Bounds on Polynomial-Time List Decoding of Rank Metric Codes

Antonia Wachter-Zeh
Institute of Communications Engineering, University of Ulm, Ulm, Germany
and Institut de Recherche Mathémathique de Rennes (IRMAR), Université de Rennes 1, Rennes, France
antonia.wachter@uni-ulm.de

***Abstract*—This contribution provides bounds on the list size of rank metric codes in order to understand whether polynomial-time list decoding is possible or not. First, an exponential upper bound is derived, which holds for any rank metric code of length n and minimum rank distance d. Second, a lower bound proves that there exists a rank metric code over $\mathbb{F}_{q^m}$ of length $n \leq m$ such that the list size is exponential in the length of the code for any radius greater than *half the minimum distance*. This implies that in rank metric there cannot exist a *polynomial* upper bound depending only on n and d as the Johnson bound for Hamming metric. These bounds reveal significant differences between codes in Hamming and rank metric.**

***Index Terms*—Rank Metric Codes, List Decoding**

I. Introduction

A *list decoding* algorithm returns the list of *all* codewords within distance at most τ from any given word. In Hamming metric, the *Johnson upper bound* [1]–[3] shows for *any* code in Hamming metric of length n and minimum Hamming distance d_H that the size of this list is polynomial in n when τ is less than the Johnson radius $\tau_J = n - \sqrt{n(n-d_H)}$. Although this fact has been known since the 1960s, a polynomial-time list decoding algorithm for *Reed–Solomon* (RS) codes up to the Johnson radius was found not earlier than 1999 by Guruswami and Sudan [4] as a generalization of the Sudan algorithm [5]. Further, in Hamming metric, it can be shown that there exists a code such that the list size becomes *exponential* in n beyond the Johnson radius [3], [6]. It is not known whether this bound also holds for RS codes.

A lower bound on the maximum list size, which is exponential in the length n of the code, rules out polynomial-time list decoding since already writing down the list has exponential complexity. On the other hand, a polynomial upper bound—as the Johnson bound for Hamming metric—shows that a polynomial-time list decoding algorithm might exist.

Codes in rank metric recently attract a lot of attention since they provide an almost optimal solution to error control in random linear network coding [7], [8]. Gabidulin codes can be seen as the rank metric equivalent to RS codes and were introduced by Delsarte [9], Gabidulin [10] and Roth [11]. So far, there is no polynomial-time list decoding algorithm (beyond half the minimum distance) for Gabidulin codes and it is not even known whether it can exist or not. Notice that there is some work investigating list decoding algorithms for special classes and subcodes of Gabidulin codes [12]–[14].

In [15], we derived a lower bound for list decoding of Gabidulin codes of length n and minimum rank distance d, which shows that the list size can be exponential in n when the radius is at least the Johnson radius $\tau_J = n - \sqrt{n(n-d)}$.

In this contribution, we investigate bounds on list decoding of (general) rank metric codes and derive two bounds on the maximum list size. Despite the numerous similarities to codes in Hamming metric, these bounds show a strongly different behavior of the list size. Our first bound is an *exponential upper bound* for any rank metric code and provides no conclusion about polynomial-time list decodability. Remarkably, the second bound shows that there exists a rank metric code over $\mathbb{F}_{q^m}$ of length $n \leq m$ such that the list size is *exponential* in the length n when the decoding radius is greater than *half the minimum distance*. For these codes, hence, no polynomial-time list decoding can exist. The derivations apply connections between constant-rank codes and constant-dimension codes by Gadouleau and Yan [16]. Moreover, our results show that purely as a function of the length n and the minimum rank distance d, there cannot exist a polynomial upper bound similar to the Johnson bound in Hamming metric.

This paper is organized as follows. Section II introduces notations, states the problem and recalls connections between constant-rank and constant-dimension codes. In Section III, we explain how list decoding in rank metric is connected to a constant-rank code and derive the two bounds. Finally, Section IV discusses the results and reveals the differences to Hamming metric. Some proofs are omitted due to space restrictions and can be found in the long version [17].

II. Preliminaries

A. Finite Field and Subspaces

Let q be a power of a prime, and denote by $\mathbb{F}_q$ the finite field of order q and by $\mathbb{F}_{q^m}$ its extension field of degree m. We use $\mathbb{F}_q^{s \times n}$ to denote the set of all $s \times n$ matrices over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}^n = \mathbb{F}_{q^m}^{1 \times n}$ for the set of all row vectors of length n over $\mathbb{F}_{q^m}$. Therefore, $\mathbb{F}_q^n$ denotes the vector space of dimension n over $\mathbb{F}_q$. A *Grassmannian* of dimension r is the set of all subspaces of $\mathbb{F}_q^n$ of dimension $r \leq n$ and denoted by $\mathcal{G}_q(n,r)$.

