Construction and Covering Properties of 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 investigated for noncoherent error correction in random network coding. The maximum cardinality of CDCs with given minimum distance and how to construct optimal CDCs are both open problems, although CDCs obtained by lifting Gabidulin codes, referred to as KK codes, are nearly optimal. In this paper, we first construct a new class of CDCs based on KK codes, referred to as augmented KK codes, whose cardinalities are greater than previously proposed CDCs. We then propose a low-complexity decoding algorithm for our augmented KK codes using that for KK codes. Our decoding algorithm corrects more errors than a bounded subspace distance decoder by taking advantage of the structure of our augmented KK codes. In the rest of the paper we investigate the covering properties of CDCs. We first derive bounds on the minimum cardinality of a CDC with a given covering radius and then determine the asymptotic behavior of this quantity. Moreover, we show that liftings of rank metric codes have the highest possible covering radius, and hence liftings of rank metric codes are not optimal packing CDCs. Finally, we construct good covering CDCs by permuting liftings of rank metric codes.**

I. Introduction

Constant-dimension codes (CDCs) are codes defined in the Grassmannians of a vector space over a finite field. Since error correction in noncoherent random network coding can be treated as a coding problem where codewords are linear subspaces, CDCs have attracted a lot of attention recently (see, for example, [1]–[5]). Two metrics have been defined for CDCs based on different channel models. A subspace metric is defined for correcting errors and erasures that typically occur on the network [1]; an injection metric is also proposed for an adversarial channel model, where an adversary has knowledge of all packets transmitted and tries to disrupt the communication by injecting properly chosen packets [2]. For CDCs, the subspace distance spectrum and the injection distance spectrum are equivalent up to a scalar, and hence either metric can be used for CDCs.

Construction of CDCs has received growing attention in the literature recently. In [1], a Singleton bound for CDCs and a family of codes were proposed, which are nearly Singleton-bound-achieving and referred to as KK codes henceforth. A multi-step construction of CDCs was proposed in [3], and we call these codes Skachek codes; Skachek codes have larger cardinalities than KK codes in some scenarios, and reduce to KK codes otherwise. Further constructions for small parameter values were given in [4] and the Johnson bound for CDCs was derived in [5]. Although the CDCs in [5] are optimal in the sense of the Johnson bound, they exist in some special cases only. Despite these previous works, the maximum cardinality of a CDC with a given minimum distance and how to construct optimal CDCs remain open problems.

Although the packing properties of CDCs were investigated in [1], [3]–[5], the covering properties of CDCs have received little attention in the literature. Covering properties are significant for error control codes, and the covering radius is a basic geometric parameter of a code [6]. For instance, if the minimum distance decoding is used, then the covering radius is the maximum weight of a correctable error vector [7]. The covering radius is also crucial for code design: if the covering radius is no less than the minimum distance of a code, then there exists a supercode with the same minimum distance and greater cardinality.

This paper has two main contributions. First, we introduce a new class of CDCs, referred to as augmented KK codes. The cardinalities of our augmented KK codes are **always greater** than those of KK codes, and in **most** cases the cardinalities of our augmented KK code are greater than those of Skachek codes. Furthermore, we propose an efficient decoding algorithm for our augmented KK codes using the bounded subspace distance decoding algorithm in [1]; our decoding algorithm corrects more errors than a bounded subspace distance decoder. Second, we investigate the covering properties of CDCs. We first derive some key geometric results for Grassmannians. Using these results, we derive upper and lower bounds on the minimum cardinality of a CDC with a given covering radius. Since these bounds are asymptotically tight, we also determine the asymptotic behavior of the minimum cardinality of a CDC with a given covering radius. Although liftings of rank metric codes can be used to construct packing CDCs that are optimal up to a scalar (KK codes, for example), we show that all liftings of rank metric codes have the greatest covering radius possible; our result implies that liftings of rank metric codes are **not optimal** packing CDCs. We finally construct good covering CDCs by permuting liftings of rank metric codes.

The rest of the paper is organized as follows. To be self-contained, Section II reviews some necessary background. In Section III, we present our augmented KK codes and a decoding algorithm for these codes. In Section IV, we investigate the covering properties of CDCs.

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

Due to space limitations, all proofs are omitted and are available in [8].

II. Preliminaries

We refer to the set of all subspaces of $\mathrm{GF}(q)^n$ with dimension r as the Grassmannian of dimension r and denote it as $E_r(q,n)$; we refer to $E(q,n)=\bigcup_{r=0}^{n} E_r(q,n)$ as the projective space. For $U,V\in E(q,n)$, both the *subspace metric* [1, (3)] $d_{\mathrm{s}}(U,V)\stackrel{\text{def}}{=}2\dim(U+V)-\dim(U)-\dim(V)$ and *injection metric* [2, Def. 1] $d_{\mathrm{i}}(U,V)\stackrel{\text{def}}{=}\dim(U+V)-\min\{\dim(U),\dim(V)\}$ are metrics over $E(q,n)$. A *subspace code* is a nonempty subset of $E(q,n)$. The minimum subspace (respectively, injection) distance of a subspace code is the minimum subspace (respectively, injection) distance over all pairs of distinct codewords.

