Combinatorial Bounds for List Decoding of Subspace Codes

Rachit Agarwal
Department of Electrical and Computer Engineering,
University of Illinois at Urbana-Champaign, IL, USA
Email: agarwa16@illinois.edu

***Abstract*—Codes constructed as subsets of the projective geometry of a vector space over a finite field have recently been shown to have applications as random network error correcting codes. If the dimension of each codeword is restricted to a fixed integer, the code forms a subset of a finite-field Grassmannian, or equivalently, a subset of the vertices of the corresponding Grassmannian graph. These codes are referred to as *codes on finite-field Grassmannian* or more generally as *subspace codes*.**

In this paper, we consider the problem of decoding subspace codes beyond half the minimum distance bound. Using random coding arguments, we derive lower and upper bounds on size of subspace codes for the first relaxation of bounded minimum distance decoding, *i.e.*, when the worst-case list size is restricted to two. An important ingredient in establishing our results is generalization of sphere-covering and sphere-packing conditions to volume-covering and volume-packing conditions, which can be of independent interest.

I. Introduction

Consider an information network given by a directed graph $\mathcal{G} = (\mathcal{V} \cup s, \mathcal{E})$, where a source s wishes to multicast some information to a set of terminals $\mathcal{T} \subseteq \mathcal{V}$. Let $\mathbb{F}_q$ be a finite field of q elements and let $\{p_1, p_2, \ldots, p_M\}$, $p_i \in \mathbb{F}_q^N$ denote a set of vectors of length N over $\mathbb{F}_q$. In random network coding [1], these vectors are injected by s into $\mathcal{G}$. Any node $v \in \mathcal{V}$, when given an opportunity to forward a packet, generates a $\mathbb{F}_q$-linear combination of the incoming packets and transmits this random combination. In the error-free case, a particular terminal collects packets y_j, $j = 1, 2, \ldots, L$ where each y_j is formed as $y_j = \sum_{i=1}^{M} h_{j,i} p_i$ with unknown, randomly chosen coefficients $h_{j,i} \in \mathbb{F}_q$. In matrix form, the matrix whose rows are the received vectors can be written as $y = H \times p$, where H is a random matrix and p is the matrix whose rows are the transmitted vectors. Noting that H being a random matrix preserves the row space of p in product Hp, Kötter-Kschischang [2] model the information transmission not via the choice of p, but rather by the choice of the vector space spanned by the rows of p.

Let $\mathcal{W}$ be an N-dimensional vector space over $\mathbb{F}_q$. The projective geometry of $\mathcal{W}$, denoted by $\mathcal{P}(\mathcal{W})$, is the set of all subspaces of $\mathcal{W}$. The dimension of an element $V \in \mathcal{P}(\mathcal{W})$ is denoted as $dim(V)$. It was shown in [2] that the function $d(A, B) := dim(A) + dim(B) - 2dim(A \cap B)$ is a metric for the space $\mathcal{P}(\mathcal{W})$. A *subspace code* is simply a non-empty subset of $\mathcal{P}(\mathcal{W})$. The minimum distance $\mathcal{D}(\mathcal{S})$ of the code $\mathcal{S}$ is defined as $\min_{A,B \in \mathcal{S}; A \neq B} d(A, B)$.

Under random network coding model, the network takes in a vector space and puts out another vector space, possibly with erasures (deletion of vectors from the transmitted space) or errors (addition of vectors to the transmitted space). A subspace code $\mathcal{S}$ with a minimum distance $\mathcal{D}(\mathcal{S})$ is guaranteed to output an unique codeword (correct all errors in the received information) as long as the number of errors $\rho < \lfloor (\mathcal{D}(\mathcal{S}) - 1)/2 \rfloor$ (referred to as Bounded Minimum Distance (BMD) decoding). We show that this is an overly pessimistic estimate of the error correcting radius due to the way the Grassmannian spheres pack in space. The packing is such that for *most* choices of the received word there will be at most one codeword within distance ρ from it even for ρ much greater than $\lfloor (\mathcal{D}(\mathcal{S}) - 1)/2 \rfloor$. Therefore, *always* insisting on a unique output will preclude decoding most such received words owing to a few pathological received words that have more than one codeword within distance $\lfloor (\mathcal{D}(\mathcal{S}) - 1)/2 \rfloor$ from them. List decoding [3]–[5] provides a way to get around this situation, and yet deal with worst-case error patterns. For codes like Reed-Solomon codes, the increase in decoding radius is quite significant [6] [7] and it is not very difficult to show that a list-decoding approach (at least for worst-case list size restricted to smaller numbers) results in an unique output with a very high probability [7].

