On the Decoder Error Probability of Bounded Rank Distance Decoders for Rank Metric Codes

Maximilien Gadouleau and Zhiyuan Yan
Department of Electrical and Computer Engineering
Lehigh University, PA 18015, USA
E-mails: {magc, yan}@lehigh.edu

***Abstract*— In this paper we investigate the decoder error probability (DEP) of bounded rank distance decoders for rank metric codes over two types of channels motivated by network coding. The first channel is a rank symmetric channel where additive errors with the same rank are equiprobable, and for the second and more general channel, errors with the same row or column space are equiprobable. For arbitrary rank metric codes, we first derive analytical expressions of as well as upper bounds on DEPs of bounded distance decoders over the rank symmetric channel, and then establish upper bounds on DEP of bounded distance decoders over the equal row (or column) space channel. Our results show that DEP of bounded distance decoders for any rank metric code with error correction capability t decreases exponentially with t^2. For maximum rank distance (MRD) codes, we determine the exact DEP of bounded distance decoders over equal row (or column) space channels as long as MRD codes or their transpose exist, and show that MRD codes have the highest DEP up to a scalar. These results provide insights on the error performance of rank metric codes used for error correction in random linear network coding.**

I. Introduction

Rank metric codes [1]–[3] have been receiving growing attention due to their applications in storage systems [2], public-key cryptosystems [4], space-time coding [5], and error control for random network coding [6]. The pioneering works in [1]–[3] have established many important properties of rank metric codes. Independently in [1]–[3], the maximum cardinality of a code with a given minimum rank distance was determined. We refer to *linear or nonlinear* codes that achieve the maximum cardinality as maximum rank distance (MRD) codes, and the class of linear MRD codes proposed independently in [1]–[3] as Gabidulin codes henceforth. Different decoding algorithms for Gabidulin codes were proposed in [1], [2], [7], [8], and their complexities were compared in [9].

While random linear network coding has proved to be a powerful tool for disseminating information in networks, it is highly susceptible to errors caused by various sources such as noise, malicious or malfunctioning nodes, or insufficient min-cut. If received packets are linearly combined at random to deduce the transmitted message, even a single error in one erroneous packet could render the entire transmission useless. Thus, error control for random linear network coding is critical and has received growing attention recently. Two types of error control techniques for random network coding have been proposed: coherent techniques [10], [11] rely on the underlying network topology, while noncoherent error control [6], [12] do not assume any specific knowledge of the network. Noncoherent techniques are hence more flexible and more adapted to time-varying networks. Codes defined in Grassmannians associated with the vector space play a significant role in error control for noncoherent random linear network coding; such codes are also referred to as constant-dimension codes (CDCs) [12]. CDCs are closely related to rank metric codes through the lifting operation [6]. In particular, liftings of Gabidulin codes are nearly optimal CDCs [12] and a generalized rank metric decoder aimed at correcting the errors occurring on the network is proposed in [6]. Thus error control in random linear network coding using CDCs can be turned into a rank metric problem [6], and the errors occurring in the network result into additive rank errors.

In this paper, we investigate the error performance of a bounded rank distance decoder for rank metric codes and MRD codes in particular, which provides insight on the performance of the decoder in [6] for Gabidulin codes. A bounded rank distance decoder for MRD codes with error correction capability t is guaranteed to correct all errors with rank no more than t. Given a received word, a bounded rank distance decoder either provides an estimate for the transmitted codeword or declares decoder failure. A decoder error occurs when the estimate is not the actual transmitted codeword. The main results of this paper are analytical expressions and upper bounds on the decoder error probability (DEP) of bounded rank distance decoders for MRD codes. We consider two types of additive rank errors, both being motivated by error correction in random linear network coding. We emphasize that the DEP considered herein is conditional: it is the probability that a bounded rank distance decoder, correcting up to t rank errors, makes an erroneous correction. Since decoder failures can be remedied by error masking or retransmission, decoder errors are often more detrimental to the overall system performance and hence often considered separately. This is the main reason we focus on the DEP.