This work was supported by the German Research Council "Deutsche Forschungsgemeinschaft" (DFG) under Grant No. Bo867/21-2.

The cardinality of $\mathcal{G}_q(n,r)$ is given by the Gaussian binomial:

$$\left|\mathcal{G}_q(n,r)\right| = \begin{bmatrix} n \\ r \end{bmatrix} \overset{\text{def}}{=} \prod_{i=0}^{r-1} \frac{q^n - q^i}{q^r - q^i},$$

with the upper and lower bounds (see e.g. [7, Lemma 4])

$$q^{r(n-r)} \leq \begin{bmatrix} n \\ r \end{bmatrix} \leq 4q^{r(n-r)}. \tag{1}$$

For two subspaces $\mathcal{U}, \mathcal{V}$ in $\mathbb{F}_q^n$, we denote by $\mathcal{U}+\mathcal{V}$ the smallest subspace containing the union of $\mathcal{U}$ and $\mathcal{V}$. The *subspace distance* between $\mathcal{U}, \mathcal{V}$ in $\mathbb{F}_q^n$ is defined by

$$\begin{aligned} d_S(\mathcal{U},\mathcal{V}) &= \dim(\mathcal{U}+\mathcal{V}) - \dim(\mathcal{U}\cap\mathcal{V}) \\ &= 2\dim(\mathcal{U}+\mathcal{V}) - \dim(\mathcal{U}) - \dim(\mathcal{V}). \end{aligned}$$

It can be shown that the subspace distance is a metric [7].

A *subspace code* is a non-empty subset of subspaces of $\mathbb{F}_q^n$ and has minimum subspace distance d_S, when all subspaces in the code have subspace distance at least d_S. The codewords of a subspace code are therefore subspaces. A $\mathsf{CD}(n, d_S, r)$ code denotes a *constant-dimension code* of dimension r and minimum subspace distance d_S, i.e., it is a special subspace code and is a subset of $\mathcal{G}_q(n,r)$.

B. Rank Metric Codes

For a given basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, there exists a one-to-one mapping for each vector $\mathbf{x} \in \mathbb{F}_{q^m}^n$ on a matrix $\mathbf{X} \in \mathbb{F}_q^{m\times n}$. Let $\mathrm{rk}(\mathbf{x})$ denote the (usual) rank of $\mathbf{X}$ over $\mathbb{F}_q$ and let $\mathcal{R}_q(\mathbf{X})$, $\mathcal{C}_q(\mathbf{X})$ denote the row and column space of $\mathbf{X}$ in $\mathbb{F}_q^n$. Throughout this paper, we use the notation as vector (e.g. from $\mathbb{F}_{q^m}^n$) or matrix (e.g. from $\mathbb{F}_q^{m\times n}$) equivalently, whatever is more convenient.

The *minimum rank distance* d_R of a code C is defined by

$$d_R = \min\left\{ \mathrm{rk}(\mathbf{c}_1 - \mathbf{c}_2) \ : \ \mathbf{c}_1, \mathbf{c}_2 \in \mathsf{C}, \mathbf{c}_1 \neq \mathbf{c}_2 \right\}.$$

An $(n, M, d)_R$ code over $\mathbb{F}_{q^m}$ denotes a code (not necessarily linear) of cardinality M and minimum rank distance $d_R = d$. Its codewords are in $\mathbb{F}_{q^m}^n$ or equivalently represented as matrices in $\mathbb{F}_q^{m\times n}$. W.l.o.g. we assume in this paper that $n \leq m$. If this is not the case, we consider the transpose of all matrices such that $n \leq m$ holds. We call n the *length* of such a block code in rank metric over $\mathbb{F}_{q^m}$.

The cardinality M of an $(n, M, d)_R$ code with $n \leq m$ is limited by a *Singleton*-like upper bound (see [8], [10]):

$$M \leq q^{\min\{n(m-d+1), m(n-d+1)\}} = q^{m(n-d+1)}. \tag{2}$$

For linear codes of length $n \leq m$ and dimension k, this implies $d_R \leq n-k+1$. If the cardinality of a code fulfills (2) with equality, the code is called a *Maximum Rank Distance* (MRD) code. A linear MRD code over $\mathbb{F}_{q^m}$ of length $n \leq m$, dimension k and minimum rank distance $d_R = n-k+1$ is denoted by $\mathsf{MRD}[n,k]$ and has cardinality $M = q^{mk}$. Note that Gabidulin codes are MRD codes.