Motivated by the above discussion, we initiate the study of list decoding subspace codes. In this paper, we consider subspace codes in which the dimension of each codeword is a fixed integer. Furthermore, we restrict our attention to the first relaxation of BMD decoding, *i.e.*, when the worst-case list size is restricted to two. Using random coding arguments, we derive lower and upper bounds on the size of the subspace codes for the first relaxation of BMD decoding. At the heart of our construction is a generalization of the well-known sphere-covering and sphere-packing bounds [8] to covering and packing of volumes, which can be of independent interest.

The rest of the paper is organized as follows. In Section II, we give necessary definitions and recall some properties of subspace codes. Section III introduces two "volumes" that are central to our construction and covers the problem of finding the size of these volumes. We formally state our results in Section IV. The rest of the three sections give the proofs for the volume-covering and volume-packing conditions, the lower bound and the upper bound on the size of the codes for decoding beyond the minimum distance bound. We close the paper with some final remarks in Section VIII.

II. Definition and Preliminaries

Let $\mathbb{F}_q$ be a finite field of q elements and let $\mathcal{W}$ be an N-dimensional vector space over $\mathbb{F}_q$. Denote by $\mathcal{P}(\mathcal{W},\ell)$ the ℓ-dimensional projective geometry of $\mathcal{W}$, *i.e.*, the set of all ℓ-dimensional subspaces of $\mathcal{W}$. A *subspace code* $\mathcal{S}$, of size $|\mathcal{S}|$, is a collection of $|\mathcal{S}|$ distinct ℓ-dimensional subspaces of $\mathcal{W}$. The distance between any two codewords A, B of a subspace code will be $d(A,B) = 2(\ell - dim(A \cap B))$. [1] The minimum distance of the code $\mathcal{S}$ is defined as $\mathcal{D}(\mathcal{S}) = \min_{A,B\in\mathcal{S};A\neq B} d(A,B)$.

The ℓ-dimension projective geometry of vector space $\mathcal{W}$ constitutes a distance-regular graph $G_{\mathcal{W},\ell}$, known as Grassmann graph [9]. $G_{\mathcal{W},\ell}$ has vertex set $\mathcal{P}(\mathcal{W},\ell)$ with an edge joining vertices U and V if they are at unit distance. The number of vertices of $G_{\mathcal{W},\ell}$ is same as the number of ℓ dimensional subspaces of an N-dimensional ambient space over $\mathbb{F}_q$ and is given by the so-called Gaussian coefficient $|\mathcal{P}(\mathcal{W},\ell)| = \begin{bmatrix} N \\ \ell \end{bmatrix}_q$.

The number of subspaces A at distance k from a given subspace B is independent of the subspace B itself and is given by: $\#\{A \in \mathcal{P}(\mathcal{W},\ell) : d(A,B) = k\} = q^{k^2} \begin{bmatrix} N-\ell \\ k \end{bmatrix} \begin{bmatrix} \ell \\ k \end{bmatrix}$. Denote by $\boldsymbol{P}(k)$ the probability that any two randomly chosen subspaces $A, B \in \mathcal{P}(\mathcal{W},\ell)$ are at distance k. Then,

$$\boldsymbol{P}(k) = Pr[d(A,B) = k] = \left[\frac{q^{k^2} \begin{bmatrix} N-\ell \\ k \end{bmatrix} \begin{bmatrix} \ell \\ k \end{bmatrix}}{|\mathcal{P}(\mathcal{W},\ell)|} \right] \tag{1}$$