The main contributions of the paper are:

- We first consider a rank symmetric channel, where all additive errors with the same rank are equiprobable. For any rank metric code over the rank symmetric channel, we derive an analytical expression for DEP of bounded distance decoders, which depends on the weight distribution of the code, as well as upper bounds. Our results show that the DEP of bounded distance decoders for

978-1-4244-4983-5/09/$25.00 © 2009 IEEE

any rank metric code with error correction capability t decreases exponentially with t^2. For MRD codes over the rank symmetric channel, we derive the exact DEP of bounded distance decoders, and show that MRD codes have the highest DEP up to a scalar.

- We then consider a more general channel, where all additive errors with the same row (or column) space are equiprobable. For any rank metric code over the equal row (or column) space channel, we derive upper bounds on the DEP of bounded rank distance decoders. Again our results show that DEP of bounded distance decoders for any rank metric code with error correction capability t decreases exponentially with t^2. For MRD codes over the equal row (or column) space channel, we derive the exact DEP of bounded distance decoders as long as MRD codes or their transpose exist.

Our work in this paper differs from the error performance analysis of rank metric codes in [13] in several aspects, and is an extension of our previous work [14]. The error performance analysis in [13] was aimed at crisscross errors and as such, assumes different channel models and considers decoder errors and decoder failures together. Our previous work [14] derived only upper bounds on bounded distance decoders for Gabidulin codes over the rank symmetric channel. Our results in this paper differ from those derived in [14] in three ways. First, they are more general in terms of the channel model, as it considers channels where all additive errors with the same row or column span are equiprobable. Second, these results are not only applicable to Gabidulin codes, but also to any linear or nonlinear rank metric code. Finally, because of their expanded span, the derivation of the results in this paper use a significantly different approach to the one used in [14].

Our results may also be seen as a nontrivial extension of the error performance of Hamming metric codes and maximum distance separable (MDS) codes in particular in [15]–[17]. In [15], an upper bound on the DEP of bounded Hamming distance decoders for Reed-Solomon codes (in fact, of any linear MDS code) was derived for a channel where all errors with the same Hamming weight are equiprobable. This work was refined in [16], where the exact DEP of linear MDS codes was determined over the same channel. In [17], the results in [15] were extended to more general channels and to any linear code. More precisely, [17] introduces error-value symmetric channels, where all errors with the same support are equiprobable, thus taking bursty channels into account. While our previous work in [14] parallels the work in [15], our analytical expression of the DEP of bounded distance decoders for MRD codes over the rank symmetric channel parallels the work in [16]. However, our approach to derive our results for MRD codes is significantly different from the one used in [16]. The equal row (or column) space channel we considered can also be viewed as counterparts of the error-value symmetric channels in [17], and hence our results for arbitrary rank metric codes over the equal row (or column) space channel parallel the results in [17].

II. Preliminaries

The set $\mathrm{GF}(q)^{m\times n}$ of $m\times n$ matrices over $\mathrm{GF}(q)$, endowed with the rank distance $d_{\mathrm{R}}(\mathbf{X},\mathbf{Y}) \stackrel{\text{def}}{=} \mathrm{rk}(\mathbf{X}-\mathbf{Y})$, constitutes a metric association scheme [3]. Its *valencies* [18] $N_{\mathrm{R}}(u)$ are the numbers of matrices at rank distance u from any matrix in $\mathrm{GF}(q)^{m\times n}$ for all u. They are given by $N_{\mathrm{R}}(u) = \begin{bmatrix} n \\ u \end{bmatrix} \alpha(m,u)$, where $\alpha(m,0)=1$ and $\alpha(m,u) = \prod_{i=0}^{u-1}(q^m - q^i)$ for $u \geq 1$ and $\begin{bmatrix} n \\ u \end{bmatrix} = \frac{\alpha(n,u)}{\alpha(u,u)}$ is the Gaussian binomial [19]. This term satisfies [14]

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

for all $0 \leq r \leq n$, where $K_q = \prod_{j=1}^{\infty}(1-q^{-j})$. The *intersection numbers* $J_{\mathrm{R}}(u,s,d)$ for rank metric codes, which are critical to association schemes, were derived in [20]. They are the volume of the intersection of two spheres with rank radii u and s and with distance d between their centers. In particular, $J_{\mathrm{R}}(t,d-t,d) = q^{t(d-t)}\begin{bmatrix} d \\ t \end{bmatrix}$ for all $0 \leq t \leq d \leq \min\{n,m\}$, and they have the following basic properties [18]:

$$N_{\mathrm{R}}(d) J_{\mathrm{R}}(u,s,d) = N_{\mathrm{R}}(u) J_{\mathrm{R}}(d,s,u) \tag{2}$$

$$\sum_{u=0}^{n} J_{\mathrm{R}}(u,s,d) = N_{\mathrm{R}}(s). \tag{3}$$

The volume of a ball with rank radius t in $\mathrm{GF}(q)^{m\times n}$ is denoted as $V_{\mathrm{R}}(t) = \sum_{s=0}^{t} N_{\mathrm{R}}(s)$.