A special class of rank metric codes are *constant-rank codes*. Such a (not necessarily linear) $\mathsf{CR}(n,d,r)$ code over $\mathbb{F}_{q^m}$ has length $n \leq m$, consists of words in $\mathbb{F}_{q^m}^n$ or equivalently of matrices in $\mathbb{F}_q^{m\times n}$, has minimum rank distance d and each codeword has rank exactly r.

The maximum cardinalities of a constant-dimension and constant-rank code for fixed parameters will be denoted by $|\mathsf{CD}(n,d_S,r)|_{\max}$ and $|\mathsf{CR}(n,d_R,r)|_{\max}$.

Further, $\mathcal{B}_\tau(\mathbf{a})$ denotes a ball of radius τ in rank metric around a word $\mathbf{a} \in \mathbb{F}_{q^m}^n$ and $\mathcal{S}_\tau(\mathbf{a})$ denotes a sphere in rank metric of radius τ around the word $\mathbf{a}$. The cardinality of a sphere of radius τ is the number of $m \times n$ matrices in $\mathbb{F}_q$, which have rank distance *exactly* τ from a word $\mathbf{a}$ and the cardinality of a ball of radius τ is the number of $m\times n$ matrices in $\mathbb{F}_q$, which have rank distance *less than or equal to* τ.

C. Constant-Dimension and Constant-Rank Codes

In this subsection, we recall known connections between constant-dimension and constant-rank codes by Gadouleau and Yan [16] and generalize some of their results, since we will use them in the next sections for bounding the list size.

Proposition 1 (Maximum Cardinality, [16]) *For all q and $1 \leq \delta \leq r \leq n \leq m$, the* ***maximum*** *cardinality of a $\mathsf{CR}(n, d_R = \delta + r, r)$ constant-rank code over $\mathbb{F}_{q^m}$ is upper bounded by the maximum cardinality of a constant-dimension code as follows:*

$$|\mathsf{CR}(n, d_R = \delta + r, r)|_{\max} \leq |\mathsf{CD}(n, d_S = 2\delta, r)|_{\max}.$$

The following proposition shows explicitly how to construct constant-rank codes out of constant-dimension codes and is a generalization of [16, Proposition 3] to constant-dimension codes of arbitrary cardinalities.

Proposition 2 (Construction of a Constant-Rank Code) *Let M be a $\mathsf{CD}(m, d_{S,M}, r)$ and N be a $\mathsf{CD}(n, d_{S,N}, r)$ constant-dimension code with $r \leq \min\{n,m\}$ and cardinalities $|\mathsf{M}|$ and $|\mathsf{N}|$. Then, there exists a $\mathsf{CR}(n, d_R, r)$ constant-rank code C of cardinality $\min\{|\mathsf{M}|, |\mathsf{N}|\}$ with $\mathcal{C}_q(\mathsf{C}) \subseteq \mathsf{M}$ and $\mathcal{R}_q(\mathsf{C}) \subseteq \mathsf{N}$. Furthermore,*

$$d_R \geq \frac{1}{2}\, d_{S,M} + \frac{1}{2}\, d_{S,N},$$

D. Constant-Dimension Codes from Lifted MRD Codes

There are several contributions about constructions of constant-dimension codes and bounds on their cardinality, see e.g. [7], [8], [18]–[23]. For our application of constant-dimension codes, the cardinality does not have to be optimal. *Lifted MRD codes* (see [8]) are sufficient and are shown in the following.

Definition 1 (Lifting, [8]) *Let the mapping $\mathcal{I} : \mathbb{F}_q^{r\times(n-r)} \to \mathcal{G}_q(n,r)$ be given by $\mathbf{X} \mapsto \mathcal{I}(\mathbf{X}) = \mathcal{R}_q([\mathbf{I}_r \ \mathbf{X}])$, where $\mathbf{I}_r$ denotes the $r\times r$ identity matrix. The subspace $\mathcal{I}(\mathbf{X})$ is called* ***lifting*** *of the matrix $\mathbf{X}$.*

If we apply this map on all codewords of a block code C, then the constant-dimension code $\mathcal{I}(\mathsf{C})$ is called lifting of C.

The following two lemmas show lifted MRD codes for some explicit parameters.

Lemma 1 (Lifted MRD Code, Even Distance, [8]) *Let d be an even integer, let $\tau \geq d/2$ and $\tau \leq n-\tau$. Let a linear $\mathsf{MRD}[\tau, \tau-d/2+1]$ code C over $\mathbb{F}_{q^{n-\tau}}$ of length τ, minimum rank distance $d_R = d/2$ and cardinality M_R be given.*

Then, the lifting of the transposed codewords, i.e.,

$$\mathcal{I}(\mathsf{C}^T) \overset{\text{def}}{=} \left\{\mathcal{I}(\mathbf{C}^T) = \mathcal{R}_q([\mathbf{I}_\tau \ \mathbf{C}^T]) : \mathbf{C} \in \mathsf{C}\right\}$$

is a $\mathsf{CD}(n, d_S, \tau)$ constant-dimension code of cardinality $M_S = M_R = q^{(n-\tau)(\tau-d/2+1)}$, minimum subspace distance $d_S = d$ and lies in the Grassmannian $\mathcal{G}_q(n,\tau)$.

