Decoder Error Probability of Bounded Distance Decoders for Constant-Dimension Codes

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

***Abstract*—Constant-dimension codes (CDCs) have been considered for error correction in random linear network coding, and low-complexity bounded distance decoders have been proposed. However, error performance, decoder error probability (DEP) in particular, of these bounded distance decoders has received little attention. In this paper, we first establish some fundamental geometric properties of the projective space. In particular, we show that the volume of the intersection of two spheres depends on only the two radii as well as the distance between and the dimensions of the two centers. Using these geometric properties, we then consider bounded distance decoders in both subspace and injection metrics and derive analytical expressions of their DEPs for CDCs over a symmetric operator channel, which ultimately depend on their distance distributions. Finally, we focus on CDCs obtained by lifting rank metric codes since their distance distributions are known, and obtain two important results. First, we obtain asymptotically tight upper bounds on the DEPs of bounded distance decoders in both metrics; the upper bounds decrease exponentially with the square of the minimum distance. Second, we show that the DEP for KK codes, obtained by lifting Gabidulin codes, is the highest up to a scalar among all CDCs obtained by lifting rank metric codes.**

I. Introduction

Random linear network coding [1]–[3] is a powerful tool for disseminating information in networks, but it is highly susceptible to errors. Since received packets are linearly combined 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. Some error control schemes model data transmission in random linear network coding as sending subspaces through an operator channel [4]. Error correction can hence be treated as a coding problem where codewords are linear subspaces and codes are subsets of the projective space of a vector space over a finite field. In particular, codes defined in Grassmannians associated with the vector space play a significant role in error control for noncoherent random network coding; such codes are also referred to as constant-dimension codes (CDCs) [4].

CDCs have been receiving a lot of attention in the literature. In addition to the subspace metric defined in [4], an injection metric was defined for adversarial channels in [5]. Although the maximum cardinality of a CDC with a given minimum distance is still unknown, many bounds and constructions have been derived in the literature (see, for example, [4], [6]), and CDCs have been shown to be asymptotically optimal subspace codes [7]. CDCs are also closely related to rank metric codes. First, CDCs can be constructed by lifting rank metric codes [8], which preserves the distance. Also, it was recently shown that CDCs are closely related to constant rank codes [9]. The maximum cardinality of a code with a given minimum rank distance was determined in [10]–[12]. We refer to codes with maximum cardinality as maximum rank distance (MRD) codes, and the class of linear MRD codes proposed independently in [10]–[12] as Gabidulin codes henceforth. In particular, liftings of Gabidulin codes are nearly optimal CDCs [4] and have low-complexity bounded subspace distance decoders [4], [8]. Although no low-complexity algorithm has been specifically proposed for bounded injection distance decoders in the literature, a bounded injection distance decoder for a CDC can be easily designed from a bounded subspace distance decoder for the same code.

One critical aspect that has received little attention in the literature is the error performance of bounded distance decoders for CDCs. Given a received word, a bounded distance decoder either declares a failure or finds a codeword within a predetermined radius of the received word. In the latter case, when the codeword produced by the bounded distance decoder is not the sent codeword, a decoder error occurs. In many applications, a decoder error is more detrimental than a decoding failure; this is indeed the case for random network coding as a decoding failure can be remedied in two ways. First, when a receiver encounters a decoding failure due to insufficient dimension, it is possible for the receiver to collect more packets from the same transmission until a decoding becomes possible. Of course, if this remedy fails, the receiver can request a retransmission. Thus the decoder error probability (DEP) is a crucial parameter for the error performance of both bounded distance decoders and the codes used in the transmission.

In this paper, we investigate the DEP of bounded distance decoders for CDCs, with a focus on those obtained by lifting rank metric codes. The main contributions of this paper are:

- Since the projective space is not an association scheme, its geometric properties are different from those that constitute association schemes. Thus, we first establish some fundamental geometric properties of the projective space. In particular, we focus on properties of balls with subspace and injection radii. For both metrics, we derive bounds on the union of spheres, and show that the volume

978-1-4244-4313-0/09/$25.00 ©2009 IEEE

of the intersection of two spheres (and hence balls) depends on only the two radii as well as the distance between and the dimensions of the two centers. These geometric properties not only are critical to our analysis of DEP for CDCs, but also open doors for future research on subspace codes.