A *rank metric code* can be viewed as a subset of $\mathrm{GF}(q)^{m\times n}$. The minimum rank distance of a code is simply the minimum distance over all pairs of distinct codewords. It is shown [1]–[3] that the maximum cardinality of a rank metric code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d is $\min\{q^{m(n-d+1)}, q^{n(m-d+1)}\}$. We refer to codes with maximum cardinality as MRD codes, and the subclass of linear MRD codes introduced independently in [1]–[3] as Gabidulin codes. The number of codewords with rank r in a linear MRD code in $\mathrm{GF}(q)^{m\times n}$ $(n \leq m)$ with minimum rank distance d was determined in [1], [3] and is denoted as $M(q,m,n,d,r)$. In particular, we have $M(q,m,n,d,d) = \begin{bmatrix} n \\ d \end{bmatrix}(q^m - 1)$.

A constant-rank code (CRC) is a rank metric code whose codewords have the same rank [21]. The maximum cardinality of a CRC in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d and constant-rank r, denoted as $A_{\mathrm{R}}(q,m,n,d,r)$, is studied in [21]. In particular, it is shown that $A_{\mathrm{R}}(q,m,n,d,r) = A_{\mathrm{R}}(q,n,m,d,r)$ and, for $n \leq m$ and $d \leq r$,

$$A_{\mathrm{R}}(q,m,n,d,r) \leq \begin{bmatrix} n \\ r \end{bmatrix} \alpha(m, r-d+1). \tag{4}$$

III. DEP of rank metric codes

We now introduce and motivate our choice of additive rank error models and their significance to error correction in random linear network coding. We consider the case of an adversary who injects linearly independent packets maliciously on the network using two strategies. In the first strategy, the adversary injects a number of packets chosen at random with equal probabilities. The packets undergo linear combinations

through the network, and result into an additive error whose rank depends on the number of packets injected. Hence our first error model assumes that all additive errors with the same rank are equiprobable. The second and more general strategy assumes the adversary has some knowledge on and takes advantage of the data transmitted or the protocol used. Hence the adversary may choose to inject some packets which corrupt the messages more efficiently than others [22]. Due to the vector-space preserving property of linear network coding, the row space of the erroneous packets remains unchanged through the linear combinations operated at different nodes. Hence, the additive error can take any value provided its row space is fixed. This leads to our second model of additive rank errors, where all errors with the same row space are equiprobable. Finally, because of the properties of the rank metric, we also consider channels where errors with the same column space are equiprobable.

A. DEP over a rank symmetric channel

We now study the DEP of a rank metric code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d using a bounded rank distance decoder over a rank symmetric channel, defined below.

Definition 1: A channel on $\mathrm{GF}(q)^{m\times n}$ is *rank symmetric* if the inputs and the outputs are matrices in $\mathrm{GF}(q)^{m\times n}$ and if all the outputs at the same rank distance from the input are equiprobable.

Since using a code $\mathcal{C}\subseteq \mathrm{GF}(q)^{m\times n}$ over a rank symmetric channel on $\mathrm{GF}(q)^{m\times n}$ is equivalent to using its transpose code $\mathcal{C}^T=\{\mathbf{C}^T:\mathbf{C}\in\mathcal{C}\}$ over a rank symmetric channel on $\mathrm{GF}(q)^{n\times m}$, we assume $n\leq m$ without loss of generality.