Lemma 2 (Lifted MRD Code, Odd Distance, [8]) *Let d be an odd integer and let $\tau \geq {}^{(d-1)}/_2 + 1$. Then,*

- *for $\tau \leq m-\tau$ and a linear $\mathsf{MRD}[\tau, \tau - {}^{(d-1)}/_2 + 1]$ code C over $\mathbb{F}_{q^{m-\tau}}$, the lifting $\mathcal{I}(\mathsf{C}^T)$ is a $\mathsf{CD}(m, d_S = d-1, \tau)$ constant-dimension code of cardinality $q^{(m-\tau)(\tau-{}^{(d-1)}/_2+1)}$,*
- *for $\tau \leq n-\tau$, $n \leq m$ and a linear $\mathsf{MRD}[\tau, \tau - {}^{(d+1)}/_2 + 1]$ code C over $\mathbb{F}_{q^{n-\tau}}$, the lifting $\mathcal{I}(\mathsf{C}^T)$ is a $\mathsf{CD}(n, d_S = d+1, \tau)$ constant-dimension code of cardinality $q^{(n-\tau)(\tau-{}^{(d+1)}/_2+1)} = q^{(n-\tau)(\tau-{}^{(d-1)}/_2)} < q^{(m-\tau)(\tau-{}^{(d-1)}/_2+1)}$.*

Lifted MRD codes are sufficient for our bounds, although there are constant-dimension codes of higher cardinality, e.g. [20].

E. Problem Statement

We analyze the question of *polynomial-time list decodability* of rank metric codes. Thus, we want to bound the maximum number of codewords in a ball of radius τ around a received word $\mathbf{r}$. This number will be called the maximum *list size* ℓ in the following. The worst-case complexity of a possible list decoding algorithm directly depends on ℓ.

Problem 1 (Maximum List Size) *Let C be an $(n, M, d)_R$ code over $\mathbb{F}_{q^m}$ of length $n \leq m$, cardinality M and minimum rank distance $d_R = d$. Let $\tau < d$. Find a lower and upper bound on the maximum number of codewords ℓ in a ball of rank radius τ around a word $\mathbf{r} = (r_0 \ r_1 \ \dots \ r_{n-1}) \in \mathbb{F}_{q^m}^n$. Hence, find a bound on*

$$\ell \overset{\text{def}}{=} \max_{\mathbf{r}\in\mathbb{F}_{q^m}^n} \left\{\left|\mathsf{C} \cap \mathcal{B}_\tau(\mathbf{r})\right|\right\}.$$

For an upper bound, we have to show that the bound holds for *any* received word $\mathbf{r}$, whereas for a lower bound it is sufficient to show that there exists (at least) one $\mathbf{r}$ for which this bound on the list size is valid. Further, we denote the list of all codewords of C in the ball of rank radius τ around a given word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ by:

$$\begin{aligned}\mathcal{L} &\overset{\text{def}}{=} \mathsf{C} \cap \mathcal{B}_\tau(\mathbf{r}) \\ &= \left\{\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_{|\mathcal{L}|} \ : \ \mathbf{c}_i \in \mathsf{C} \text{ and } \operatorname{rk}(\mathbf{r}-\mathbf{c}_i) \leq \tau, \ \forall i\right\},\end{aligned} \qquad (3)$$

with cardinality $|\mathcal{L}| \leq \ell$.

III. Bounds on the List Size of Rank Metric Codes

A. Connection between Constant-Rank Codes and the List Size

As in (3), denote the list of codewords when decoding up to $\tau < d$ errors with an $(n, M, d_R = d)_R$ code C by

$$\begin{aligned}\mathcal{L} = \left\{\mathbf{c}_1, c_2, \dots, \mathbf{c}_{|\mathcal{L}|}\right\} &= \mathsf{C} \cap \mathcal{B}_\tau(\mathbf{r}) \\ &= \sum_{i=0}^{\tau} \left(\mathsf{C} \cap \mathcal{S}_i(\mathbf{r})\right),\end{aligned}$$

for some received word $\mathbf{r} \in \mathbb{F}_{q^m}^n$. Consider only the codewords in rank distance *exactly* τ from the received word, i.e.:

$$\left\{\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_{\overline{\ell}}\right\} \overset{\text{def}}{=} \mathsf{C} \cap \mathcal{S}_\tau(\mathbf{r}).$$