- Using the geometric properties described above, we consider bounded distance decoders in both subspace and injection metrics and derive analytical expressions of their DEPs for CDCs over a symmetric operator channel, which ultimately depend on their distance distributions.
- Finally, we focus on CDCs obtained by lifting rank metric codes since their distance distributions are known, and obtain two important results. First, we obtain asymptotically tight upper bounds on the DEPs of bounded distance decoders in both metrics; the upper bounds decrease exponentially with the square of the minimum distance. Second, we show that DEP for KK codes is the highest up to a scalar among all CDCs obtained by lifting rank metric codes. Our study of the DEP of liftings of rank metric codes is based on constant-rank codes (CRCs) [9], a class of rank metric codes closely related to CDCs.

We note that most proofs are omitted due to space restrictions, and can be found in [13].

II. Preliminaries

A. Rank metric codes

The set $\mathrm{GF}(q)^{m\times n}$ of $m\times n$ matrices over $\mathrm{GF}(q)$, endowed with the rank distance $d_{\mathrm{R}}(\mathbf{X},\mathbf{Y}) \stackrel{\mathrm{def}}{=} \mathrm{rk}(\mathbf{X}-\mathbf{Y})$, constitutes a metric association scheme [10].

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 [10]–[12] 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 maximum rank distance (MRD) codes, and the subclass of linear MRD codes introduced independently in [10]–[12] 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 [10], [11] and is denoted as $M(q,m,n,d,r)$. In particular, we have $M(q,m,n,d,d) = \begin{bmatrix} n \\ d \end{bmatrix}(q^m-1)$, where the term $\begin{bmatrix} n \\ d \end{bmatrix} = \prod_{i=0}^{d-1} \frac{q^n-q^i}{q^d-q^i}$ is the Gaussian binomial, which satisfies

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

for all $0 \leq d \leq n$ [14], where $K_q = \prod_{j=1}^{\infty}(1-q^{-j})$.

A constant-rank code (CRC) is a rank metric code whose codewords have the same rank [9]. 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 [9]. 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 $d \leq r$,

$$A_{\mathrm{R}}(q,m,n,d,r) \leq \begin{bmatrix} n \\ r \end{bmatrix} \alpha(m, r-d+1), \tag{2}$$

where $\alpha(m,u) = \prod_{i=0}^{u-1}(q^m-q^i)$.

B. Constant-dimension codes

We refer to the set of all subspaces of $\mathrm{GF}(q)^n$ with dimension r as the Grassmannian $E_r(q,n)$, and we also refer to $E(q,n) = \bigcup_{r=0}^{n} E_r(q,n)$ as the projective space. For $U,V \in E(q,n)$, the subspace metric [4] $d_{\mathrm{S}}(U,V) \stackrel{\mathrm{def}}{=} \dim(U+V) - \dim(U\cap V)$ and the injection metric [5] $d_{\mathrm{I}}(U,V) \stackrel{\mathrm{def}}{=} \frac{1}{2}d_{\mathrm{S}}(U,V) + \frac{1}{2}|\dim(U) - \dim(V)|$ are both metrics over $E(q,n)$. Furthermore, $E_r(q,n)$ endowed with the injection metric forms a metric association scheme [15], whose intersection numbers $J_{\mathrm{C}}(r,u,s,d)$ were determined in [7]. The intersection numbers represent the volume of the intersection of two spheres in the Grassmannian with radii u and s and distance d between their respective centers.