The Grassmannian $E_r(q,n)$ endowed with both the subspace and injection metrics forms an association scheme [1], [9]. For all $U,V\in E_r(q,n)$, $d_{\mathrm{s}}(U,V)=2d_{\mathrm{i}}(U,V)$ and the injection distance provides a natural distance spectrum, i.e., $0\le d_{\mathrm{i}}(U,V)\le r$. We have $|E_r(q,n)|=\begin{bmatrix}n\\r\end{bmatrix}$, where $\begin{bmatrix}n\\r\end{bmatrix}=\prod_{i=0}^{r-1}\frac{q^n-q^i}{q^r-q^i}$ is the Gaussian binomial [10], which satisfies

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

for all $0\le r\le n$, where $K_q=\prod_{j=1}^{\infty}(1-q^{-j})$ [11]. We denote the number of subspaces in $E_r(q,n)$ at distance d from a given subspace as $N_{\mathrm{c}}(d)=q^{d^2}\begin{bmatrix}r\\d\end{bmatrix}\begin{bmatrix}n-r\\d\end{bmatrix}$ [1], and denote the volume of a ball in $E_r(q,n)$ of radius t as $V_{\mathrm{c}}(t)=\sum_{d=0}^{t}N_{\mathrm{c}}(d)$.

A constant-dimension code is a subset of $E_r(q,n)$, and is thus a subspace code whose codewords have the same dimension. We denote the **maximum** cardinality of a CDC in $E_r(q,n)$ with minimum distance d as $A_{\mathrm{c}}(q,n,r,d)$. Constructions of CDCs and bounds on $A_{\mathrm{c}}(q,n,r,d)$ have been given in [1], [3]–[5], [12]. In particular, $A_{\mathrm{c}}(q,n,r,1)=\begin{bmatrix}n\\r\end{bmatrix}$ and it is shown [3], [5] for $r\le\lfloor\frac{n}{2}\rfloor$ and $2\le d\le r$,

$$\frac{q^{n(r-d+1)}-q^{(r+l)(r-d+1)}}{q^{r(r-d+1)}-1}\le A_{\mathrm{c}}(q,n,r,d)\le\frac{\begin{bmatrix}n\\r-d+1\end{bmatrix}}{\begin{bmatrix}r\\r-d+1\end{bmatrix}}, \tag{2}$$

where $l\equiv n \bmod r$. We denote the lower bound on $A_{\mathrm{c}}(q,n,r,d)$ in (2) as $L(q,n,r,d)$. The lower bound is due to the class of codes proposed by Skachek [3], and we refer to these codes as Skachek codes.

CDCs are closely related to rank metric codes [13]–[15], which can be viewed as sets of matrices in $\mathrm{GF}(q)^{m\times n}$. The rank distance between two matrices $\mathbf{C},\mathbf{D}\in\mathrm{GF}(q)^{m\times n}$ is defined as $d_{\mathrm{R}}(\mathbf{C},\mathbf{D})\stackrel{\text{def}}{=}\mathrm{rk}(\mathbf{C}-\mathbf{D})$. The maximum cardinality of a rank metric code in $\mathrm{GF}(q)^{m\times n}$ with minimum distance d is given by $\min\{q^{m(n-d+1)},q^{n(m-d+1)}\}$ and codes that achieve this cardinality are referred to as maximum rank distance (MRD) codes. In this paper, we shall only consider either MRD codes introduced independently in [13]–[15] for $n\le m$, or their transpose codes for $n>m$. The minimum cardinality $K_{\mathrm{R}}(q^m,n,\rho)$ of a code in $\mathrm{GF}(q)^{m\times n}$ with rank covering radius ρ is studied in [16], [17] and satisfies $K_{\mathrm{R}}(q^m,n,\rho)=K_{\mathrm{R}}(q^n,m,\rho)$ [16].

CDCs are related to rank metric codes through the lifting operation [18]. Denoting the row space of a matrix $\mathbf{M}$ as $R(\mathbf{M})$, the lifting of $\mathbf{C}\in\mathrm{GF}(q)^{r\times(n-r)}$ is denoted 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 $d_{\mathrm{i}}(I(\mathbf{C}),I(\mathbf{D}))=d_{\mathrm{R}}(\mathbf{C},\mathbf{D})$ [18]. A KK code in $E_r(q,n)$ with minimum injection distance d is the lifting $I(\mathcal{C})\subseteq E_r(q,n)$ of an MRD code $\mathcal{C}\subseteq\mathrm{GF}(q)^{r\times(n-r)}$ with minimum rank distance d and cardinality $\min\{q^{(n-r)(r-d+1)},q^{r(n-r-d+1)}\}$. An efficient bounded subspace distance decoding algorithm for KK codes was also given in [1]. Although the algorithm was presented for $r\le\frac{n}{2}$, it can be easily generalized to all r.