Clearly, this gives a lower bound on the maximum list size: $\ell \geq \overline{\ell} = |\mathsf{C} \cap \mathcal{S}_\tau(\mathbf{r})|$. Now, consider a translate of all codewords of rank distance exactly τ as follows:

$$\overline{\mathcal{L}} \overset{\text{def}}{=} \left\{\mathbf{r}-\mathbf{c}_1, \mathbf{r}-\mathbf{c}_2, \dots, \mathbf{r}-\mathbf{c}_{\overline{\ell}}\right\}.$$

This set $\overline{\mathcal{L}}$ is a $\mathsf{CR}(n, d_R \geq d, \tau)$ constant-rank code since $\operatorname{rk}(\mathbf{r}-\mathbf{c}_i) = \tau$ for all $i = 1, \dots, \overline{\ell}$ and its minimum rank distance is at least d, since

$$\operatorname{rk}(\mathbf{r}-\mathbf{c}_i-\mathbf{r}+\mathbf{c}_j) = \operatorname{rk}(\mathbf{c}_i-\mathbf{c}_j) \geq d, \quad \forall i,j, \ i \neq j.$$

The cardinality of this constant-rank code is $\overline{\ell}$ and for $\tau < d$, it is non-linear, since the rank of its codewords is less than its minimum distance.

Hence, a translate of the list of all codewords in rank distance exactly τ from the received word can be interpreted as a constant-rank code, which makes it possible to use bounds on the cardinality of a constant-rank code to obtain bounds on the list size ℓ.

B. Upper Bound on the List Size

The upper bound presented in this subsection is an upper bound on the list size when decoding rank metric codes and holds for *any* code in rank metric and *any* received word.

Theorem 1 (Upper Bound on the List Size) *Let $\lfloor {}^{(d-1)}/_2 \rfloor < \tau < d \leq n \leq m$. Then, for **any** $(n, M, d)_R$ code over $\mathbb{F}_{q^m}$ in rank metric, the maximum list size is upper bounded as follows:*

$$\begin{aligned}\ell &\leq 1 + \sum_{t=\lfloor \frac{d-1}{2} \rfloor+1}^{\tau} \frac{\begin{bmatrix} n \\ 2t+1-d \end{bmatrix}}{\begin{bmatrix} t \\ 2t+1-d \end{bmatrix}} \\ &\leq 1 + 4 \sum_{t=\lfloor \frac{d-1}{2} \rfloor+1}^{\tau} q^{(2t-d+1)(n-t)}.\end{aligned}$$

Proof: Let $\{\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_{\overline{\ell}}\} = \mathsf{C} \cap \mathcal{S}_t(\mathbf{r})$ for some $(n, M, d)_R$ code C and $t \leq \tau$. As explained in Section III-A, for any $\mathbf{r} \in \mathbb{F}_{q^m}^n$

$$\overline{\mathcal{L}} = \{\mathbf{r}-\mathbf{c}_1, \mathbf{r}-\mathbf{c}_1 \dots, \mathbf{r}-\mathbf{c}_{\overline{\ell}}\}$$

can be seen as a $\mathsf{CR}(n, d_R \geq d, t)$ constant-rank code. Therefore, for any word $\mathbf{r} \in \mathbb{F}_{q^m}^n$, the cardinality of $\overline{\mathcal{L}}$ can be upper bounded by:

$$\begin{aligned}|\overline{\mathcal{L}}| = \big|\mathsf{C} \cap \mathcal{S}_t(\mathbf{r})\big| &\leq |\mathsf{CR}(n, d_R \geq d, t)|_{\max} \\ &\leq |\mathsf{CR}(n, d, t)|_{\max}.\end{aligned}$$

We can upper bound this maximum cardinality by Proposition 1 with $\delta = d - t$ and $r = t$ by:

$$|\mathsf{CR}(n, d, t)|_{\max} \leq |\mathsf{CD}(n, d_S = 2(d-t), t)|_{\max}.$$

For upper bounding this cardinality, we use the Wang–Xing–Safavi-Naini bound [18] and obtain:

$$|\mathsf{CD}(n, d_S = 2(d-t), t)|_{\max} \leq \frac{\begin{bmatrix} n \\ t-(d-t)+1 \end{bmatrix}}{\begin{bmatrix} t \\ t-(d-t)+1 \end{bmatrix}}. \tag{4}$$

In the ball of radius $\lfloor (d-1)/2 \rfloor$ around $\mathbf{r}$, there is at most one codeword of C and therefore the contribution to the list size is at most one. For higher t, we sum up (4) from $t = \lfloor (d-1)/2 \rfloor + 1$ up to τ and with (1), the statement follows. ■

Notice that this bound gives (almost) the same upper bound as we showed in [15, Theorem 2], which can slightly be improved if we use better upper bounds for constant-dimension codes instead of (4), for example the iterated Johnson bound for constant-dimension codes [19, Corollary 3]. However, the Wang–Xing–Safavi-Naini bound provides a nice closed-form expression and is asymptotically tight.