Although the projective space $E(q,n)$ does not form an association scheme, some geometric results have been derived and are reviewed below. The number of subspaces with dimension s at subspace distance d from a subspace with dimension r, denoted as $N_{\mathrm{S}}(r,s,d)$, is $q^{u(d-u)}\begin{bmatrix} r \\ u \end{bmatrix}\begin{bmatrix} n-r \\ d-u \end{bmatrix}$ when $u = \frac{r+d-s}{2}$ is an integer, or 0 otherwise [7]. The number of subspaces with dimension s at injection distance d from a subspace with dimension r is given by $N_{\mathrm{I}}(r,s,d) = N_{\mathrm{S}}(r,s,2d-|r-s|)$ [7]. Hence $N_{\mathrm{I}}(r,s,d) = q^{d(d-\delta)}\begin{bmatrix} \omega \\ d \end{bmatrix}\begin{bmatrix} n-\omega \\ d-\delta \end{bmatrix}$, where $\delta = |r-s|$ and $\omega = r$ if $r \geq s$ and $\omega = n-r$ otherwise.

A subset of $E_r(q,n)$ is called a constant-dimension code (CDC). CDCs are related to rank metric codes through CRCs or through the lifting operation [8], described below. The row space of a matrix $\mathbf{C}$ is denoted as $R(\mathbf{C})$. The lifting of $\mathbf{C} \in \mathrm{GF}(q)^{r\times(n-r)}$ is defined as $I(\mathbf{C}) = R(\mathbf{I}_r|\mathbf{C}) \in E_r(q,n)$. For all $\mathbf{C},\mathbf{D} \in \mathrm{GF}(q)^{r\times(n-r)}$, we have $d_{\mathrm{I}}(I(\mathbf{C}), I(\mathbf{D})) = d_{\mathrm{R}}(\mathbf{C},\mathbf{D})$ [8]. Therefore, the injection distance distribution of the lifting is equal to the rank distance distribution of the original code. Liftings of MRD codes were introduced in [8]; in particular, the lifting of a Gabidulin code is referred to as a KK code.

III. Geometric properties of the projective space

In this section, we establish some fundamental geometric properties of balls in $E(q,n)$ with subspace or injection radii, which will be critical to our analysis of DEP for CDCs.

First, we study the properties of balls with subspace radii. For all $A \in E_a(q,n), B \in E_b(q,n)$, we denote the number of subspaces with dimension c in the intersection of two spheres with subspace radii u and s centered at A and B, respectively, as $J_{\mathrm{S}}(u,s;A,B,c) = |\{C \in E_c(q,n) : d_{\mathrm{S}}(A,C) = u, d_{\mathrm{S}}(B,C) = s\}|$.

Theorem 1: For all $A \in E_a(q,n), B \in E_b(q,n)$ with $d_{\mathrm{S}}(A,B) = w$, $J_{\mathrm{S}}(u,s;A,B,c)$ depends on A and B only through a, b, and w. We thus have $J_{\mathrm{S}}(u,s;A,B,c) = J_{\mathrm{S}}(u,s,w;a,b,c)$.

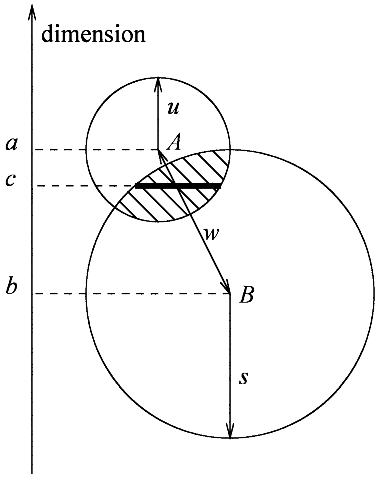

Fig. 1. Intersection of balls in the subspace metric

The intersection of spheres with subspace radii is related to the volume of these spheres in Corollary 1 below.

Corollary 1: For all parameter values,

$$N_{\mathrm{S}}(a,b,w)J_{\mathrm{S}}(u,s,w;a,b,c) = N_{\mathrm{S}}(a,c,u)J_{\mathrm{S}}(w,s,u;a,c,b), \tag{3}$$

$$\sum_{u=0}^{n} J_{\mathrm{S}}(u,s,w;a,b,c) = N_{\mathrm{S}}(b,c,s). \tag{4}$$

The set of all subspaces of $\mathrm{GF}(q)^n$, endowed with the subspace (or injection) metric, does not form an association scheme. Indeed, the intersection of two spheres does not only depend on the radii of the spheres and on the distance between their respective centers. Theorem 1 is a fundamental property of spheres in the subspace metric, as it shows that the intersection only depends on the parameters mentioned above and the dimension of the centers.

