^{m(n-\rho) - \sum_i \rho_i (n_i - \rho_i)} \right\}. \tag{3}$$

Proof: By Lemma 7, we have $K_{\mathrm{R}}(q^m, n, \rho) \leq \prod_i K_{\mathrm{R}}(q^m, n_i, \rho_i)$ for all possible sequences $\{\rho_i\}$ and $\{n_i\}$. For all i, we have $K_{\mathrm{R}}(q^m, n_i, \rho_i) \leq q^{(m-\rho_i)(n-\rho_i)}$ by Corollary 6, and hence, $K_{\mathrm{R}}(q^m, n, \rho) \leq q^{\sum_i (m-\rho_i)(n_i-\rho_i)} = q^{m(n-\rho) - \sum_i \rho_i (n_i - \rho_i)}$. □

It is clear that the upper bound in (3) is tighter than the upper bound in Proposition 6. It can also be shown that it is tighter than the bound in Corollary 6.

The following upper bound is an adaptation of [26, Theorem 12.1.2].

Proposition 12: For $0 < \rho < n \leq m$

$$K_{\mathrm{R}}(q^m, n, \rho) \leq \frac{1}{1 - \log_{q^{mn}}(q^{mn} - v(\rho))} + 1.$$

Our proof, given in part C of the Appendix, adopts the approach used to prove [26, Theorem 12.1.2]. Refining [26, Theorem 12.2.1] for the rank metric, we obtain the following upper bound.

Proposition 13: For $0 < \rho < n \leq m$ and $a \stackrel{\mathrm{def}}{=} \min\{n, 2\rho\}$,

$$K_{\mathrm{R}}(q^m, n, \rho) \leq k_{v(\rho)} \left(\frac{1}{\min\{s, j\}} - \frac{1}{v(\rho)} \right) + \frac{q^{mn}}{v(\rho)} H_{\min\{s,j\}}, \tag{4}$$

where $k_{v(\rho)} = q^{mn} - v(\rho) q^{m(n-a)}$, $j = \lceil v(\rho) - v(\rho)^2 q^{-ma} \rceil$, $s = v(\rho) - \sum_{i=a-\rho}^{\rho} q^{i(a-i)} \begin{bmatrix} a \\ i \end{bmatrix}$, and $H_k \stackrel{\mathrm{def}}{=} \sum_{i=1}^{k} \frac{1}{i}$ is the kth harmonic number.

Proof: We denote the vectors of $\mathrm{GF}(q^m)^n$ as $\boldsymbol{v}_i$ for $i = 0, 1, \ldots, q^{mn} - 1$ and we consider a $q^{mn} \times q^{mn}$ square matrix $\boldsymbol{A}$ defined as $a_{i,j} = 1$ if $d_{\mathrm{R}}(\boldsymbol{v}_i, \boldsymbol{v}_j) \leq \rho$ and $a_{i,j} = 0$ otherwise. Note that each row and each column of $\boldsymbol{A}$ has exactly $v(\rho)$ ones. We present an algorithm that selects K columns of $\boldsymbol{A}$ with no all-zero rows. These columns thus represent a code with cardinality K and covering radius ρ.

Set $\boldsymbol{A}_{v(\rho)} = \boldsymbol{A}$ and $k_{v(\rho)+1} = q^{mn}$. For $i = v(\rho), v(\rho) - 1, \ldots, 1$, repeat the following step. First, select from $\boldsymbol{A}_i$ a maximal set of K_i columns of weight i with pairwise disjoint supports. Then, remove these columns and all the $iK_i = k_{i+1} - k_i$ rows incident to one of them, and denote the remaining $k_i \times (q^{mn} - K_{v(\rho)} - \cdots - K_i)$ matrix as $\boldsymbol{A}_{i-1}$. The set of all $K = K_{v(\rho)} + \cdots + K_1$ selected columns hence contains no all-zero rows and forms a covering code.

For $2\rho \le n$, we can select an $(n, n-2\rho, 2\rho+1)$ linear MRD code $\mathcal{C}$ for the first step. Because an MRD code is maximal, its codewords correspond to a maximal set of columns with disjoint supports. If $2\rho > n, \mathcal{C}$ is chosen to be a single codeword, and $K_{v(\rho)} = 1$. Thus, $K_{v(\rho)} = q^{m(n-a)}$ and $k_{v(\rho)} = q^{mn} - v(\rho)q^{m(n-a)}$, where $a = \min\{n, 2\rho\}$.