III. Construction of CDCs

In this section, we construct a new class of CDCs, referred to as augmented KK codes, which properly contain KK codes. We also show that the cardinalities of our augmented KK codes are greater than those of Skachek codes in most cases. Furthermore, we propose a low-complexity decoder for our augmented KK codes based on the bounded subspace distance decoder in [1]. Since dual CDCs preserve the distance, we assume $r\le\frac{n}{2}$ without loss of generality.

A. Augmented KK codes

Our augmented KK code is so named because it has a layered structure and the first layer is simply a KK code. We denote a KK code in $E_r(q,n)$ with minimum injection distance d ($d\le r$ by definition) and cardinality $q^{(n-r)(r-d+1)}$ as $\mathcal{E}^0$. For $1\le k\le\lfloor\frac{r}{d}\rfloor$, we first define two MRD codes $\mathcal{C}^k$ and $\mathcal{D}^k$, and then construct $\mathcal{E}^k$ based on $\mathcal{C}^k$ and $\mathcal{D}^k$. $\mathcal{C}^k$ is an MRD code in $\mathrm{GF}(q)^{(r-kd)\times kd}$ with minimum distance d for $k\le\lfloor\frac{r}{d}\rfloor-1$ ($\lfloor\frac{n-r}{d}\rfloor\ge\lfloor\frac{r}{d}\rfloor$) and $\mathcal{C}^{\lfloor\frac{r}{d}\rfloor}=\{\mathbf{0}\}\subseteq\mathrm{GF}(q)^{\left(r-\lfloor\frac{r}{d}\rfloor d\right)\times\lfloor\frac{r}{d}\rfloor d}$; $\mathcal{D}^k$ is an MRD code in $\mathrm{GF}(q)^{r\times(n-r-kd)}$ with minimum distance d for $k\le\lfloor\frac{n-r}{d}\rfloor-1$ and $\mathcal{D}^{\lfloor\frac{n-r}{d}\rfloor}=\{\mathbf{0}\}\subseteq\mathrm{GF}(q)^{r\times\left(n-r-\lfloor\frac{n-r}{d}\rfloor d\right)}$. For $1\le k\le\lfloor\frac{r}{d}\rfloor$, $I(\mathcal{C}^k)$ and $I(\mathcal{D}^k)$ are either trivial codes or KK codes with minimum injection distance d in $E_{r-kd}(q,r)$ and $E_r(q,n-kd)$, respectively. For $1\le k\le\lfloor\frac{r}{d}\rfloor$, $\mathbf{C}_i^k\in\mathcal{C}^k$, and $\mathbf{D}_j^k\in\mathcal{D}^k$, we define $E_{i,j}^k\in E_r(q,n)$ as the row space of $\left(\begin{array}{c|c|c}\mathbf{I}_{r-kd}&\mathbf{C}_i^k&\mathbf{0}\\\hline\mathbf{0}&\mathbf{0}&\mathbf{I}_{kd}\end{array}\right)\mathbf{D}_j^k$ and $\mathcal{E}^k=\{E_{i,j}^k\}_{i,j=0}^{|\mathcal{C}^k|-1,|\mathcal{D}^k|-1}$. Our augmented KK code is simply $\mathcal{E}=\bigcup_{k=0}^{\lfloor\frac{r}{d}\rfloor}\mathcal{E}^k$. It can be shown that $\mathcal{E}$ has minimum injection distance d, and hence minimum subspace distance $2d$.

Let us first determine the cardinality of our augmented KK codes. By construction, $\mathcal{E}$ has cardinality $|\mathcal{E}|=q^{(n-r)(r-d+1)+\sum_{k=1}^{\lfloor\frac{r}{d}\rfloor}|\mathcal{C}^k||\mathcal{D}^k|}$, where $|\mathcal{C}^{\lfloor\frac{r}{d}\rfloor}|=1$ and $|\mathcal{C}^k|=\min\{q^{(r-kd)(kd-d+1)},q^{kd(r-kd-d+1)}\}$ for $1\le k\le\lfloor\frac{r}{d}\rfloor-1$ and $|\mathcal{D}^{\lfloor\frac{n-r}{d}\rfloor}|=1$ and $|\mathcal{D}^k|=\min\{q^{r(n-r-kd-d+1)},q^{(n-r-kd)(r-d+1)}\}$ for $1\le k\le\lfloor\frac{n-r}{d}\rfloor-1$.