Theorem 1 also implies that the intersection of two balls in $E(q,n)$ with subspace radii, represented as the shaded area in Figure 1, only depends on a, b, u, s, and w. Furthermore, for all c, the number of subspaces with dimension c in the intersection, represented as the black line in Figure 1, only depends on the parameters above and c.

Although the value of $J_{\mathrm{S}}(u,s,w;a,b,c)$ is unknown in general, we remark that for $a=b=c$, $J_{\mathrm{S}}(2u,2s,2w;a,a,a) = J_{\mathrm{C}}(a,u,s,w)$, the intersection number of the association scheme for $E_a(q,n)$. We also determine its value when $w = u+s$ below.

Proposition 1: When $w = u+s$, we have

$$J_{\mathrm{S}}(u,s,u+s;a,b,c) = \begin{bmatrix} \frac{a-b+u+s}{2} \\ \frac{c-b+s}{2} \end{bmatrix} \begin{bmatrix} \frac{b-a+u+s}{2} \\ \frac{c-a+u}{2} \end{bmatrix}. \tag{5}$$

It is easy to show that $J_{\mathrm{S}}(u,s,u+s;a,b,c) = 0$ when $u > \min\{a+c, a+2b-c\}$, $s > \min\{b+c, 2a+b-c\}$, or $u+s > \min\{a+b,n\}$.

We now study balls with injection radii. We first prove a technical upper bound on the volume of spheres, which will be instrumental in Section IV-B.

Lemma 1: For all r and s, let $\delta = |r-s|$ and $\omega = r$ if $r \geq s$ and $\omega = n-r$ otherwise. Then for all $t \leq \min\left\{r+s, \frac{n}{2}\right\}$, $\sum_{d=0}^{t} N_{\mathrm{I}}(r,s,d) < K_q^{-2} N_q q^{g(t)}$, where $g(d) = d(n+\delta-d) - \delta(n-\omega+\delta)$ and $N_q = \sum_{i=0}^{\infty} q^{-i^2}$.

For all $A \in E_a(q,n), B \in E_b(q,n)$, we denote $J_{\mathrm{I}}(u,s;A,B,c) = |\{C \in E_c(q,n) : d_{\mathrm{I}}(A,C) = u, d_{\mathrm{I}}(B,C) = s\}|$. Proposition 2 below is the counterpart of Theorem 1 for the injection metric.

Proposition 2: For all $A \in E_a(q,n), B \in E_b(q,n)$ with $d_{\mathrm{I}}(A,B) = w$, we have $J_{\mathrm{I}}(u,s;A,B,c) = J_{\mathrm{S}}(2u-|a-c|, 2s-|b-c|, 2w-|a-b|;a,b,c) = J_{\mathrm{I}}(u,s,w;a,b,c)$.

Corollary 2: For all parameter values,

$$N_{\mathrm{I}}(a,b,w)J_{\mathrm{I}}(u,s,w;a,b,c) = N_{\mathrm{I}}(a,c,u)J_{\mathrm{I}}(w,s,u;a,c,b), \tag{6}$$

$$\sum_{u=0}^{n} J_{\mathrm{I}}(u,s,w;a,b,c) = N_{\mathrm{I}}(b,c,s). \tag{7}$$

Although the value of $J_{\mathrm{I}}(u,s,w;a,b,c)$ is unknown in general, we have $J_{\mathrm{I}}(u,s,w;a,a,a) = J_{\mathrm{C}}(a,u,s,w)$. We also determine a special value below.