Unfortunately, our upper bound on the list size of rank metric codes is exponential in the length of the code. However, the lower bound of Section III-C will show that any upper bound depending only on the length $n \leq m$ and the minimum rank distance d has to be exponential in $(\tau - \lfloor (d-1)/2 \rfloor)(n-\tau)$, since there exists a rank metric code with such a list size.

C. Lower Bound on the List Size

In this subsection, we prove the most significant difference to codes in Hamming metric: We derive the existence of a rank metric code over $\mathbb{F}_{q^m}$ of length $n \leq m$ with exponential list size for any decoding radius *greater than half the minimum distance*. First, we prove the existence of a certain constant-rank code.

Theorem 2 (Constant-Rank Code) *Let $\lfloor (d-1)/2 \rfloor < \tau < d \leq n \leq m$ and $\tau \leq n - \tau$. Then, there exists a $\mathsf{CR}(n, d_R \geq d, \tau)$ constant-rank code over $\mathbb{F}_{q^m}$ of cardinality $q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}$.*

Proof: First, assume d is even. Let us construct a $\mathsf{CD}(m, d, \tau)$ constant-dimension code M and a $\mathsf{CD}(n, d, \tau)$ code N by lifting an $\mathsf{MRD}[\tau, \tau - d/2 + 1]$ code over $\mathbb{F}_{q^{m-\tau}}$ of minimum rank distance $d/2$ and an $\mathsf{MRD}[\tau, \tau - d/2 + 1]$ code over $\mathbb{F}_{q^{n-\tau}}$ of minimum rank distance $d/2$ as in Lemma 1. Then, with Lemma 1:

$$|\mathsf{N}| = q^{(n-\tau)(\tau - d/2 + 1)} \leq |\mathsf{M}| = q^{(m-\tau)(\tau - d/2 + 1)}.$$

From Proposition 2, we know therefore there exists a $\mathsf{CR}(n, d_R, \tau)$ code of cardinality

$$\min\{|\mathsf{N}|, |\mathsf{M}|\} = q^{(n-\tau)(\tau - d/2 + 1)} = q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}.$$

For its rank distance by Proposition 2, the following holds:

$$d_R \geq \frac{1}{2}\, d_{S,M} + \frac{1}{2}\, d_{S,N} = d.$$

Second, assume d is odd. Let M be a $\mathsf{CD}(m, d-1, \tau)$ code and N be a $\mathsf{CD}(n, d+1, \tau)$ code, constructed as in Lemma 2. Then,

$$|\mathsf{N}| = q^{(n-\tau)(\tau - (d+1)/2 + 1)} \leq |\mathsf{M}| = q^{(m-\tau)(\tau - (d-1)/2 + 1)}.$$

From Proposition 2, we know therefore there exists a $\mathsf{CR}(n, d_R, \tau)$ code of cardinality

$$\min\{|\mathsf{N}|, |\mathsf{M}|\} = q^{(n-\tau)(\tau - (d-1)/2)} = q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}.$$

With Proposition 2, the rank distance d_R is lower bounded by:

$$d_R \geq \frac{1}{2}\, d_{S,M} + \frac{1}{2}\, d_{S,N} = \frac{1}{2}\,(d-1) + \frac{1}{2}\,(d+1) = d.$$

■

This can now directly be used to show the existence of a rank metric code with exponential list size.

Theorem 3 (Lower Bound on the List Size) *Let $\lfloor (d-1)/2 \rfloor < \tau < d \leq n$ and $\tau \leq n - \tau$. Then, there exists an $(n, M, d_R \geq d)_R$ code C over $\mathbb{F}_{q^m}$ of length $n \leq m$ and minimum rank distance $d_R \geq d$, and a word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ such that*

$$\ell \geq \big|\mathsf{C} \cap \mathcal{B}_\tau(\mathbf{r})\big| \geq q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}. \tag{5}$$

Proof: Let the $\mathsf{CR}(n, d_R \geq d, \tau)$ constant-rank code from Theorem 2 consist of the codewords:

$$\big\{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_{|\mathsf{N}|}\big\}.$$

This code has cardinality $|\mathsf{N}| = q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}$ (see Theorem 2). Choose $\mathbf{r} = \mathbf{0}$, and hence, $\mathrm{rk}(\mathbf{r} - \mathbf{a}_i) = \mathrm{rk}(\mathbf{a}_i) = \tau$ for all $i = 1, \dots, |\mathsf{N}|$ since the $\mathbf{a}_i$ are codewords of a constant-rank code of rank τ.