Let us compare the cardinality of our augmented KK codes to those of KK and Skachek codes. Note that all three codes are CDCs with minimum injection distance d in $E_r(q,n)$. First, it is easily shown that our augmented KK codes properly contain KK codes for all parameter values.

r	d	KK	Skachek	Augmented KK
2	2	256	340	320
3	2	16384	16640	17408
	3	128	144	144
4	2	262144	262144	278544
	3	4096	4096	4112
	4	64	64	65
5	2	1048576	1048576	1056769
	3	32768	32768	32769
	4	1024	1024	1025
	5	32	32	33

TABLE I
CARDINALITIES OF KK CODES, SKACHEK CODES, AND AUGMENTED KK CODES IN $E_r(2,10)$ FOR $2 \leq r \leq 5$.

This is a clear distinction from Skachek codes with cardinality $L(q,n,r,d)$, which by (2) reduce to KK codes for $3r > n$. When $3r \leq n$, we can show that $|\mathcal{E}| - q^{(n-r)(r-d+1)} > K_q q^{(r-d)(r-d+1)}(L(q,n,r,d) - q^{(n-r)(r-d+1)})$, and our augmented KK codes have a greater cardinality than Skachek codes when $d < r$. We emphasize that for CDCs of dimension r, their minimum injection distance d satisfies $d \leq r$. A Skachek code is constructed in multiple steps, and in the i-th step ($i \geq 1$), subspaces that correspond to a KK code in $E_r(q, n-ir)$ are added to the code. When $d = r$, our augmented KK code $\mathcal{E}$ is actually the code obtained after the first step.

To illustrate the differences between KK codes, Skachek codes, and our augmented KK codes, the cardinalities of the three classes of codes are compared in Table I for $q = 2$, $n = 10$, and $2 \leq r \leq 5$. For the parameters considered in Table I, augmented KK codes have the greatest cardinality for all but one case, where $d = r = 2$.

B. Decoding of Augmented KK codes

Let $\mathbf{A} = (\mathbf{A}_0|\mathbf{A}_3) \in \mathrm{GF}(q)^{a\times n}$ be the received matrix, where $\mathbf{A}_0 \in \mathrm{GF}(q)^{a\times r}$ and $\mathbf{A}_3 \in \mathrm{GF}(q)^{a\times(n-r)}$. We propose a decoding algorithm that either produces the unique codeword in $\mathcal{E}$ closest to $R(\mathbf{A})$ in the subspace metric or returns a failure. Suppose the minimum subspace distance of our augmented KK codes is denoted as $2d$, a bounded distance decoder would find the codeword that is closest to $R(\mathbf{A})$ up to subspace distance $d-1$. Our decoding algorithm always returns the correct codeword if it is at subspace distance at most $d-1$ from the received subspace, thus correcting more errors than a bounded subspace distance decoder.

Given the layered structure of $\mathcal{E}$, our decoding algorithm for $\mathcal{E}$ is based on a decoding algorithm for $\mathcal{E}^k$, shown below in Algorithm 1, for any k. We denote the codewords in $\mathcal{E}^0$ as $E^0_{0,j}$ for $0 \leq j \leq |\mathcal{E}^0| - 1$.

Algorithm 1: $\mathrm{EBDD}(k, \mathbf{A})$.
Input: k and $\mathbf{A} = (\mathbf{A}_1|\mathbf{A}_2|\mathbf{A}_3) \in \mathrm{GF}(q)^{a\times n}$, $\mathbf{A}_1 \in \mathrm{GF}(q)^{a\times(r-kd)}$, $\mathbf{A}_2 \in \mathrm{GF}(q)^{a\times kd}$, $\mathbf{A}_3 \in \mathrm{GF}(q)^{a\times(n-r)}$.
Output: $(E^k_{i,j}, d_k, f_k)$.

1.1 If $k = 0$, use the decoder for $\mathcal{E}^0$ to obtain $E^0_{0,j}$, calculate $d_k = d_{\mathrm{s}}(R(\mathbf{A}), E^0_{0,j})$, and return $(E^0_{0,j}, d_k, 0)$. If the decoder returns a failure, return $(I(\mathbf{0}), d, 0)$.

1.2 Use the decoder of $I(\mathcal{C}^k)$ on $(\mathbf{A}_1|\mathbf{A}_2)$ to obtain $\mathbf{C}^k_i$. If the decoder returns a failure, set $\mathbf{C}^k_i = \mathbf{0}$, $\mathbf{D}^k_j = \mathbf{0}$ and return $(E^k_{i,j}, d, 0)$.

1.3 Use the decoder of $I(\mathcal{D}^k)$ on $(\mathbf{A}_1|\mathbf{A}_3)$ to obtain $\mathbf{D}^k_j$. If the decoder returns a failure, set $\mathbf{D}^k_j = \mathbf{0}$ and return $(E^k_{i,j}, d, 0)$.