Proposition 3: For all u and s, $J_{\mathrm{I}}(u,s,w;a,b,c) = 0$ for $w > u+s-\frac{|a-c|+|b-c|-|a-b|}{2}$ and

$$J_{\mathrm{I}}\left(u,s,u+s-\frac{|a-c|+|b-c|-|a-b|}{2};a,b,c\right) = \begin{bmatrix} u+s-\frac{b-a+|a-c|+|b-c|}{2} \\ s-\frac{b-c+|b-c|}{2} \end{bmatrix} \begin{bmatrix} u+s-\frac{a-b+|a-c|+|b-c|}{2} \\ u-\frac{a-c+|a-c|}{2} \end{bmatrix}.$$

IV. DEP of Bounded Distance Decoders for CDCs over a Symmetric Operator Channel

A. DEP of bounded subspace distance decoder

We study the DEP of a bounded subspace distance decoder in $E(q,n)$ for a CDC in $E_r(q,n)$ over a *symmetric operator channel*, defined below. Without loss of generality, we assume $2r \leq n$ as in [4]. An operator channel is a channel where the inputs and outputs are subspaces in $E(q,n)$. As assumed in [4], the channel may erase some dimensions of the transmitted subspace as well as inject some erroneous dimensions. We refer to these as erasures and errors, respectively. If the input has dimension r and ϵ errors and ρ erasures occur, the output has dimension $v = r - \epsilon + \rho$ and is at subspace distance $u = \epsilon + \rho$ from the input. We refer to an operator channel as a *symmetric operator channel* when all outputs corresponding to ϵ errors and ρ erasures are equiprobable. Since the dimension of the output and its subspace distance from the transmitted subspace are both determined by ϵ and ρ, a symmetric operator channel implies that all outputs with the same dimension and at the same subspace distance from the input are equiprobable, and vice versa.

Let $\mathcal{C} \subseteq E_r(q,n)$ be a CDC with minimum subspace distance $2d$, and given any subspaces at subspace distance up to $d-1$ from the codeword, a bounded distance decoder will produce the codeword. Thus, the DEP of the bounded distance decoder depends on both ϵ and ρ, or equivalently on both u and v. The bounded subspace distance decoder will result in a failure when $v < r-d+1$ or $v > r+d-1$. The decoder decodes correctly if and only if $u \leq d-1$, and returns a failure for $u = d$. The DEP $P_{\rm S}(C,u,v)$ when $u \geq d+1$ and $r-d+1 \leq v \leq r+d-1$ is based on the distance distribution of the code, denoted as $A_w(C) = |\{D \in \mathcal{C} : d_{\rm I}(D,C) = w\}| = |\{D \in \mathcal{C} : d_{\rm S}(D,C) = 2w\}|$.

Proposition 4: When $u \geq d+1$ and $r-d+1 \leq v \leq r+d-1$, the DEP of a bounded subspace distance decoder for a CDC in $E_r(q,n)$ with minimum subspace distance $2d$ over a symmetric operator channel is given by

$$P_{\rm S}(C,u,v) = \frac{1}{N_{\rm S}(r,v,u)} \sum_{w=d}^{r} A_w(C) \cdot \sum_{s=0}^{d-1} J_{\rm S}(u,s,2w;r,r,v). \tag{8}$$

Furthermore, if the CDC is the lifting of a rank metric code, then

$$\begin{aligned} P_{\rm S}(I(\mathbf{C}),u,v) &\leq \frac{1}{N_{\rm S}(r,v,u)} \sum_{w=d}^{r} \begin{bmatrix} r \\ w \end{bmatrix} \alpha(n-r,w-d+1) \\ &\quad \cdot \sum_{s=0}^{d-1} J_{\rm S}(u,s,2w;r,r,v) & (9) \\ &< K_q^{-3} P_q q^{-\tau(n-r-v+\tau)}, & (10) \end{aligned}$$

where $\tau = \frac{d-1+v-r}{2}$ and $P_q = \sum_{i=0}^{\infty} q^{-\frac{3}{4}i^2}$.

Proof: We have $P_{\rm S}(C,u,v) = \frac{D(C,u,v)}{N_{\rm S}(r,v,u)}$, where $D(C,u,v)$ is the number of decodable subspaces with dimension v and at subspace distance u from C. For a codeword C' at subspace distance $2w$ from C, there are exactly $\sum_{s=0}^{d-1} J_{\rm S}(u,s,2w;r,r,v)$ subspaces with dimension v, at distance u from C, and at distance $\leq d-1$ from C' by Theorem 1. Summing for all C', we obtain (8).