We now establish two upper bounds on k_i for $1 \le i \le v(\rho)$. First, it is obvious that $k_i \le k_{v(\rho)}$. Also, every row of $\boldsymbol{A}_{i-1}$ contains exactly $v(\rho)$ ones; on the other hand, every column of $\boldsymbol{A}_{i-1}$ contains at most $i-1$ ones. Hence, for $1 \le i \le v(\rho), v(\rho)k_i \le (i-1)(q^{mn} - K_{v(\rho)} - \cdots - K_i) \le (i-1)q^{mn}$, and thus

$$k_i \le (i-1)\frac{q^{mn}}{v(\rho)}. \tag{5}$$

Clearly, $k_1 = 0$ by (5). We have $k_{v(\rho)} \le (i-1)\frac{q^{mn}}{v(\rho)}$ if $i - 1 \ge j \stackrel{\text{def}}{=} \left\lceil \frac{v(\rho)k_{v(\rho)}}{q^{mn}} \right\rceil$.

We now establish an upper bound on $K = \sum_{i=1}^{v(\rho)} K_i$. For any vector $\boldsymbol{x} \in \mathrm{GF}(q^m)^n$, we have $d_{\mathrm{R}}(\boldsymbol{x}, \mathcal{C}) \le 2\rho$. This is trivial for $2\rho > n$, while for $2\rho \le n$, this is because MRD codes are maximal codes. For $2\rho \le n$, at least $q^{\rho^2} \begin{bmatrix} 2\rho \\ \rho \end{bmatrix}$ vectors in $B_\rho(\boldsymbol{x})$ are already covered by $\mathcal{C}$ by Proposition 5. For $2\rho > n$, it can be shown that at least $\sum_{i=n-\rho}^{\rho} q^{i(n-i)} \begin{bmatrix} n \\ i \end{bmatrix}$ vectors in $B_\rho(\boldsymbol{x})$ are already covered by $\mathcal{C}$. It follows that after the first step, the column weight is at most $s \stackrel{\text{def}}{=} v(\rho) - \sum_{i=a-\rho}^{\rho} q^{i(a-i)} \begin{bmatrix} a \\ i \end{bmatrix}$. Because $s \ge \max\{1 \le i < v(\rho) : K_i > 0\}, K = K_{v(\rho)} + \sum_{i=1}^{s} K_i = K_{v(\rho)} + \frac{k_{v(\rho)}}{s} + \sum_{i=2}^{s} \frac{k_i}{i(i-1)}$. Using the two upper bounds on k_i above, we obtain $K \le k_{v(\rho)} \left(\frac{1}{\min\{s,j\}} - \frac{1}{v(\rho)} \right) + \frac{q^{mn}}{v(\rho)} H_{\min\{s,j\}}$. □

Because [26, Theorem 12.1.2] is referred to as the Johnson–Stein–Lovász theorem, we refer to the algorithm described in the proof of Proposition 13 as the Johnson–Stein–Lovász (JSL) algorithm. The upper bound in Proposition 13 can be loosened into the following.

Corollary 7: For $0 < \rho < n \le m, K_{\mathrm{R}}(q^m, n, \rho) \le \frac{q^{mn}}{v(\rho)} \left(\ln v(\rho) + \gamma + \frac{1}{2v(\rho)+1/3} \right)$, where γ is the Euler–Mascheroni constant [34].

Proof: Using (5), we obtain $K = \sum_{i=1}^{v(\rho)} \frac{k_{i+1}-k_i}{i} \le \frac{q^{mn}}{v(\rho)} + \sum_{i=2}^{v(\rho)} \frac{k_i}{i(i-1)} \le \frac{q^{mn}}{v(\rho)} H_{v(\rho)}$. The proof is concluded by $H_{v(\rho)} < \ln v(\rho) + \gamma + \frac{1}{2v(\rho)+1/3}$ [34]. □

D. Covering Properties of Linear Rank Metric Codes

Proposition 6 yields bounds on the dimension of a linear code with a given rank covering radius.

Proposition 14: An (n, k) linear code over $\mathrm{GF}(q^m)$ with rank covering radius ρ satisfies $n - \rho - \frac{\rho(n-\rho) - \log_q K_q}{m} < k \le n - \rho$.