1.4 Calculate $d_k = d_{\mathrm{s}}(R(\mathbf{A}), E^k_{i,j})$ and $f_k = 2d - \max\{d_{\mathrm{s}}(R(\mathbf{A}_1|\mathbf{A}_2), I(\mathbf{C}^k_i)), d_{\mathrm{s}}(R(\mathbf{A}_1|\mathbf{A}_3), I(\mathbf{D}^k_j))\}$ and return $(E^k_{i,j}, d_k, f_k)$.

Algorithm 1 is based on the bounded distance decoder proposed in [1]. When $k = 0$, $\mathcal{E}^0$ is simply a KK code, and the algorithm in [1] is used directly; when $k \geq 1$, given the structure of $\mathcal{E}^k$, two decoding attempts are made based on $(\mathbf{A}_1|\mathbf{A}_2)$ and $(\mathbf{A}_1|\mathbf{A}_3)$, and both use the decoding algorithm in [1].

We remark that Algorithm 1 always returns $(E^k_{i,j}, d_k, f_k)$. If a unique nearest codeword in $\mathcal{E}^k$ at distance no more than $d-1$ from $R(\mathbf{A})$ exists, then Steps 1.2 and 1.3 succeed and Algorithm 1 returns the unique nearest codeword in $E^k_{i,j}$. However, when such unique codeword in $\mathcal{E}^k$ at distance no more than $d-1$ does not exist, the return value f_k can be used to find the unique nearest codeword because f_k is a lower bound on the distance from the received subspace to any other codeword in $\mathcal{E}^k$. Also, when $f_k = 0$, Algorithm 2 below always returns a failure. Thus, we call Algorithm 1 an enhanced bounded distance decoder.

The algorithm for $\mathcal{E}$ thus follows.

Algorithm 2: Decoder for $\mathcal{E}$.
Input: $\mathbf{A} = (\mathbf{A}_0|\mathbf{A}_3) \in \mathrm{GF}(q)^{a\times n}$, $\mathbf{A}_0 \in \mathrm{GF}(q)^{a\times r}$, $\mathbf{A}_3 \in \mathrm{GF}(q)^{a\times(n-r)}$.
Output: Either a failure or the unique nearest codeword in $\mathcal{E}$ from $R(\mathbf{A})$.

2.1 If $\mathrm{rk}(\mathbf{A}) < r - d + 1$, return a failure.

2.2 Calculate $r - \mathrm{rk}(\mathbf{A}_0) = ld + m$ where $0 \leq l \leq \lfloor \frac{r}{d} \rfloor$ and $0 \leq m < d$.

2.3 Call $\mathrm{EBDD}(l, \mathbf{A})$ to obtain $(E^l_{i,j}, d_l, f_l)$. If $d_l \leq d-1$, return $E^l_{i,j}$.

2.4 If $m = 0$, return a failure. Otherwise, call $\mathrm{EBDD}(l+1, \mathbf{A})$ to obtain $(E^{l+1}_{s,t}, d_{l+1}, f_{l+1})$. If $d_{l+1} \leq d-1$, return $E^{l+1}_{s,t}$.

2.5 If $d_l < \min\{d+m, f_l, d_{l+1}, f_{l+1}, 2d-m\}$, return $E^l_{i,j}$. If $d_{l+1} < \min\{d+m, d_l, f_l, f_{l+1}, 2d-m\}$, return $E^{l+1}_{s,t}$.

2.6 Return a failure.

Proposition 1: If the received subspace is at subspace distance at most $d-1$ from a codeword in $\mathcal{E}$, then Algorithm 2 returns this codeword. Otherwise, Algorithm 2 returns either a failure or the unique nearest codeword to the received subspace in the subspace metric.

We note that when $\mathrm{rk}(\mathbf{A}) < r - d + 1$, Steps 1.2 and 1.3 would both fail, and Algorithm 2 will return a failure. We also justify why Algorithm 2 returns a failure if $d_l \geq d$ and $m = 0$ in Step 2.3. Suppose $d_l \geq d$ and $m = 0$ and we apply Algorithm 1 for $\mathcal{E}^{l+1}$. Then we have $d_l \geq d + m$ and $d_{l+1} \geq |d - m| = d + m$. Therefore, neither inequality in Step 2.5 is satisfied and the decoder returns a failure.