Let $I(\mathcal{C})$ be the lifting of a rank metric code $\mathcal{C}$ in ${\rm GF}(q)^{r\times(n-r)}$. For $\mathbf{C} \in \mathcal{C}$, $\{I(\mathbf{D}-\mathbf{C}) : \mathbf{D} \in \mathcal{C}, d_{\rm R}(\mathbf{D},\mathbf{C}) = w\}$ is the lifting of a CRC in ${\rm GF}(q)^{r\times(n-r)}$ with minimum rank distance at least d and rank w, and hence $A_w(I(\mathbf{C})) \leq A_{\rm R}(q,n-r,r,d,w) \leq \begin{bmatrix} r \\ w \end{bmatrix} \alpha(n-r,w-d+1)$ by (2), which leads to (9). By (1),

$$A_w(I(\mathbf{C})) < K_q^{-1} q^{-(n-r)(d-1)} N_{\rm S}(r,r,2w). \tag{11}$$

We obtain

$$\begin{aligned} &P_{\rm S}(I(\mathbf{C}),u,v) \\ &= \sum_{w=d}^{r} A_w(I(\mathbf{C})) \sum_{s=0}^{d-1} \frac{J_{\rm S}(2w,s,u;r,v,r)}{N_{\rm S}(r,r,2w)} & (12) \\ &< K_q^{-1} q^{-(n-r)(d-1)} \sum_{w=d}^{r} \sum_{s=0}^{d-1} J_{\rm S}(2w,s,u;r,v,r) & (13) \\ &\leq K_q^{-1} q^{-(n-r)(d-1)} \sum_{s=0}^{d-1} N_{\rm S}(v,r,s) & (14) \\ &< K_q^{-3} P_q q^{\frac{d-1}{2}\left(2r-n-\frac{d-1}{2}\right)-\frac{v-r}{2}\left(n-2r-\frac{v-r}{2}\right)}, & (15) \end{aligned}$$

where (12), (13), (14), and (15) follow (3), (11), (4), and [7], respectively. ■

We remark that the bound in (10) is trivial for $v = r-d+1$ or $r = \frac{n}{2}$ and $v = \frac{n}{2}-d+1$. This is due to the fact that CDCs in $E_r(q,n)$ with minimum subspace distance $2d$ and maximum cardinality produce asymptotically tight packings of $E_{r-d+1}(q,n)$, and CDCs in $E_{\frac{n}{2}}(q,n)$ with maximum cardinality produce asymptotically tight packings of $E_{\frac{n}{2}-d+1}(q,n)$.

We now show that liftings of MRD codes have the highest DEP among all liftings up to a scalar in all nontrivial cases. We denote the DEP of the lifting of an MRD code in ${\rm GF}(q)^{r\times(n-r)}$ with minimum rank distance d as $P_{\rm S,MRD}(u,v)$.

Corollary 3: Let $\mathcal{C}$ be any rank metric code in ${\rm GF}(q)^{r\times(n-r)}$ $(r \leq n-r)$ with minimum rank distance d and let $\mathbf{C} \in \mathcal{C}$. Then if $q > 2$, $r < n-r$, or $d \neq n-r-1$, $P_{\rm S}(I(\mathbf{C}),u,v) < H_q P_{\rm S,MRD}(u,v)$, where $H_2 = 3.5$ and $H_q = \frac{q-1}{q-2}$ for $q > 2$.

If the probability that the received subspace is at subspace distance u from the sent codeword decreases rapidly with u, then the overall DEP is dominated by $P_{\rm S}(C,d+1,v)$. Proposition 5 below determines this value, and shows that it asymptotically reaches the upper bound in (10) for liftings of MRD codes.