Let $\mathcal{B}(U,\rho)$ denote the sphere of radius ρ around U, i.e.

$$\mathcal{B}(U,\rho) = \{V \in \mathcal{P}(\mathcal{W},\ell) : d(U,V) \leq \rho\}$$

We will generally refer to this sphere as a Grassmannian ball. We will occasionally make use of the expression for the distance of a subspace from a set of (collection of) subspaces and will denote it as $d(U,\mathcal{Z}) = min\{d(U,V) : U \in \mathcal{P}(\mathcal{W},\ell), V \in \mathcal{Z} \subseteq \mathcal{P}(\mathcal{W},\ell)\}$.

Definition 1 ((ρ, L)-List-decodable Code): Let ρ and L be positive integers. A subspace code $\mathcal{S} \subseteq \mathcal{P}(\mathcal{W},\ell)$ is said to be $(\rho, L)-$ list-decodable if for every $U \in \mathcal{P}(\mathcal{W},\ell)$, the Grassmannian ball of radius ρ centered at U contains at most L codewords of $\mathcal{S}$. In other words, for a $(\rho, L)-$ list-decodable code, we have:

$$|\mathcal{B}(U,\rho) \cap \mathcal{S}| \leq L, \qquad \forall\ U \in \mathcal{P}(\mathcal{W},\ell)$$

The parameter ρ is called the **list decoding radius** and the parameter L is called the **list size**.

Definition 2 (Intersection Number, Intersection Size): For any pair of subspaces $U, V \in \mathcal{P}(\mathcal{W},\ell)$ with $d(U,V) = \delta$, their **intersection number** is defined as:

$$\lambda_{i,j}(\delta) = \#\{X \in \mathcal{P}(\mathcal{W},\ell) : d(X,U) = i\ ;\ d(X,V) = j\}$$

We define the **Intersection size** ζ as:

$$\zeta(\delta, z) = \sum_{i=1}^{z} \sum_{j=1}^{z} \lambda_{i,j}(\delta) = |\mathcal{B}(U,z) \cap \mathcal{B}(V,z)| \Big|_{d(U,V)=\delta}$$

It is known that the intersection number $\lambda_{i,j}(\delta)$ for two vertices u, v of a distance-regular graph is dependent only on the distance δ between u and v and not the specific choice of vertices [9]. A technique to compute the intersection numbers for any distance regular graph is given in [9] (for a simpler algorithm for Grassmannian graph, see [10]).

Consider a set $\mathcal{S} = \{s_1, s_2, \ldots, s_{|\mathcal{S}|}\}$ as a collection of $|\mathcal{S}|$ distinct subspaces from $\mathcal{P}(\mathcal{W},\ell)$. We wish to randomly generate the set $\mathcal{S}$ (and hence, a subspace code) without any restriction other than dimension of the code ($\mathcal{S} \subseteq \mathcal{P}(\mathcal{W},\ell)$) and find a necessary condition when the set $\mathcal{S}$ corresponds to a $(\rho, 2)$- list decodable code. If all the subspaces in $\mathcal{S}$ are distinct for this condition, we say that there exists a code of size $|\mathcal{S}|$ that never outputs a list of size larger than two when decoded up to a decoding radius ρ.

Henceforth, we will use the notation $[n]$ for the set of integers $\{1, 2, \ldots, n\}$ and $\binom{[n]}{2}$ for the set of all subsets of $[n]$ of cardinality 2.

III. Two volumes

In this section, we introduce two volumes generated by the intersection of Grassmannian balls of certain specified radius with centers as two subspaces $U, V \in \mathcal{P}(\mathcal{W},\ell)$. We also consider a problem that is central to our construction: computing the size of these volumes.