Given a matrix $\mathbf{M}\in\mathrm{GF}(q)^{m\times n}$ as input, a bounded distance decoder for a code $\mathcal{C}$ either produces the codeword in $\mathcal{C}$ at distance at most $t=\lfloor\frac{d-1}{2}\rfloor$ from $\mathbf{M}$ if such a codeword exists, or returns a failure otherwise. The *decoder error probability* (DEP) is the probability that the decoder produces a codeword different to the one that was sent. The output of the bounded rank distance decoder depends on $u=d_{\mathrm{R}}(\mathbf{M},\mathbf{C})$, where $\mathbf{C}\in\mathcal{C}$ is the sent codeword. The decoder returns $\mathbf{C}$ if and only if $u\leq t$, and returns a failure for $t<u<d-t$. The DEP for $u\geq d-t$ depends on the rank distance distribution $A_w(\mathbf{C})$ of the code.

Proposition 1: Assuming a codeword $\mathbf{C}\in\mathcal{C}$, a code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d, is sent over a rank symmetric channel and the channel output is distance u from $\mathbf{C}$, the DEP of a bounded rank distance decoder satisfies

$$\begin{aligned} P_{\mathrm{R}}(\mathbf{C},u) &= \frac{1}{N_{\mathrm{R}}(u)}\sum_{w=d}^{n}A_w(\mathbf{C})\sum_{s=0}^{t}J_{\mathrm{R}}(u,s,w) && (5)\\ &\leq \frac{1}{N_{\mathrm{R}}(u)}\sum_{w=d}^{n}\begin{bmatrix}n\\w\end{bmatrix}\alpha(m,w-d+1)\\ &\quad\cdot\sum_{s=0}^{t}J_{\mathrm{R}}(u,s,w) && (6)\\ &< K_q^{-2}q^{-t(m-n+t)}. && (7)\end{aligned}$$

Proof: We have $P_{\mathrm{R}}(\mathbf{C},u)=\frac{D(\mathbf{C},u)}{N_{\mathrm{R}}(u)}$, where $D(\mathbf{C},u)$ is the number of decodable matrices at distance u from $\mathbf{C}$. The set of decodable matrices is the disjoint union of balls with radius t around the codewords. For any codeword $\mathbf{D}$ at distance w from $\mathbf{C}$, there exist exactly $J_{\mathrm{R}}(u,s,w)$ matrices $\mathbf{M}$ such that $d_{\mathrm{R}}(\mathbf{D},\mathbf{M})=s$ and $d_{\mathrm{R}}(\mathbf{C},\mathbf{M})=u$. Summing for all s and all $\mathbf{D}$, we obtain (5).

Also, since $\{\mathbf{D}-\mathbf{C}:\mathbf{D}\in\mathcal{C},d_{\mathrm{R}}(\mathbf{D},\mathbf{C})=w\}$ is a CRC with minimum distance at least d and constant-rank w, we have $A_w(\mathbf{C})\leq A_{\mathrm{R}}(q,m,n,d,w)\leq\begin{bmatrix}n\\w\end{bmatrix}\alpha(m,w-d+1)$ by (4), which leads to (6). We have $\begin{bmatrix}n\\w\end{bmatrix}\alpha(m,w-d+1)<K_q^{-1}q^{-m(d-1)}N_{\mathrm{R}}(w)$, and hence

$$\begin{aligned} P_{\mathrm{R}}(\mathbf{C},u) &< \frac{1}{N_{\mathrm{R}}(u)}K_q^{-1}q^{-m(d-1)}\sum_{s=0}^{t}\sum_{w=d}^{n}N_{\mathrm{R}}(w)J_{\mathrm{R}}(u,s,w)\\ &= K_q^{-1}q^{-m(d-1)}\sum_{s=0}^{t}\sum_{w=d}^{n}J_{\mathrm{R}}(w,s,u) && (8)\\ &\leq K_q^{-1}q^{-m(d-1)}V_{\mathrm{R}}(t), && (9)\end{aligned}$$

where (8) and (9) follow (2) and (3), respectively. Using $V_{\mathrm{R}}(t)<K_q^{-1}q^{t(m+n-t)}$ [14], we obtain (7). ∎

It is remarkable that the upper bound on the DEP in (7) does not depend on $\mathbf{C}$ and u for **any rank metric code**. In fact, applying (7) to linear MRD codes leads to [14, Proposition 6]. This general result on the error performance of rank metric codes parallel that for Hamming metric codes [17].

We now show that MRD codes have the **greatest** DEP among all rank metric codes up to a scalar in nontrivial cases. Let us denote the DEP of an MRD code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d as $P_{\mathrm{R,MRD}}(u)$.