Proof: The upper bound was proved as part of the proof of Proposition 6. We now prove the lower bound. By the sphere covering bound, we have $q^{mk} > \frac{q^{mn}}{v(\rho)}$. However, by Lemma 5, we have $v(\rho) < q^{\rho(m+n-\rho) - \log_q K_q}$, and hence, $q^{mk} > q^{mn - \rho(m+n-\rho) + \log_q K_q}$. □

We do not adapt the bounds in Propositions 8 and 9 as their advantage over the lower bound in Proposition 14 is not significant. Next, we show that the dimension of a linear code with a given rank covering radius can be determined under some conditions.

Proposition 15: Let $\mathcal{C}$ be an (n, k) linear code over $\mathrm{GF}(q^m) (n \le m)$ with rank covering radius ρ. Then, $k = n - \rho$ if $\rho \in \{0, 1, n-1, n\}$ or $\rho(n-\rho) \le m + \log_q K_q$, 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, because $k \le n - \rho$ by Proposition 14, it suffices to prove that $k \ge n - \rho$. First, suppose $\rho = 1$, then k satisfies $q^{mk} > \frac{q^{mn}}{v(1)}$ by the sphere covering bound. However, $v(1) < q^{m+n} \le q^{2m}$, and hence, $k > n - 2$. Second, if $\rho(n-\rho) \le m + \log_q K_q$, then $0 < \frac{1}{m}(\rho(n-\rho) - \log_q K_q) \le 1$ and $k \ge n - \rho$ by Proposition 14. 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 $\rho \ge d_{\mathrm{R}}(\mathcal{C}') = n - k$, as noted in Section II-B, and hence, $k \ge n - \rho$. The case $k = n$ is straightforward. Finally, if $\mathcal{C}$ is an ELS of dimension k, then for all $\boldsymbol{x}$ with rank n and for any $\boldsymbol{c} \in \mathcal{C}, d_{\mathrm{R}}(\boldsymbol{x}, \boldsymbol{c}) \ge \mathrm{rk}(\boldsymbol{x}) - \mathrm{rk}(\boldsymbol{c}) \ge n - k$. □

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

Corollary 8: Let $\mathcal{G}$ be an (n, k, d_{R}) generalized Gabidulin code $(n \le m)$, and let $\mathcal{G}^l$ be the code obtained by l Cartesian products of $\mathcal{G}$ for $l \ge 1$. Then, the rank covering radius of $\mathcal{G}^l$ satisfies $\rho(\mathcal{G}^l) \ge d_{\mathrm{R}} - 1$.

Note that when $n = m, \mathcal{G}^l$ is a maximal code, and hence, Corollary 8 can be further strengthened.

Corollary 9: Let $\mathcal{G}$ be an (m, k, d_{R}) generalized Gabidulin code over $\mathrm{GF}(q^m)$, and let $\mathcal{G}^l$ be the code obtained by l Cartesian products of $\mathcal{G}$. Then, $\rho(\mathcal{G}^l) = d_{\mathrm{R}} - 1$.

E. Numerical Methods

In addition to the above bounds, we use several different numerical methods to obtain tighter upper bounds for relatively small values of m, n, and ρ. First, the JSL algorithm described in the proof of Proposition 13 is implemented for small parameter values. Second, local search algorithms [26] similar to the ones available for Hamming metric codes are somewhat less complex than the JSL algorithm. Although the complexity for large parameter values is prohibitive, it is feasible. Third, we construct linear codes with good covering properties, because linear codes have lower complexity.

We can finally verify if a covering radius is achievable by a given code size by brute force verification, thereby establishing lower bounds on $K_{\mathrm{R}}(q^m, n, \rho)$. Obviously, this is practical for only small parameter values.