Definition 3: Given two subspaces $U, V \in \mathcal{P}(\mathcal{W},\ell)$ and a non-negative integer z, the set $\chi_z(U,V)$ is the volume generated by the intersection of the Grassmannian Balls of radius z centered at U and V, i.e.,

$$\chi_z(U,V) = \mathcal{B}(U,z) \cap \mathcal{B}(V,z)$$

Definition 4: Given a pair of subspaces $U, V \in \mathcal{P}(\mathcal{W},\ell)$ and a non-negative integer z, the set $\xi_z(U,V)$ is defined as:

$$\xi_z(U,V) = \{X \in \mathcal{P}(\mathcal{W},\ell) : d(X, \chi_z(U,V)) \leq z\}$$

For any two subspaces U, V with $d(U,V) \leq 2z$, we give two interpretations of the set $\xi_z(U,V)$. First, the set $\xi_z(U,V)$ is the collection of all subspaces in $\mathcal{P}(\mathcal{W},\ell)$ within distance z from any point in $\chi_z(U,V)$ (shaded volume shown in Fig. 2 (a)); and, second, the volume $\xi_z(U,V)$ is precisely the union of all spheres of radius z containing the pair (U,V).

One of the main problems in realizing efficient lower and upper bounds on size of list-decodable subspace codes is to find tight bounds for the size of the two volumes introduced above. If two subspaces U, V intersect non-trivially, we can precisely compute $|\chi_z(U,V)|$ using the intersection numbers for the Grassmannian. Precisely computing the size of $\xi_z(U,V)$ is a significantly harder problem. In the rest of the section, we present techniques to bound the size of the two volumes.

Claim 1: For any pair of subspaces $U, V \in \mathcal{P}(\mathcal{W},\ell)$ and a positive integer z, the size of the set $\chi_z(U,V)$ is given by $|\chi_z(U,V)| \Big|_{d(U,V)=\delta} = \sum_{i=1}^{z} \sum_{j=1}^{z} \lambda_{i,j}(\delta)$

Claim 2: Given a pair of subspaces $U, V \in \mathcal{P}(\mathcal{W},\ell)$, the cardinality of the set $\xi_z(U,V)$ depends only on the distance between U and V and not on the subspaces themselves.

[1] The factor of 2 will not play any role in our formulations, and we scale all the distances by 2, calling the distance in units.

The following lemma gives a bound on the size of $\xi_z(U,V)$:

Lemma 1: For any pair of subspaces $U, V \in \mathcal{P}(\mathcal{W},\ell)$ and a non-negative integer z, the following holds:

$$|\xi_z(U,V)| \bigg|_{d(U,V)=\delta} \leq \zeta(\delta, 2z) \tag{2}$$

Proof: Let U, V be a pair of codewords in $\mathcal{P}(\mathcal{W},\ell)$ such that $d(U,V) \leq 2z$. Then by definition of $\xi_z(U,V)$ and $\chi_z(U,V)$, there exists for each subspace $X \in \xi_z(U,V)$, atleast one subspace X' such that $d(U,X') \leq z$, $d(V,X') \leq z$ and $d(X,X') \leq z$. Recall that $d(.,.)$ is a metric in $\mathcal{P}(\mathcal{W},\ell)$. Hence, by the triangle inequality, we have:

$$\begin{aligned} d(U,X) &\leq d(U,X') + d(X',X) \leq z + z = 2 \cdot z \\ d(V,X) &\leq d(V,X') + d(X',X) \leq z + z = 2 \cdot z \end{aligned}$$

Hence, every subspace $X \in \xi_z(U,V)$ is also a member of $\chi_{2z}(U,V)$. In other words, $\xi_z(U,V) \subseteq \chi_{2z}(U,V)$, or, $|\xi_z(U,V)| \leq |\chi_{2z}(U,V)|$. The correctness of the lemma follows by using Claim 1 and Definition 2. ■

We will frequently use the two volumes and the results of Claim 1 and Lemma 1 in the following sections.

IV. Our Results

We give a formal statement of our results below:

Theorem 1 (Volume-Covering Condition): The collection of subspaces $\mathcal{S} = \{s_i : s_i \in \mathcal{P}(\mathcal{W},\ell)\}$ of length $|\mathcal{S}|$ defines a subspace code that is $(\rho, 2)-$ list decodable if $\forall t \in [|\mathcal{S}|]/\{i,j\}$, we have $s_t \notin \xi_\rho(s_i, s_j)$, $\quad \forall \{i,j\} \in \binom{[|\mathcal{S}|]}{2}$.