Corollary 1: Let $\mathcal{C}$ be any rank metric code in $\mathrm{GF}(q)^{m\times n}$ $(n\leq m)$ with minimum rank distance d and let $\mathbf{C}\in\mathcal{C}$. Then if $q>2$, $n<m$, or $d\neq m-1$, $P_{\mathrm{R}}(\mathbf{C},u)<H_qP_{\mathrm{R,MRD}}(u)$, where $H_2=3.5$ and $H_q=\frac{q-1}{q-2}$ for $q>2$.

Proof: By [21], we have $H_qM(q,m,n,d,r)>A_{\mathrm{R}}(q,m,n,d,r)$ for $n\geq r\geq d$, as long as $q>2$, $n<m$, or $d\neq m-1$. Hence $H_qP_{\mathrm{R,MRD}}(u)>\frac{1}{N_{\mathrm{R}}(u)}\sum_{w=d}^{n}A_{\mathrm{R}}(q,m,n,d,w)\sum_{s=0}^{t}J_{\mathrm{R}}(u,s,w)\geq P_{\mathrm{R}}(\mathbf{C},u)$. ∎

In many applications, the probability that the received matrix is at distance u from the sent codeword decreases rapidly with u, and hence the overall DEP can be approximated by $P_{\mathrm{R}}(\mathbf{C},d-t)$. We consider this special case next.

Proposition 2: Assume a codeword $\mathbf{C}\in\mathcal{C}$, a code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d, is sent over a rank symmetric channel and the channel output is distance $u=d-t$ from $\mathbf{C}$, the DEP of a bounded rank distance decoder is given by

$$P_{\mathrm{R}}(\mathbf{C},d-t)=q^{t(d-t)}\frac{\begin{bmatrix}d\\t\end{bmatrix}}{\begin{bmatrix}n\\d-t\end{bmatrix}\alpha(m,d-t)}A_d(\mathbf{C}). \qquad (10)$$

In particular, the DEP of an MRD code satisfies $P_{\mathrm{R,MRD}}(d-t)>K_qq^{-t(m+n-t)}$ when $d=2t+1$.

Proof: First, (5) yields $P_{\mathrm{R}}(\mathbf{C},d-t)=\frac{J_{\mathrm{R}}(d-t,t,d)}{N_{\mathrm{R}}(d-t)}A_d(\mathbf{C})$, which gives (10). For an MRD code, we have $A_d(\mathbf{C})=$

$M(q,m,n,d,d) = \begin{bmatrix} n \\ d \end{bmatrix}(q^m - 1)$. Using the bounds on the Gaussian binomial in (1), we obtain $P_{\text{R,MRD}}(d-t) > K_q q^{-t(m-n+t)}$ when $d = 2t+1$. ■

When $u = d-t$, Proposition 2 above not only provides the DEP for any code, but also shows that the upper bound on the DEP for MRD codes in (7) is **tight** up to a scalar.

B. DEP over an equal row or column space channels

We now consider channels where the errors with the same row (or column) space are equiprobable.

Definition 2: A channel on $\mathrm{GF}(q)^{m\times n}$ is equal row (column) space if the error is additive and the error patterns with the same row (column) space are equiprobable.

Equal row and column space channels are interesting in several respects. First, rank symmetric channels are both equal row and equal column space channels, hence the following results will be generalizations of those in Section III-A. Also, considering these more general channels does not dramatically affect the tightness of the bounds. Finally, it is remarkable that these channels may also be used to model other applications of rank metric codes. Rank metric codes can be used for the correction of two-dimension errors [2], [23] (i.e., errors confined to a certain number of rows and columns) in storage equipments. Hence, our model encompasses the case of two-dimensional errors, where some rows or columns are more likely to be in error than others.

Note that using a code $\mathcal{C}$ over an equal row space channel on $\mathrm{GF}(q)^{m\times n}$ is equivalent to using its transpose code over a column space channel on $\mathrm{GF}(q)^{n\times m}$. We study equal row space channels first. In this case, it is clear that the DEP depends not only on the rank u of the error, but also on its row space $U \in E_u(q,n)$. We hence derive a bound on $P_{\text{R}}(\mathbf{C},U)$ for all codes, and we also obtain the exact value of $P_{\text{R}}(U)$ for linear MRD codes when $n \le m$, thus generalizing the results in Proposition 1 for equal row space channels.