By Proposition 1, Algorithm 2 decodes beyond the half distance. However, the decoding radius of Algorithm 2 is limited. It is easy to see that the decoding radius of Algorithm 2 is at most $d + \lfloor \frac{d}{2} \rfloor$ due to the terms $d + m$ and $2d - m$ in the inequalities in Step 2.5. We emphasize that this is just an upper bound, and its tightness is unknown. Suppose $r - \mathrm{rk}(\mathbf{A}_0) = ld + m$, when Algorithm 2 decodes beyond half distance, it is necessary that f_l and f_{l+1} be both nonzero in Step 2.5. This implies that the row space of $(\mathbf{A}_1|\mathbf{A}_2)$ is at subspace distance no more than $d-1$ from $I(\mathcal{C}^l)$ and $I(\mathcal{C}^{l+1})$ and that the row spaces of $(\mathbf{A}_1|\mathbf{A}_3)$ are at subspace distance no more than $d-1$ from $I(\mathcal{D}^l)$ and $I(\mathcal{D}^{l+1})$.

We note that the inequalities in Step 2.5 are strict in order to ensure that the output of the decoder is the **unique** nearest codeword from the received subspace. However, if one of the nearest codewords is an acceptable outcome, then equality can be included in the inequalities in Step 2.5.

Our decoding algorithm can be readily simplified in order to obtain a bounded subspace distance decoder, by removing Step 2.5. We emphasize that the general decoding algorithm has the same order of complexity as this simplified bounded subspace distance decoding algorithm.

The complexity of the bounded subspace distance decoder in [1] for a KK code in $E(q,n)$ is on the order of $O(n^2)$ operations over $\mathrm{GF}(q)^{n-r}$ for $r \leq \frac{n}{2}$, which is hence the complexity of decoding $\mathcal{E}^0$. This algorithm can be easily generalized to include the case where $r > \frac{n}{2}$, and we obtain a complexity on the order of $O(n^2)$ operations over $\mathrm{GF}(q^{\max\{r,n-r\}})$. Thus the complexity of decoding $I(\mathcal{C}^k)$ and $I(\mathcal{D}^k)$ for $k \geq 1$ is on the order of $O(r^2)$ operations over $\mathrm{GF}(q^{\max\{kd,r-kd\}})$ and $O((n-kd)^2)$ operations over $\mathrm{GF}(q^{\max\{r,n-kd-r\}})$, respectively. The complexity of the decoding algorithm for $\mathcal{E}^k$ is on the order of the maximum of these two quantities. It is easily shown that the complexity is maximized for $k = 0$, that is, our decoding algorithm has the same order of complexity as the algorithm for the KK code $\mathcal{E}^0$.

IV. Covering properties of CDCs

The packing properties of CDCs have been studied in [1], [3]–[5], [12] and an asymptotic packing rate of CDCs was defined and determined in [1]. Henceforth in this section, we focus on the covering properties of CDCs in the Grassmannian instead. We emphasize that without loss of generality, we consider only the injection distance and assume $r \leq \frac{n}{2}$ in this section.

A. Properties of balls in the Grassmannian

We first investigate the properties of balls in the Grassmannian $E_r(q,n)$, which will be instrumental in our study of covering properties of CDCs. First, we derive bounds on the volume of balls in $E_r(q,n)$.

We now determine the volume of the intersection of two **spheres** of radii u and s respectively and distance d between their centers, which is referred to as the intersection number $J_{\mathrm{c}}(u,s,d)$ of the association scheme [19]. The intersection number is an important parameter of an association scheme.

Lemma 1: For all u, s, and d between 0 and r,

$$J_{\mathrm{c}}(u,s,d) = \frac{1}{\begin{bmatrix} n \\ r \end{bmatrix} N_{\mathrm{c}}(d)} \sum_{i=0}^{r} \mu_i E_u(i) E_s(i) E_d(i),$$

where $\mu_i = \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix}$ and $E_j(i)$ is a q-Eberlein polynomial [20].

Although Lemma 1 is obtained by a direct application of Theorems 3.5 and 3.6 in [21, Chapter II], we present it formally here since it is a fundamental geometric property of the Grassmannian and is very instrumental in our study of CDCs. Let $I_{\mathrm{c}}(u,s,d)$ denote the intersection of two **balls** in $E_r(q,n)$ with radii u and s and distance d between their centers. Since $I_{\mathrm{c}}(u,s,d) = \sum_{i=0}^{u} \sum_{j=0}^{s} J_{\mathrm{c}}(i,j,d)$, Lemma 1 also leads to an analytical expression for $I_{\mathrm{c}}(u,s,d)$.

We derive below an upper bound on the union of balls in $E_r(q,n)$ with the same radius.

Lemma 2: The volume of the union of *any* K balls in $E_r(q,n)$ with radius ρ is at most

$$\begin{aligned} B_{\mathrm{c}}(K,\rho) = KV_{\mathrm{c}}(\rho) &- \sum_{a=1}^{l} I_{\mathrm{c}}(\rho,\rho,r-a+1) \\ &\cdot [A_{\mathrm{c}}(q,n,r,r-a+1) - A_{\mathrm{c}}(q,n,r,r-a+2)] \\ &- [K - A_{\mathrm{c}}(q,n,r,r-l+1)] I_{\mathrm{c}}(\rho,\rho,r-l), \end{aligned} \quad (3)$$

where $l = \max\{a : K \geq A_{\mathrm{c}}(q,n,r,r-a+1)\}$.