Theorem 2 (Volume-Packing Condition): The collection of subspaces $\mathcal{S} = \{s_i : s_i \in \mathcal{P}(\mathcal{W},\ell)\}$ of length $|\mathcal{S}|$ defines a subspace code that is $(\rho, 2)-$ list decodable if for every $i, j, m \in [|\mathcal{S}|]$, we have:

$$\chi_\rho(s_i, s_j) \bigcap \chi_\rho(s_m, s_m) = \emptyset$$

Theorem 3 (Lower Bound): There exists a subspace code of size $|\mathcal{S}|$ that is $(\rho, 2)-$ list decodable, if the following condition is satisfied:

$$|\mathcal{S}| > 0.5 + \sqrt{\frac{4 \cdot |\mathcal{P}(\mathcal{W},\ell)|}{\sum_{k=1}^{\ell} \boldsymbol{P}(k).\zeta(k, 2\rho)}}$$

Theorem 4 (Upper Bound): There exists a code defined on finite-field Grassmannian of size $|\mathcal{S}|$ that is $(\rho, 2)-$ list decodable, if the following condition is satisfied:

$$|\mathcal{S}| \leq 1 + \sqrt[3]{\frac{6 \cdot |\mathcal{P}(\mathcal{W},\ell)|}{\left(\sum_{k=1}^{\ell} \boldsymbol{P}(k).\zeta(k,\rho)\right)\left(\sum_{k=1}^{\rho} \boldsymbol{P}(k)\right)}}$$

Bounds on the size of the subspace codes for the case of BMD decoding are presented in [2]. Fig. 1 compares the performance of our bounds to the bounds for BMD decoding for a certain set of parameters. For discussion on performance of our bounds with various parameters, see [10]. For all parameters, the lower bound of Theorem 3 is higher than the lower bound for BMD decoding; the upper bound approaches the sphere-packing bound with increase in the size of the finite field.

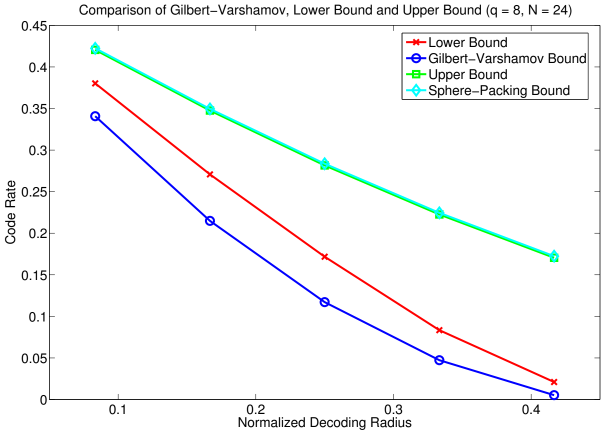

Fig. 1. Comparison of derived lower and upper bounds with Gilbert-Varshamov and Sphere-packing bounds. The upper bound approaches sphere-packing bound as the size of finite field increases.

V. Volume Covering and Volume Packing Conditions

Theorem 1 and Theorem 2 give generalizations of standard sphere-covering and sphere-packing conditions for the case of BMD decoding [8] to voume-covering and volume-packing conditions for $(\rho, 2)$-list decodability. In this section, we provide formal proofs of correctness of Theorem 1 and Theorem 2. Intuitively, the conditions are shown in Fig. 2. The volume-covering (volume-packing) condition states that for each pair (triplet) of subspaces in the code, the shaded area must intersect at exactly two (zero) subspaces.

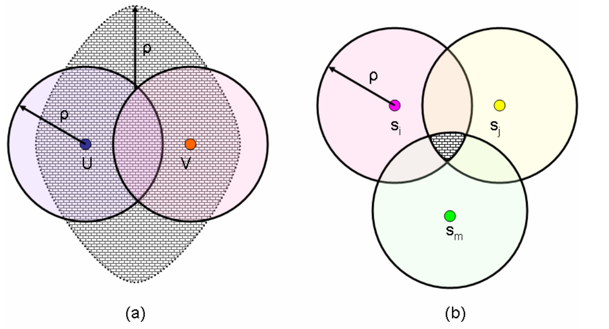

Fig. 2. Pictorial Representation of (a) Volume-Covering (b) Volume-Packing Condition. The shaded volumes must have a null intersection with the code.