Proposition 3: Assuming a codeword $\mathbf{C} \in \mathcal{C}$, a code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d, is sent over an equal row space channel and the channel error has row space $U \in E_u(q,n)$, the DEP of a bounded rank distance decoder satisfies

$$\begin{aligned} P_{\text{R}}(\mathbf{C},U) &\le \frac{1}{N_{\text{R}}(u)} \sum_{w=d}^{n} \begin{bmatrix} n \\ w \end{bmatrix} \alpha(m, w-d+1) \\ &\quad \cdot \sum_{s=0}^{t} J_{\text{R}}(u,s,w) \qquad (11) \\ &< K_q^{-2} q^{-t(m-n+t)}. \qquad (12) \end{aligned}$$

Furthermore, if $n \le m$ and $\mathcal{C}$ is a linear MRD code, then the DEP is given by

$$P_{\text{R,MRD}}(U) = \frac{1}{N_{\text{R}}(u)} \sum_{w=d}^{n} M(q,m,n,d,w) \sum_{s=0}^{t} J_{\text{R}}(u,s,w). \qquad (13)$$

The proof of Proposition 3 is given in Appendix A. We remark that the right hand sides of (11) and (12) are exactly the ones in (6) and (7), respectively. Therefore, the upper bounds on the DEP obtained for rank symmetric channels are generalized to row symmetric channels without loss of tightness. By comparing (13) to (5), we also conclude that the DEP of a linear MRD code in $\mathrm{GF}(q)^{m\times n}$ $(n \le m)$ over any row space channel is equal to that of the same code over a rank symmetric channel.

A similar upper bound can be obtained for an equal column space channel.

Proposition 4: Assuming a codeword $\mathbf{C} \in \mathcal{C}$, a code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d, is sent over an equal column space channel and the channel error has column space $U \in E_u(q,m)$, the DEP of a bounded rank distance decoder satisfies

$$\begin{aligned} P_{\text{R}}(\mathbf{C},U) &\le \frac{1}{N_{\text{R}}(u)} \sum_{w=d}^{n} \begin{bmatrix} m \\ w \end{bmatrix} \alpha(n, w-d+1) \\ &\quad \cdot \sum_{s=0}^{t} J_{\text{R}}(u,s,w) \\ &< K_q^{-2} q^{-t(n-m+t)}. \end{aligned}$$

Furthermore, if $n \ge m$ and $\mathcal{C}$ is the transpose code of a linear MRD code, then the DEP is given by

$$P_{\text{R,MRD}}(U) = \frac{1}{N_{\text{R}}(u)} \sum_{w=d}^{m} M(q,n,m,d,w) \sum_{s=0}^{t} J_{\text{R}}(u,s,w).$$

The proof of Proposition 4 is similar to that of Proposition 3 and is hence omitted.

IV. Conclusion and Discussion

In this paper, we investigated the error performance of a bounded rank distance decoder for rank metric codes over two types of channels. We derived bounds on the decoder error probability of any rank metric code and determined the order of the decoder error probability of MRD codes, and in particular of Gabidulin codes, under these settings. However, the decoder proposed in [6] for Gabidulin codes is a generalized bounded rank distance decoder, which can also correct the so-called erasures and deviations [6]. Hence our results can be applied to the decoder in [6] for the special case where no erasures and no deviations occurred. Nonetheless, we believe our study provides insight on the error performance of the decoder proposed in [6]. Furthermore, a natural extension of our work is the study of the error performance of the decoder in [6] in the case where errors, erasures, and deviations occurred.

Appendix

A. Proof of Proposition 3

In order to prove Proposition 3, we need two technical lemmas. For any $\mathbf{R} \in \mathrm{GF}(q)^{m\times n}$, we denote the number of matrices with row space W and at rank distance s from $\mathbf{R}$ as $g(W,s,\mathbf{R})$. We prove below that $g(W,s,\mathbf{R})$ only depends on $\mathbf{R}$ through its row space.

Lemma 1: For all $\mathbf{R},\mathbf{S} \in \mathrm{GF}(q)^{m\times n}$ with the same row space U, $g(W,s,\mathbf{R}) = g(W,s,\mathbf{S})$, and hence $g(W,s,\mathbf{R}) = g(W,s,U)$.