F. Tables

In Table I, we provide bounds on $K_{\mathrm{R}}(2^m, n, \rho)$, for $2 \le m \le 7, 2 \le n \le m$, and $1 \le \rho \le 6$. Obviously, $K_{\mathrm{R}}(q^m, n, \rho) = 1$ when $\rho = n$. For other sets of parameters, the tightest lower

TABLE I
BOUNDS ON $K_{\mathrm{R}}(2^m, n, \rho)$, FOR $2 \leq m \leq 7, 2 \leq n \leq m$, AND $1 \leq \rho \leq 6$

m	n	$\rho=1$	$\rho=2$	$\rho=3$	$\rho=4$	$\rho=5$	$\rho=6$
2	2	e 3 F	1				
3	2	e 4 B	1				
	3	e 11-16 F	g 4 C	1			
4	2	e 7-8 B	1				
	3	e 40-64 B	d 4-7 F	1			
	4	f 293-722 F	e 10-48 G	b 3-7 F	1		
5	2	e 12-16 B	1				
	3	e 154-256 B	d 6-8 B	1			
	4	e 2267-4096 B	e 33-256 C	d 4-8 C	1		
	5	e 34894-2^{17} C	e 233-2881 E	a 9-32 H	b 3-8 C	1	
6	2	e 23-32 B	1				
	3	e 601-1024 B	d 11-16 B	1			
	4	e 17822-2^{15} B	c 124-256 B	d 6-16 C	1		
	5	e 550395-2^{20} B	e 1770-2^{14} C	f 31-256 C	a 3-16 C	1	
	6	f 17318410-2^{26} C	f 27065-413582 E	f 214-4211 E	f 9-181 D	b 3-16 C	1
7	2	e 44-64 B	1				
	3	e 2372-4096 B	d 20-32 B	1			
	4	e 141231-2^{18} B	f 484-1024 B	a 9-16 B	1		
	5	e 8735289-2^{24} B	e 13835-2^{15} B	a 111-1024 C	a 5-16 C	1	
	6	e 549829402-2^{30} B	f 42229-2^{22} C	e 1584-2^{15} C	f 29-734 E	a 3-16 C	1
	7	e 34901004402-2^{37} C	f 13205450-239280759 E	e 23978-586397 E	f 203-5806 E	a 8-242 D	b 3-16 C

and upper bounds on $K_{\mathrm{R}}(q^m, n, \rho)$ are given, and letters associated with the numbers are used to indicate the tightest bound. The lower case letters "a"–"f" correspond to the lower bounds in Propositions 6–8, Corollaries 2 and 3, and Proposition 9, respectively. The lower case letter "g" corresponds to lower bounds obtained by brute force verification. The upper case letters "A"–"E" denote the upper bounds in Proposition 6, Corollary 6, and Propositions 11–13, respectively. The upper case letters "F"–"H" correspond to upper bounds obtained by the JSL algorithm, local search algorithm, and explicit linear constructions, respectively.

In Table II, we provide bounds on the minimum dimension k for $q = 2, 4 \leq m \leq 8, 4 \leq n \leq m$, and $2 \leq \rho \leq 6$. The unmarked entries correspond to Proposition 15. The lower case letters "a" and "e" correspond to the lower bound in Proposition 14 and the adaptation of Corollary 3 to linear codes, respectively. The lower case letter "h" corresponds to lower bounds obtained by brute force verification for linear codes. The upper case letter "A" corresponds to the upper bound in Proposition 14. The upper case letter "H" corresponds to upper bounds obtained by explicit linear constructions.

Although no analytical expression for $I(\rho, d)$ is known to us, it can be obtained by simple counting for the bounds in Proposition 8 or Corollary 3. In part D of the Appendix, we present the values of $I(q^m, n, \rho, d)$ used in calculating the values of the bounds in Proposition 8 and Corollary 2 displayed in Table I. We also present the codes, obtained by the numerical methods in Section V-E, that achieve the tightest upper bounds in Tables I and II.

G. 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 III, we consider the case where $\lim_{n\to\infty} \frac{n}{m} = b$, where b is a constant. In other words, these asymptotic covering properties provide insights

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

m	n	$\rho=2$	$\rho=3$	$\rho=4$	$\rho=5$	$\rho=6$
4	4	h 2 A	1	0		
5	4	e 2 A	1	0		
	5	a 2-3 A	a 1 H	1	0	
6	4	2	1	0		
	5	a 2-3 A	a 1-2 A	1	0	
	6	a 3-4 A	a 2-3 A	a 1-2 A	1	0
7	4	2	1	0		
	5	a 2-3 A	a 1-2 A	1	0	
	6	a 3-4 A	a 2-3 A	a 1-2 A	1	0
	7	a 4-5 A	a 3-4 A	a 2-3 A	a 1-2 A	1
8	4	2	1	0		
	5	3	2	1	0	
	6	a 3-4 A	a 2-3 A	a 1-2 A	1	0
	7	a 4-5 A	a 3-4 A	a 2-3 A	a 1-2 A	1
	8	a 5-6 A	a 3-5 A	a 2-4 A	a 1-3 A	a 1-2 A

on the covering properties of long rank metric codes over large fields.