Proposition 5: The DEP of a CDC in $E_r(q,n)$ with minimum subspace distance $2d$ using a bounded subspace distance decoder over a symmetric operator channel, provided the received subspace is at subspace distance $d+1$ from the sent codeword, is given by

$$P_{\rm S}(C,d+1,v) = q^{-(d-\tau)(\tau+1)} \frac{\begin{bmatrix} d \\ \tau \end{bmatrix} \begin{bmatrix} d \\ \tau+1 \end{bmatrix}}{\begin{bmatrix} r \\ d-\tau \end{bmatrix} \begin{bmatrix} n-r \\ \tau+1 \end{bmatrix}} A_d(C). \tag{16}$$

In particular, the DEP of the lifting of an MRD code satisfies $P_{\rm S,MRD}(d+1,v) > K_q^2 q^{-\tau(n-r-v+\tau)}$.

Proposition 5 and (10) indicate that when the received subspace has dimension $v \leq r$, the DEP of a lifting of an MRD code in ${\rm GF}(q)^{r\times(n-r)}$ with minimum rank distance d is on the same order of that of its puncturing in ${\rm GF}(q)^{v\times(n-r)}$ with minimum distance $d+v-r$.

We remark that on a symmetric operator channel, all outputs with the same dimension and at the same subspace distance from the input are equiprobable. Note that if we assume that all channel outputs with the same distance to the transmitted subspace are equiprobable, it implies a symmetric operator channel and thus the results derived above for the symmetric operator channel still hold.

B. DEP of bounded injection decoder

We now study the DEP of a CDC using a bounded injection decoder over a symmetric operator channel. Again since the dimension of the output and its injection distance from the transmitted subspace are both determined by ϵ and ρ, a symmetric operator channel implies that all outputs with the same dimension $v = r+\epsilon-\rho$ and at the same injection distance $\mu = \max\{\epsilon,\rho\}$ from the input are equiprobable, and vice versa.

The DEP of a bounded distance decoder depends on both μ and v. The code has minimum injection distance d and can correct subspaces at injection distance up to $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ from the codeword. As a result, the bounded injection distance decoder produces a failure if $v < r - t$ or $v > r + t$. The decoder decodes correctly if and only if $\mu \leq t$, and returns a failure for $t < \mu < d - t$. We determine below the DEP $P_{\rm I}(C, \mu, v)$ for $\mu \geq d - t$.

Proposition 6: The DEP of using a bounded injection distance decoder for a CDC in $E_r(q, n)$ with minimum injection distance d over a symmetric operator channel is given by $P_{\rm I}(C, \mu, v) = 0$ for $\mu < d - t + |r - v|$ and

$$P_{\rm I}(C, \mu, v) = \frac{1}{N_{\rm I}(r, v, \mu)} \sum_{w=d}^{r} A_w(C) \cdot \sum_{s=0}^{t} J_{\rm I}(\mu, s, w; r, r, v) \qquad (17)$$

otherwise. Furthermore, if the CDC is the lifting of a rank metric code, then

$$\begin{aligned} P_{\rm I}(I(\mathbf{C}), \mu, v) &\leq \frac{1}{N_{\rm I}(r, v, \mu)} \sum_{w=d}^{r} \begin{bmatrix} r \\ w \end{bmatrix} \alpha(n - r, w - d + 1) \\ &\quad \cdot \sum_{s=0}^{t} J_{\rm I}(\mu, s, w; r, r, v) \qquad (18) \\ &< K_q^{-3} N_q q^{-t(n-2r-\delta+t)-\delta(n-\omega+\delta)}, \qquad (19) \end{aligned}$$

where $\delta = |r - v|$ and $\omega = v$ if $v \geq r$ and $\omega = n - v$ otherwise.

We remark that $\mu \geq d - t + |r - v|$ is equivalent to $\min\{\epsilon, \rho\} \geq d - t$. Therefore, Proposition 6 indicates that both $d - t$ errors and $d - t$ erasures have to occur for the bounded injection distance decoder to decode erroneously.

We show below that liftings of MRD codes have the highest maximum decoder error probability up to a scalar for nontrivial cases. We denote the DEP of the lifting of an MRD code in $\mathrm{GF}(q)^{r \times (n-r)}$ with minimum rank distance d as $P_{\rm I,MRD}(\mu, v)$.