Proof: Suppose $\mathbf{X} \in \mathrm{GF}(q)^{m\times n}$ has row space W and satisfies $\mathrm{rk}(\mathbf{X}-\mathbf{R}) = s$. We can express $\mathbf{S} = \mathbf{AR}$, where $\mathbf{A} \in \mathrm{GF}(q)^{m\times m}$ has full rank, hence $\mathbf{Y} = \mathbf{AX}$ has row space W and satisfies $\mathrm{rk}(\mathbf{Y}-\mathbf{S}) = \mathrm{rk}(\mathbf{X}-\mathbf{R}) = s$. Thus $g(W,s,\mathbf{S}) \geq g(W,s,\mathbf{R})$. Using $\mathbf{R} = \mathbf{A}^{-1}\mathbf{S}$, we show that $g(W,s,\mathbf{S}) \leq g(W,s,\mathbf{R})$; hence $g(W,s,\mathbf{R}) = g(W,s,\mathbf{S})$. ■

Lemma 2: For all $U \in E_u(q,n)$, $\sum_{W\in E_w(q,n)} g(U,s,W) = \begin{bmatrix} n \\ w \end{bmatrix} J_{\mathrm{R}}(u,s,w)$.

Proof: By counting the number of pairs of matrices $(\mathbf{R},\mathbf{W})$ where $\mathfrak{R}(\mathbf{R}) = U$, $\mathfrak{R}(\mathbf{W}) = W$, and $d_{\mathrm{R}}(\mathbf{R},\mathbf{W}) = s$ in two ways, we have $\alpha(m,u)g(W,s,U) = \alpha(m,w)g(U,s,W)$. Hence $\sum_{W\in E_w(q,n)} g(U,s,W) = \frac{\alpha(m,u)}{\alpha(m,w)} \sum_{W\in E_w(q,n)} g(W,s,U) = \frac{\alpha(m,u)}{\alpha(m,w)} J_{\mathrm{R}}(w,s,u)$. Using (2), we obtain $\sum_{W\in E_w(q,n)} g(U,s,W) = \frac{\begin{bmatrix} n \\ w \end{bmatrix}}{\begin{bmatrix} n \\ u \end{bmatrix}} J_{\mathrm{R}}(u,s,w)$. ■

We now give the proof of Proposition 3.

Proof: Let $\mathcal{C}$ be a rank metric code in $\mathrm{GF}(q)^{m\times n}$ with minimum rank distance d. We have $P_{\mathrm{R}}(\mathbf{C},U) = \frac{1}{\alpha(m,u)} \sum_{s=0}^{t} \delta(U,s,\mathbf{C})$, where $\delta(U,s,\mathbf{C})$ is the number of matrices $\mathbf{X}$ at distance s from the code, and such that $\mathfrak{R}(\mathbf{X}-\mathbf{C}) = U$. Hence $\delta(U,s,\mathbf{C}) = \sum_{W:\dim(W)\geq d} A_W(\mathbf{C}) g(U,s,W)$, where $A_W(\mathbf{C}) = |\{\mathbf{D} \in \mathcal{C} : \mathfrak{R}(\mathbf{D}-\mathbf{C}) = W\}|$ for all $W \in E(q,n)$. We now give an upper bound on $A_W(\mathbf{C})$. Let $C_W = \{\mathbf{D}-\mathbf{C} : \mathbf{D} \in \mathcal{C}, \mathfrak{R}(\mathbf{D}-\mathbf{C}) = W\}$, then the restriction of C_W to W [14] forms a constant-rank code in $\mathrm{GF}(q)^{m\times w}$ with constant-rank w and minimum distance d. Therefore, $A_W(\mathbf{C}) \leq A_{\mathrm{R}}(q,m,w,d,w) \leq \alpha(m,w-d+1)$ by (4). The DEP hence satisfies

$$
\begin{aligned}
&P_{\mathrm{R}}(\mathbf{C},U) \\
&= \frac{1}{\alpha(m,u)} \sum_{s=0}^{t} \sum_{w=d}^{n} \sum_{W\in E_w(q,n)} A_W(\mathbf{C}) g(U,s,W) \\
&\leq \frac{1}{\alpha(m,u)} \sum_{s=0}^{t} \sum_{w=d}^{n} \alpha(m,w-d+1) \sum_{W\in E_w(q,n)} g(U,s,W) \\
&= \frac{1}{N_{\mathrm{R}}(u)} \sum_{w=d}^{n} \begin{bmatrix} n \\ w \end{bmatrix} \alpha(m,w-d+1) \sum_{s=0}^{t} J_{\mathrm{R}}(u,s,w), \qquad (14)
\end{aligned}
$$

where (14) follows Lemma 2.