The asymptotic form of the bounds in Lemma 5 is given in the lemma below.

Lemma 11: For $0 \leq \delta \leq \min\{1, b^{-1}\}$, $\lim_{n\to\infty}[\log_{q^{mn}} V_{\lfloor \delta n \rfloor}(q^m, n)] = \delta(1 + b - b\delta)$.

Proof: By Lemma 5, we have $q^{d_{\mathrm{R}}(m+n-d_{\mathrm{R}})} \leq v(d_{\mathrm{R}}) < K_q^{-1} q^{d_{\mathrm{R}}(m+n-d_{\mathrm{R}})}$. Taking the logarithm, this becomes $\delta(1 + b - b\delta) \leq \log_{q^{mn}} v(\lfloor \delta n \rfloor) < \delta(1 + b - b\delta) - \frac{\log_q K_q}{mn}$. The proof is concluded by taking the limit when n tends to infinity. □

Define $r \stackrel{\text{def}}{=} \frac{\rho}{n}$ and $k(r) = \lim_{n\to\infty} \inf[\log_{q^{mn}} K_{\mathrm{R}}(q^m, n, \rho)]$. The bounds in Proposition 6 and Corollary 7 together solve the asymptotic sphere covering problem.

Theorem I: For all b and r, $k(r) = (1 - r)(1 - br)$.

Proof: By Lemma 11, the sphere covering bound asymptotically becomes $k(r) \geq (1 - r)(1 - br)$. Also, by Corollary 7, $K_{\mathrm{R}}(q^m, n, \rho) \leq \frac{q^{mn}}{v(\rho)}[1 + \ln v(\rho)] \leq \frac{q^{mn}}{v(\rho)}[1 + mn \ln q]$, and hence, $\log_{q^{mn}} K_{\mathrm{R}}(q^m, n, \rho) \leq$

$\log_{q^{mn}} \frac{q^{mn}}{v(\rho)} + O((mn)^{-1} \ln mn)$. By Lemma 11, this asymptotically becomes $k(r) \leq (1-r)(1-br)$. Note that although we assume $n \leq m$ above for convenience, both bounds in Proposition 6 and Corollary 7 hold for any values of m and n. □

APPENDIX

A. Proof of Proposition 9

We first establish a key lemma.

Lemma 12: If $\boldsymbol{z} \in Z$ and $0 < \rho < n$, then $|A \cap B_1(\boldsymbol{z})| \leq v(1) - q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix}$.

Proof: By definition of ρ, there exists $\boldsymbol{c} \in C$ such that $d_{\mathrm{R}}(\boldsymbol{z}, \boldsymbol{c}) \leq \rho$. By Proposition 3, $|B_1(\boldsymbol{z}) \cap B_{\rho-1}(\boldsymbol{c})|$ gets its minimal value for $d_{\mathrm{R}}(\boldsymbol{z}, \boldsymbol{c}) = \rho$, which is $q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix}$ by Proposition 5. A vector at distance $\leq \rho - 1$ from any codeword does not belong to A. Therefore, $B_1(\boldsymbol{z}) \cap B_{\rho-1}(\boldsymbol{c}) \subseteq B_1(\boldsymbol{z}) \backslash A$, and hence, $|A \cap B_1(\boldsymbol{z})| = |B_1(\boldsymbol{z})| - |B_1(\boldsymbol{z}) \backslash A| \leq v(1) - |B_1(\boldsymbol{z}) \cap B_{\rho-1}(\boldsymbol{c})|$. □

We now give a Proof of Proposition 9.