We remark that using any upper bound on $A_{\mathrm{c}}(q,n,r,r-a+1)$ in the proof of Lemma 2 leads to a valid upper bound on $B_{\mathrm{c}}(K,\rho)$. Hence, although the value of $A_{\mathrm{c}}(q,n,r,r-a+1)$ is unknown in general, the upper bound in (2) can be used in (3) in order to obtain an upper bound on the volume of the union on balls in the Grassmannian.

B. Covering CDCs

The *covering radius* of a CDC $\mathcal{C} \subseteq E_r(q,n)$ is defined as $\rho = \max_{U \in E_r(q,n)} d_{\mathrm{I}}(U,\mathcal{C})$. We denote the minimum cardinality of a CDC in $E_r(q,n)$ with covering radius ρ as $K_{\mathrm{c}}(q,n,r,\rho)$. Since $K_{\mathrm{c}}(q,n,n-r,\rho) = K_{\mathrm{c}}(q,n,r,\rho)$, we assume $r \leq \lfloor \frac{n}{2} \rfloor$. Also, $K_{\mathrm{c}}(q,n,r,0) = \begin{bmatrix} n \\ r \end{bmatrix}$ and $K_{\mathrm{c}}(q,n,r,r) = 1$, hence we assume $0 < \rho < r$ henceforth. We first derive lower bounds on $K_{\mathrm{c}}(q,n,r,\rho)$.

Lemma 3: For all q, n, $r \leq \lfloor \frac{n}{2} \rfloor$, and $0 < \rho < r$, $K_{\mathrm{c}}(q,n,r,\rho) \geq \min\left\{K : B_{\mathrm{c}}(K,\rho) \geq \begin{bmatrix} n \\ r \end{bmatrix}\right\} \geq \frac{\begin{bmatrix} n \\ r \end{bmatrix}}{V_{\mathrm{c}}(\rho)}$.

The latter lower bound in Lemma 3 is referred to as the sphere covering bound for CDCs. We remark that this bound is a simple union bound, which does not involve the intersection of balls. However, the Grassmannian is an association scheme, which provides an analytical formula for the volume $I_{\mathrm{c}}(u,s,d)$ of the intersection of two balls. The earlier upper bound in Lemma 3 takes advantage of this property through the formula for $B_{\mathrm{c}}(K,\rho)$ in Lemma 2. Since the volume of the intersection of three balls has a completely different behavior, considering the intersection of more than two balls would be much more difficult.

We now derive upper bounds on $K_{\mathrm{c}}(q,n,r,\rho)$. First, we investigate how to expand covering CDCs.

Lemma 4: For all q, n, $r \leq \left\lfloor \frac{n}{2} \right\rfloor$, and $0 < \rho < r$, $K_{\mathrm{c}}(q,n,r,\rho) \leq K_{\mathrm{c}}(q,n-1,r,\rho-1) \leq \begin{bmatrix} n-\rho \\ r \end{bmatrix}$, and $K_{\mathrm{c}}(q,n,r,\rho) \leq K_{\mathrm{c}}(q,n,r-1,\rho-1) \leq \begin{bmatrix} n \\ r-\rho \end{bmatrix}$.

The next bound is a direct application of [6, Theorem 12.2.1].

Proposition 2: For all q, n, $r \leq \left\lfloor \frac{n}{2} \right\rfloor$, and $0 < \rho < r$, $K_{\mathrm{c}}(q,n,r,\rho) \leq \frac{\begin{bmatrix} n \\ r \end{bmatrix}}{V_{\mathrm{c}}(\rho)} \{1 + \ln V_{\mathrm{c}}(\rho)\}$.

The bound in Proposition 2 can be refined by applying the greedy algorithm described in [22] to CDCs. This algorithm begins with a code for which the balls with radius ρ centered at the codewords cover the most subspaces in the Grassmannian. Hence, the algorithm uses a code with minimum distance $2\rho+1$ for $2\rho+1 \leq r$, or a single codeword for $2\rho+1 > r$. Since the performance of the algorithm depends only on the cardinality of the code, we use below our augmented KK codes, which have the greatest known cardinality in most cases. We remark that due to our discussion in Section III, Skachek codes have a greater cardinality and hence should be preferably used when $2\rho + 1 = r$.