When C is an MRD code with minimum rank distance d, it can be shown that $A_W(\mathbf{C}) = M(q,m,w,d,w) = \begin{bmatrix} n \\ w \end{bmatrix}^{-1} M(q,m,n,d,w)$, and hence

$$
\delta(U,s,\mathbf{C}) = \frac{\alpha(m,u)}{N_{\mathrm{R}}(u)} \sum_{w=d}^{n} M(q,m,n,d,w) J_{\mathrm{R}}(u,s,w),
$$

which leads to (13). ■

REFERENCES

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

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

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

[4] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a non-commutative ring and their application in cryptology," *LNCS*, vol. 573, pp. 482–489, 1991.

[5] P. Lusina, E. M. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Trans. Info. Theory*, vol. 49, pp. 2757–2760, Oct. 2003.

[6] D. Silva, F. R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Info. Theory*, vol. 54, no. 9, pp. 3951–3967, 2008.

[7] G. Richter and S. Plass, "Fast decoding of rank-codes with rank errors and column erasures," *Proc. IEEE Int. Symp. on Information Theory*, p. 398, June 2004.

[8] P. Loidreau, "A Welch-Berlekamp like algorithm for decoding Gabidulin codes," *Proc. International Workshop on Coding and Cryptography*, 2005.

[9] M. Gadouleau and Z. Yan, "Complexity of decoding Gabidulin codes," *Proc. IEEE CISS*, pp. 1081–1085, March 2008.

[10] R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Commun. Inform. Syst.*, vol. 6, no. 1, pp. 19–36, 2006.

[11] N. Cai and R. W. Yeung, "Network error correction, part II: Lower bounds," *Commun. Inform. Syst.*, vol. 6, no. 1, pp. 37–54, 2006.

[12] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Info. Theory*, vol. 54, no. 8, pp. 3579–3591, August 2008.

[13] R. M. Roth, "Probabilistic crisscross error correction," *IEEE Trans. Info. Theory*, vol. 43, no. 5, pp. 1425–1438, Sept. 1997.

[14] M. Gadouleau and Z. Yan, "On the decoder error probability of bounded rank-distance decoders for maximum rank distance codes," *IEEE Trans. Info. Theory*, vol. 54, no. 7, pp. 3202–3206, July 2008.

[15] R. J. McEliece and L. Swanson, "On the decoder error probability for Reed-Solomon codes," *IEEE Trans. Info. Theory*, vol. 32, no. 5, pp. 701–703, Sept. 1986.

[16] K.-M. Cheung, "More on the decoder error probability for Reed-Solomon codes," *IEEE Trans. Info. Theory*, vol. 35, no. 4, pp. 895–900, July 1989.

[17] L. Tolhuizen, "A universal upper bound on the miscorrection probability with bounded distance decoding for a code used on an error-value symmetric channel," *Proc. Eurocode, Int. Symp. on Coding Theory and Applications*, pp. 313–320, 1992.

[18] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*, ser. A Series of Modern Surveys in Mathematics. Springer-Verlag, 1989, vol. 18, no. 3.

[19] G. E. Andrews, *The Theory of Partitions*, ser. Encyclopedia of Mathematics and its Applications, G.-C. Rota, Ed. Reading, MA: Addison-Wesley, 1976, vol. 2.

[20] M. Gadouleau and Z. Yan, "Bounds on covering codes with the rank metric," *to appear in IEEE Communications Letters*, August 2009, available at http://arxiv.org/abs/0809.2968.

[21] ——, "Constant-rank codes and their connection to constant-dimension codes," *submitted to IEEE Trans. Info. Theory*, July 2008, available at http://arxiv.org/abs/0803.2262.

[22] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," 2008, available at http://arxiv.org/abs/0805.3824v1.

[23] E. M. Gabidulin, "Optimal codes correcting lattice-pattern errors," *Problems on Information Transmission*, vol. 21, no. 2, pp. 3–11, 1985.