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

$$\begin{aligned} \gamma &\stackrel{\text{def}}{=} \epsilon[q^{mn} - |C|v(\rho-1)] - (\epsilon-1)[|C|v(\rho) - q^{mn}] \quad (6) \\ &\leq \epsilon|A| - (\epsilon-1)|Z| \\ &\leq \epsilon|A| - (\epsilon-1)|A \cap Z| = \epsilon|A \backslash Z| + |A \cap Z| \quad (7) \end{aligned}$$

where (7) follows from $|Z| \leq |C|v(\rho) - q^{mn}$, given in Section V-B

$$\begin{aligned} \gamma &\leq \sum_{\boldsymbol{a} \in A \backslash Z} E_C(B_1(\boldsymbol{a})) + \sum_{\boldsymbol{a} \in A \cap Z} E_C(B_1(\boldsymbol{a})) \\ &= \sum_{\boldsymbol{a} \in A} E_C(B_1(\boldsymbol{a})) \quad (8) \end{aligned}$$

where (8) follows from Lemma 8 and $|A \cap Z| \leq E_C(A \cap Z)$.

$$\begin{aligned} \gamma &\leq \sum_{\boldsymbol{a} \in A} \sum_{\boldsymbol{x} \in B_1(\boldsymbol{a}) \cap Z} E_C(\{\boldsymbol{x}\}) \\ &= \sum_{\boldsymbol{x} \in Z} \sum_{\boldsymbol{a} \in B_1(\boldsymbol{x}) \cap A} E_C(\{\boldsymbol{x}\}) \\ &= \sum_{\boldsymbol{x} \in Z} |A \cap B_1(\boldsymbol{x})| E_C(\{\boldsymbol{x}\}) \quad (9) \end{aligned}$$

where (9) follows the fact that the second summation is over disjoint sets $\{\boldsymbol{x}\}$. By Lemma 12, we obtain

$$\begin{aligned} \gamma &\leq \sum_{\boldsymbol{x} \in Z} \left(v(1) - q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix} \right) E_C(\{\boldsymbol{x}\}) \\ &= \left(v(1) - q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix} \right) E_C(Z) \\ &= \left(v(1) - q^{\rho-1} \begin{bmatrix} \rho \\ 1 \end{bmatrix} \right) (|C|v(\rho) - q^{mn}). \quad (10) \end{aligned}$$

Combining (10) and (6), we obtain the bound in Proposition 9. □

B. Proof of Corollary 5

For $\rho = n-1$, (10) becomes $\phi[q^{mn} - |C|v(n-2)] - (\phi - 1)[|C|v(n-1) - q^{mn}] \leq \left(v(1) - q^{n-2} \begin{bmatrix} n-1 \\ 1 \end{bmatrix} \right) (|C|v(n-1) - q^{mn})$. Substituting $\phi = \alpha|C| - \beta$ and rearranging, we obtain the quadratic inequality in Corollary 5.

C. Proof of Proposition 12

Given a radius ρ and a code C, denote the set of vectors in $\mathrm{GF}(q^m)^n$ at distance $>\rho$ from C as $P_\rho(C)$. 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 $\mathrm{GF}(q^m)$ of length n and cardinality K as S_K. Clearly, $|S_K| = \binom{Q}{K}$. The average value of $p_\rho(C)$ for all codes $C \in S_K$ is given by

$$\begin{aligned} \frac{1}{|S_K|} \sum_{C \in S_K} p_\rho(C) &= \frac{1}{|S_K|} Q^{-1} \sum_{C \in S_K} |P_\rho(C)| \\ &= \frac{1}{|S_K|} Q^{-1} \sum_{C \in S_K} \sum_{\boldsymbol{x} \in F | d_{\mathrm{R}}(\boldsymbol{x}, C) > \rho} 1 \\ &= \frac{1}{|S_K|} Q^{-1} \sum_{\boldsymbol{x} \in F} \sum_{C \in S_K | d_{\mathrm{R}}(\boldsymbol{x}, C) > \rho} 1 \\ &= \frac{1}{|S_K|} Q^{-1} \sum_{\boldsymbol{x} \in F} \binom{Q - v(\rho)}{K} \\ &= \binom{Q - v(\rho)}{K} \Big/ \binom{Q}{K}. \quad (11) \end{aligned}$$

Equation (11) comes from the fact that there are $\binom{Q-v(\rho)}{K}$ codes with cardinality K that do not cover $\boldsymbol{x}$. For all K, there exists a code $C' \in S_K$ for which $p_\rho(C')$ is no more than the average, that is

$$p_\rho(C') \leq \binom{Q}{K}^{-1} \binom{Q - v(\rho)}{K} \leq (1 - Q^{-1}v(\rho))^K.$$

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

D. Numerical Results

The values of $I(q^m, n, \rho, d)$, used in calculating the bounds in Proposition 8 or Corollary 2, obtained by counting are $I(2^4, 3, 2, 3) = 560$, $I(2^5, 3, 2, 3) = 1232$, $I(2^5, 4, 3, 4) = 31\,040$, $I(2^6, 3, 2, 3) = 2576$, $I(2^6, 4, 2, 3) = 2912$, $I(2^6, 4, 3, 4) = 756\,800$, and $I(2^7, 3, 2, 3) = 5264$.