Moreover, $d_R(\mathbf{a}_i, \mathbf{a}_j) = \mathrm{rk}(\mathbf{a}_i - \mathbf{a}_j) \geq d$ since the constant-rank code has minimum rank distance at least d. Therefore, $\mathbf{a}_1, \dots, \mathbf{a}_{|\mathsf{N}|}$ are codewords of an $(n, M, d_R \geq d)_R$ code C over $\mathbb{F}_{q^m}$ in rank metric, which lie on the sphere of rank radius τ around $\mathbf{r} = \mathbf{0}$ (which is not a codeword of C).

Hence, there exists an $(n, M, d_R \geq d)_R$ code C over $\mathbb{F}_{q^m}$ such that $\ell \geq |\mathsf{C} \cap \mathcal{B}_\tau(\mathbf{r})| \geq |\mathsf{C} \cap \mathcal{S}_\tau(\mathbf{r})| = |\mathsf{N}| = q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}$. ■

This rank metric code C is not a linear code since it has codewords of weight τ, but minimum rank distance d.

For constant code rate $R = k/n$ and constant relative decoding radius τ/n, where $\tau > \lfloor (d-1)/2 \rfloor$, (5) gives

$$\ell \geq q^{n^2 (1 - \tau/n)(\tau/n - 1/2(1-R))} = q^{n^2 \cdot const}.$$

Therefore, the lower bound on list decoding of this $(n, M, d_R \geq d)_R$ code is exponential in $n \leq m$ for any

$\tau > \lfloor (d-1)/2 \rfloor$ and Theorem 3 shows that there exist codes, where the number of codewords in a rank metric ball around the all-zero word is exponential in n, thereby prohibiting polynomial-time list decoding.

The next corollary shows that the restriction $\tau \leq n - \tau$ does not limit the code rate for which Theorem 3 shows an exponential behavior of the list size. For the special case of $\tau = \lfloor (d-1)/2 \rfloor + 1$, the condition $\tau \leq n - \tau$ is always fulfilled for even minimum distance since $d \leq n$. For odd minimum $d - 1 \leq n$ has to hold. Note that $d = n$ is a trivial code.

Corollary 1 (Special Case $\tau = \lfloor (d-1)/2 \rfloor + 1$) *Let $n \leq m$, $\tau = \lfloor (d-1)/2 \rfloor + 1$ and $d \leq n-1$ when d is odd. Then, there exists a $(n, M, d_R \geq d)_R$ code C over $\mathbb{F}_{q^m}$ with $n \leq m$ and a word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ such that $|\mathsf{C} \cap \mathcal{B}_\tau(\mathbf{r})| \geq q^{(n-\tau)}$.*

This corollary hence shows that for any $n \leq m$ and *any code rate*, there exists a rank metric code of rank distance at least d whose list size can be exponential in n.

IV. Interpretation and Conclusion

This section interprets the results from the previous sections and compares them to known bounds on list decoding in Hamming metric (see e.g. [3, Chapters 4 and 6]).

Theorem 3 shows that for any $n \leq m$ and d, there is a code over $\mathbb{F}_{q^m}$ of minimum rank distance at least d and a word in $\mathbb{F}_{q^m}^n$ such that there is a ball of any radius $\tau > \lfloor (d-1)/2 \rfloor$, which contains a number of codewords that is exponential in the length n. Hence, for these rank metric codes *no* polynomial-time list decoding algorithm beyond half the minimum distance exists. However, this does not mean that this holds for *any* rank metric code. In particular, the theorem does not provide a conclusion if there exists a *linear* code or even a *Gabidulin* code with this list size. In order to find a *polynomial* upper bound, it will be necessary to use further properties of the code (such as linearity or a concrete weight distribution) in the derivation.

In particular, for Gabidulin codes, there is still an unknown region between half the minimum distance and the Johnson radius since we could only prove that the list size can be exponential beyond the Johnson radius (see [15]).

Further, our lower bound from Theorem 3 implies that there cannot exist a polynomial upper bound depending only on the length of the code n and minimum rank distance d similar to the Johnson bound in Hamming metric.