Proposition 3: Let k_0 be the cardinality of an augmented KK code with minimum distance $2\rho + 1$ in $E_r(q,n)$ for $2\rho < r$ and $k_0 = 1$ for $2\rho \geq r$. Then for all $k \geq k_0$, there exists a CDC with cardinality k which covers at least $\begin{bmatrix} n \\ r \end{bmatrix} - u_k$ subspaces, where $u_{k_0} \stackrel{\text{def}}{=} \begin{bmatrix} n \\ r \end{bmatrix} - k_0 V_{\mathrm{c}}(\rho)$ and $u_{k+1} = u_k - \left\lceil \frac{u_k V_{\mathrm{c}}(\rho)}{\min\left\{\begin{bmatrix} n \\ r \end{bmatrix} - k, B_{\mathrm{c}}(u_k,\rho)\right\}} \right\rceil$ for all $k \geq k_0$. Thus $K_{\mathrm{c}}(q,n,r,\rho) \leq \min\{k : u_k = 0\}$.

Using the bounds derived above, it can be shown that $K_{\mathrm{c}}(q,n,r,\rho)$ is on the order of $q^{r(n-r)-\rho(n-\rho)}$.

We finish this section by studying the covering properties of liftings of rank metric codes. We first prove that they have maximum covering radius.

Lemma 5: Let $I(\mathcal{C}) \subseteq E_r(q,n)$ be the lifting of a rank metric code in $\mathrm{GF}(q)^{r\times(n-r)}$. Then $I(\mathcal{C})$ has covering radius r.

Lemma 5 is significant for the design of CDCs. It is shown in [1] that liftings of rank metric codes can be used to construct nearly optimal packing CDCs. However, Lemma 5 indicates that for any lifting of a rank metric code, there exists a subspace at distance r from the code. Hence, adding this subspace to the code leads to a supercode with higher cardinality and the same minimum distance since $d \leq r$. Thus an optimal CDC cannot be designed from a lifting of a rank metric code.

Although liftings of rank metric codes have poor covering properties, below we construct a class of covering CDCs by using permuted liftings of rank metric covering codes. We thus relate the minimum cardinality of a covering CDC to that of a covering code with the rank metric.

Proposition 4: For all q, n, $r \leq \left\lfloor \frac{n}{2} \right\rfloor$, and $0 < \rho < r$, $K_{\mathrm{c}}(q,n,r,\rho) \leq \binom{n}{r} K_{\mathrm{R}}(q^{n-r},r,\rho)$.

It is shown in [16] that for $r \leq n-r$, $K_{\mathrm{R}}(q^{n-r},r,\rho)$ is on the order of $q^{r(n-r)-\rho(n-\rho)}$, which is also the order of $K_{\mathrm{c}}(q,n,r,\rho)$. The bound in Proposition 4 is relatively tighter for large q since $\binom{n}{r}$ is independent of q. Also, since $\binom{n}{r} \leq 2^n$ for all r, it can be easily shown that the bound in Proposition 4 is asymptotically optimal. Finally, since the exact value of $K_{\mathrm{R}}(q^{n-r},r,\rho)$ is in general unknown [16], it is difficult to compare the upper bound in Proposition 4 to that in Proposition 2.

REFERENCES

[1] 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.

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

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

[4] A. Kohnert and S. Kurz, "Construction of large constant dimension codes with a prescribed minimum distance," *Mathematical Methods in Computer Science, LNCS*, vol. 5393, pp. 31–42, December 2008.

[5] S.-T. Xia and F.-W. Fu, "Johnson type bounds on constant dimension codes," *Designs, Codes and Cryptography*, vol. 50, no. 2, pp. 163–172, February 2009.

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

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

[8] M. Gadouleau and Z. Yan, "Construction and covering properties of constant-dimension codes," *submitted to IEEE Trans. Info. Theory*, 2009, available at http://arxiv.org/abs/0903.2675.

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

[10] 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.

[11] 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.

[12] E. M. Gabidulin and M. Bossert, "Codes for network coding," in *Proc. IEEE Int. Symp. on Information Theory*, Toronto, ON, July 2008, pp. 867–870.

[13] 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.

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

[15] 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.

[16] M. Gadouleau and Z. Yan, "Packing and covering properties of rank metric codes," *IEEE Trans. Info. Theory*, vol. 54, no. 9, pp. 3873–3883, September 2008.

[17] ——, "Bounds on covering codes with the rank metric," *submitted to IEEE Communications Letters*, September 2008, available at http://arxiv.org/abs/0809.2968.

[18] 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.

[19] 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.

[20] P. Delsarte, "Properties and applications of the recurrence $F(i+1,k+1,n+1) = q^{k+1}F(i,k+1,n) - q^k F(i,k,n)$," *SIAM Journal of Applied Mathematics*, vol. 31, no. 2, pp. 262–270, September 1976.

[21] E. Bannai and T. Ito, *Algebraic Cominatorics I. Association Schemes*. The Benjamin/Cummings Publishing Company, 1983.

[22] W. E. Clark and L. A. Dunning, "Tight upper bounds for the domination numbers of graphs with given order and minimum degree," *The Electronic Journal of Combinatorics*, vol. 4, 1997.