We now present the codes, obtained by computer search, that achieve the tightest upper bounds in Tables I and II. The finite fields use the default generator polynomials from MATLAB [35]. First, the linear code used to show that $K_{\mathrm{R}}(2^5, 5, 3) \leq 32$ has a generator matrix given by $\boldsymbol{G} = (1, \alpha, \alpha^2, 0, 0)$, where α is a primitive element of $\mathrm{GF}(2^5)$. We use the *skip-vector* form [36] to represent the other codes obtained by computer search. The skip-vector form of a code $C = \{\boldsymbol{c}_i\}_{i=0}^{K-1}$ over $\mathrm{GF}(q^m)^n$ can be obtained as follows. First, each codeword $\boldsymbol{c}_i \in \mathrm{GF}(q^m)^n$ is represented by an integer x_i in $[0, q^{mn} - 1]$ according to the

lexicographical order. Second, the integers x_i are sorted in ascending order; the resulting integers are denoted as x'_i. Third, calculate y_i defined as $y_0 = x'_0$ and $y_i = x'_i - x'_{i-1} - 1$ for $1 \leq i \leq K-1$. Fourth, if $y_i = y_{i+1} = \ldots = y_{i+k-1}$, then we write y_i^k.

Below are the codes obtained by the JSL algorithm:

$\boldsymbol{K}_{\mathrm{R}}(2^2, 2, 1) = 3 \quad 0^3$
$\boldsymbol{K}_{\mathrm{R}}(\mathbf{2^{3,3,1}}) \leq \mathbf{16} \quad 5\ 25\ 66\ 21\ 51\ 9\ 20\ 5\ 85\ 21\ 2\ 25\ 49\ 9\ 84\ 5$
$\boldsymbol{K}_{\mathrm{R}}(\mathbf{2}^4, 3, 2) \leq \mathbf{7} \quad 135\ 689\ 34\ 420\ 477\ 522\ 759$
$\boldsymbol{K}_{\mathrm{R}}(\mathbf{2^{4,4,1}}) \leq 722.$

For brevity, the details of this code are omitted.[1] Below is the code obtained by a local search algorithm: $\boldsymbol{K}_{\mathrm{R}}(\mathbf{2^{4,4,2}}) \leq 48 \quad 1493\ 1124\ 265\ 285\ 1030\ 2524\ 1366\ 493\ 6079\ 968\ 2145\ 848\ 312\ 473\ 1307\ 712\ 1088\ 2274\ 1380\ 1114\ 1028\ 567\ 422\ 1462\ 699\ 203\ 180\ 4669\ 146\ 978\ 3933\ 1810\ 2083\ 345\ 354\ 659\ 1054\ 2314\ 1443\ 2660\ 2675\ 1512\ 756\ 1229\ 95\ 2144\ 1624\ 1148$

REFERENCES

[1] L. Hua, "A theorem on matrices over a field and its applications," *Chinese Math. Soc.*, vol. 1, no. 2, pp. 109–163, 1951.

[2] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *J. Combinat. Theory A*, vol. 25, pp. 226–241, 1978.

[3] P. Lusina, E. M. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2757–2760, Oct. 2003.

[4] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a noncommutative ring and their application in cryptology," in *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1991, vol. 573, pp. 482–489.

[5] E. M. Gabidulin, "Optimal codes correcting lattice-pattern errors," *Probl. Inf. Transm.*, vol. 21, no. 2, pp. 3–11, 1985.

[6] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 328–336, Mar. 1991.

[7] D. Silva, F. R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory* [Online]. Available: http://arxiv.org/abs/0711.0708, submitted for publication

[8] M. Gadouleau and Z. Yan, "Constant-rank codes," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, ON, Canada, Jul. 2008, pp. 876–880.