These results show surprising differences between codes in Hamming and rank metric. *Any* ball in Hamming metric of radius less than the Johnson radius $\tau_J = n - \sqrt{n(n-d)}$ always contains a *polynomial* number of codewords of *any* code in Hamming metric of length n and minimum Hamming distance d. Moreover, in Hamming metric there exist codes such that the list size is exponential in n if the radius is slightly greater than the Johnson radius [3], [6], whereas in rank metric we proved that this happens directly beyond half the minimum distance.

Acknowledgment

The author thanks Pierre Loidreau for the valuable discussions and the careful reading of the manuscript.

References

[1] S. Johnson, “A new Upper Bound for Error-Correcting Codes,” *IRE Transactions on Information Theory*, vol. 8, no. 3, pp. 203–207, Apr. 1962.

[2] L. A. Bassalygo, “New Upper Bounds for Error Correcting Codes,” *Problems of Information Transmission*, vol. 1, no. 4, pp. 41–44, 1965.

[3] V. Guruswami, *List Decoding of Error-Correcting Codes: Winning Thesis of the 2002 ACM Doctoral Dissertation Competition (Lecture Notes in Computer Science)*. Springer, Dec. 1999.

[4] V. Guruswami and M. Sudan, “Improved Decoding of Reed-Solomon and Algebraic-Geometry Codes,” *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1757–1767, Sept. 1999.

[5] M. Sudan, “Decoding of Reed Solomon Codes beyond the Error-Correction Bound,” *Journal of Complexity*, vol. 13, no. 1, pp. 180–193, Mar. 1997.

[6] O. Goldreich, R. Rubinfeld, and M. Sudan, “Learning polynomials with queries: the highly noisy case,” *SIAM Journal on Discrete Mathematics*, vol. 13, no. 4, 2000.

[7] R. Kötter and F. R. Kschischang, “Coding for Errors and Erasures in Random Network Coding,” *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, July 2008.

[8] D. Silva, F. R. Kschischang, and R. Kötter, “A Rank-Metric Approach to Error Control in Random Network Coding,” *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 3951–3967, 2008.

[9] P. Delsarte, “Bilinear Forms over a Finite Field, with Applications to Coding Theory,” *J. Comb. Theory, Ser. A*, vol. 25, no. 3, pp. 226–241, 1978.

[10] E. M. Gabidulin, “Theory of Codes with Maximum Rank Distance,” *Probl. Peredachi Inf.*, vol. 21, no. 1, pp. 3–16, 1985.

[11] R. M. Roth, “Maximum-Rank Array Codes and their Application to Crisscross Error Correction,” *IEEE Transactions on Information Theory*, vol. 37, no. 2, pp. 328–336, 1991.

[12] H. Mahdavifar and A. Vardy, “Algebraic List-Decoding on the Operator Channel,” in *IEEE International Symposium on Information Theory (ISIT 2010)*, June 2010, pp. 1193–1197.

[13] ——, “List-Decoding of Subspace Codes and Rank-Metric Codes up to Singleton Bound,” in *IEEE International Symposium on Information Theory 2012 (ISIT 2012)*, July 2012, pp. 1488–1492.

[14] V. Guruswami and C. Xing, “List Decoding Reed–Solomon, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound,” *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 19, no. 146, 2012.

[15] A. Wachter-Zeh, “Bounds on List Decoding Gabidulin Codes,” in *Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2012)*, June 2012, pp. 329–334.

[16] M. Gadouleau and Z. Yan, “Constant-Rank Codes and Their Connection to Constant-Dimension Codes,” *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3207–3216, July 2010.

[17] A. Wachter-Zeh, “Bounds on List Decoding of Rank Metric Codes,” *preprint*, 2012. [Online]. Available: http://arxiv.org/abs/1301.4643

[18] H. Wang, C. Xing, and R. Safavi-Naini, “Linear Authentication Codes: Bounds and Constructions,” *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 866–872, Apr. 2003.

[19] S. Xia and F. Fu, “Johnson type bounds on constant dimension codes,” *Designs, Codes and Cryptography*, vol. 50, no. 2, pp. 163–172, Feb. 2009.

[20] T. Etzion and N. Silberstein, “Error-Correcting Codes in Projective Spaces Via Rank-Metric Codes and Ferrers Diagrams,” *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 2909–2919, July 2009.

[21] V. Skachek, “Recursive Code Construction for Random Networks,” *IEEE Transactions on Information Theory*, vol. 56, no. 3, pp. 1378–1382, Mar. 2010.

[22] T. Etzion and A. Vardy, “Error-Correcting Codes in Projective Space,” *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1165–1173, Feb. 2011.

[23] C. Bachoc, F. Vallentin, and A. Passuello, “Bounds for Projective Codes from Semidefinite Programming,” *preprint*, May 2012. [Online]. Available: http://arxiv.org/abs/1205.6406