Corollary 4: Let $\mathcal{C}$ be a rank metric code in $\mathrm{GF}(q)^{r \times (n-r)}$ ($r \leq n - r$) with minimum rank distance d and let $\mathbf{C} \in \mathcal{C}$. Then if $q > 2$ or $r < n - r$ or $d \neq n - r - 1$, $P_{\rm I}(I(\mathbf{C}), \mu, v) < H_q P_{\rm I,MRD}(\mu, v)$, where $H_2 = 3.5$ and $H_q = \frac{q-1}{q-2}$ for $q > 2$.

If the probability that the received subspace is at injection distance μ from the sent codeword decreases rapidly with μ, then the overall DEP is dominated by $P_{\rm I}(C, d - t + \delta, v)$. Proposition 7 below determines this value, and shows that it asymptotically reaches the upper bound in (19) for liftings of MRD codes.

Proposition 7: The DEP of a CDC in $E_r(q, n)$ with minimum injection distance d using a bounded injection distance decoder over a symmetric operator channel provided the received subspace is at injection distance $\mu = d - t + \delta$ from the sent codeword is given by

$$P_{\rm I}(C, d{-}t{+}\delta, v) = q^{-(d-t)(d-t+\delta)} \frac{\begin{bmatrix} d \\ t - \frac{\delta - r + v}{2} \end{bmatrix} \begin{bmatrix} d \\ t - \frac{\delta + r - v}{2} \end{bmatrix}}{\begin{bmatrix} \omega \\ d - t + \delta \end{bmatrix} \begin{bmatrix} n - \omega \\ d - t \end{bmatrix}} A_d(C). \qquad (20)$$

In particular, the DEP of the lifting of an MRD code satisfies $P_{\rm I,MRD}(d - t + \delta, v) > K_q^2 q^{-t(n-2r-\delta+t)-\delta(n-\omega+\delta)}$ for $v \geq r$.

Let $\mathcal{C} \subseteq E_r(q, n)$ be a CDC with minimum injection distance d, and let $U \in E(q, n)$ be at injection distance at most t from $C \in \mathcal{C}$, the transmitted subspace. Then U is at subspace distance $\leq 2t \leq d - 1$ from C. Therefore, any subspace that is decodable by a bounded injection decoder can also be decoded by a bounded subspace decoder for $\mathcal{C}$. As a result, a bounded injection distance decoder can hence be simply designed using a bounded subspace decoder.

Also, a bounded subspace distance decoder for a CDC can hence correct more patterns of errors and erasures than a bounded injection distance for the same code. By comparing the approximations in Propositions 5 and 7, it can be shown that for KK codes, the DEP of the bounded subspace distance is always greater than the DEP of the bounded injection distance decoder. The only situation where they are on the same order is for $d = 2t = 1$ and $v = r$, i.e., the received subspace is in $E_r(q, n)$, where both decoders decode exactly the same subspaces. There is hence a clear tradeoff between error correction capability and decoder error probability.

References

[1] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Info. Theory*, vol. 52, no. 10, pp. 4413–4430, October 2006.

[2] C. Fragouli and E. Soljanin, *Network Coding Fundamentals*. Now Publishers Inc, 2007.

[3] T. Ho and D. S. Lun, *Network coding: an introduction*. New York NY: Cambridge University Press, 2008.

[4] 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.

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

[6] V. Skachek, "Recursive code construction for random networks," 2008, available at http://arxiv.org/abs/0806.3650v1.

[7] M. Gadouleau and Z. Yan, "Packing and covering properties of subspace codes," *submitted to IEEE Trans. Info. Theory*, 2008, available at http://arxiv.org/abs/0811.4163.

[8] 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, September 2008.

[9] M. Gadouleau and Z. Yan, "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.

[10] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory A*, vol. 25, no. 3, pp. 226–241, November 1978.

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

[12] 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.

[13] M. Gadouleau and Z. Yan, "On the decoder error probability of rank metric codes and constant-dimension codes," *submitted to IEEE Trans. Info. Theory*, 2009, available at http://arxiv.org/abs/0812.2379.

[14] ——, "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] P. Delsarte, "Association schemes and *t*-designs in regular semilattices," *Journal of Combinatorial Theory A*, vol. 20, no. 2, pp. 230–243, March 1976.