[9] M. Gadouleau and Z. Yan, "Constant-rank codes and their connection to constant-dimension codes," in *Proc. 1st IEEE Int. Workshop Wireless Network Coding*, Jun. 2008, pp. 32–37.

[10] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inf. Transm.*, vol. 21, no. 1, pp. 1–12, Jan. 1985.

[11] N. Suresh-Babu, "Studies on rank distance codes," Ph.D. dissertation, IIT Madras, Madras, India, Feb. 1995.

[12] K. Chen, "On the nonexistence of perfect codes with rank distance," *Mathematische Nachrichten*, vol. 182, pp. 89–98, 1996.

[1]They are available at http://arxiv.org/PS_cache/cs/pdf/0701/0701098v4.pdf

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

[14] W. B. Vasantha and R. J. Selvaraj, "Multi-covering radii of codes with rank metric," in *Proc. IEEE Inf. Theory Workshop*, Oct. 2002, pp. 215–.

[15] G. Richter and S. Plass, "Fast decoding of rank-codes with rank errors and column erasures," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2004, pp. 398–.

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

[17] E. M. Gabidulin and P. Loidreau, "On subcodes of codes in the rank metric," in *Proc. IEEE Int. Symp. Inf. Theory*, Sep. 2005, pp. 121–123.

[18] P. Loidreau, "A Welch-Berlekamp like algorithm for decoding Gabidulin codes," in *Proc. Int. Workshop Coding and Cryptography*, 2005, pp. 36–45.

[19] M. Gadouleau and Z. Yan, "Properties of codes with the rank metric," *Proc. IEEE Globecom*, pp. 1–5, Nov. 2006.

[20] M. Gadouleau and Z. Yan, "Decoder error probability of MRD codes," in *Proc. IEEE Int. Theory Workshop*, Oct. 2006, pp. 264–268 [Online]. Available: http://arxiv.org/abs/cs/0610148

[21] M. Gadouleau and Z. Yan, "On the decoder error probability of bounded rank-distance decoders for maximum rank distance codes," *IEEE Trans. Inf. Theory* [Online]. Available: http://arxiv.org/pdf/cs.IT/0612051, to be published

[22] P. Loidreau, "Properties of codes in rank metric," [Online]. Available: http://arxiv.org/pdf/cs.DM/0610057

[23] P. Delsarte, "Four fundamental parameters of a code and their combinatorial significance," *Inf. Control*, vol. 23, pp. 407–438, 1973.

[24] T. Berger, *Rate Distortion Theory: A Mathematical Basis for Data Compression*, ser. Information and System Sciences, T. Kailath, Ed. Englewood Cliffs, NJ: Prentice-Hall, 1971.

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

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

[27] P. Loidreau, "Ŕtude et Optimisation de Cryptosystèmes à Clé Publique Fondés sur la Théorie des Codes Correcteurs," Ph.D. dissertation, École Polytechnique, Paris, France, May 2001.

[28] G. E. Andrews, "The theory of partitions," in *Encyclopedia of Mathematics and its Applications*, G.-C. Rota, Ed. Reading, MA: Addison-Wesley, 1976, vol. 2.

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

[30] P. Delsarte and V. I. Levenshtein, "Association schemes and coding theory," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2477–2504, Oct. 1998.

[31] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, "Further results on the covering radius of codes," *IEEE Trans. Inf. Theory*, vol. IT-32, no. 5, pp. 680–694, Sep. 1986.

[32] G. van Wee, "Improved sphere bounds on the covering radius of codes," *IEEE Trans. Inf. Theory*, vol. IT-34, no. 2, pp. 237–245, Mar. 1988.

[33] G. van Wee, "Bounds on packings and coverings by spheres in q-ary and mixed Hamming spaces," *J. Combinat. Theory A*, vol. 57, pp. 116–129, 1991.

[34] C.-P. Chen and F. Qi, "The best bounds of harmonic sequence," Jun. 2003 [Online]. Available: http://arxiv:math.ca/0306233v1

[35] The MathWorks, Inc., "MATLAB communications toolbox function reference: gf," Natick, MA [Online]. Available: http://www.mathworks.com/access/helpdesk/help/toolbox/comm/ug/gf.html

[36] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant weight codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1334–1380, Nov. 1990.