Proof of Theorem 1. We first show that the set $\mathcal{S}$ actually defines a code, which when decoded up to radius ρ outputs a list of no more than two codewords. From the definition of list-decodability, this requires that a Grassmannian ball of radius ρ around any space in $\mathcal{P}(\mathcal{W},\ell)$ must contain at most two codewords. Intuitively, recall that for any two subspaces s_i, s_j in the set $\mathcal{S}$, the volume $\xi_\rho(s_i, s_j)$ is by definition the union of all spheres that contain the two subspaces s_i and s_j. If none of these spheres (and hence, the volume) contain any other codeword from $\mathcal{S}$, then the code $\mathcal{S}$ defines a code that is $(\rho, 2)-$ list decodable.

More formally, assume for sake of contradiction, that there exists a $(\rho, 2)$-list decodable code $\mathcal{S}$ and a subspace $s_t \in \mathcal{S}$ such that $s_t \in \xi_\rho(s_i, s_j)$ for some $s_i, s_j \in \mathcal{S}$. Then, by definition, there exists a subspace $s \in \chi_\rho(s_i, s_j)$ such that $d(s, s_t) \leq \rho$. Also, note that $d(s, s_i) \leq \rho$ and $d(s, s_j) \leq \rho$. Hence, for the received erroneous word s, any decoding algorithm will output a list of size three. This contradicts the assumption that $\mathcal{S}$ is a $(\rho, 2)$-list-decodable code.

Finally, we note that for any set $\mathcal{S}$ that complies with the theorem, $s_i, i \in [|\mathcal{S}|]$ will be distinct. To see this, assume that $s_i = s_j$ for some $i, j \in [|\mathcal{S}|]$. Let $s_t \in \mathcal{S}, t \in [|\mathcal{S}|]$. By construction, $\xi_\rho(s_i, s_t)$ contains both s_i and s_t. Since s_j is equal to s_i by the assumption, s_j is also contained in $\xi_\rho(s_i, s_t)$. This violates the condition of the lemma. Hence, all elements of $\mathcal{S}$ are distinct and so, $\mathcal{S}$ defines a code of size $|\mathcal{S}|$. □

Proof of Theorem 2. Assume that there exists some $s_m \in \mathcal{S}$ such that $\chi_\rho(s_i, s_j) \bigcap \chi_\rho(s_m, s_m) \neq \emptyset$. Then, there will exist a received subspace $s_r \in \mathcal{P}(\mathcal{W}, \ell)$ such that $d(s_r, s_i) \leq \rho$, $d(s_r, s_j) \leq \rho$ and $d(s_r, s_m) \leq \rho$. Hence, for a received subspace s, there exist three codewords within distance ρ. This contradicts the condition that the worst-case list size is restricted to two. Hence the proof. □

Notice that the volume-covering and volume-packing conditions of Theorem 1 and Theorem 2 are natural generalizations of the sphere-covering and sphere-packing conditions for BMD decoding. Indeed, if s_i and s_j in the condition of Theorem 1 coincide, the condition states that the projective geometry must be contained in the union of all Grassmannian Balls of radius $2\rho = \mathcal{D}(\mathcal{C}) - 1$, where $\mathcal{D}(\mathcal{C}) = 2\rho + 1$ is the minimum distance of the code, precisely the condition for unique decoding.

Similar remarks can be provided for the volume-packing condition. When the subspaces s_i, s_j coincide in the condition of Theorem 2 for the upper bound, the condition states that all the spheres of radius ρ in the projective geometry must be disjoint, precisely the sphere-packing bound condition.

VI. Proof for Theorem 3

Let $E_{i,j}$ be the event that a randomly selected subspace $s \in \mathcal{P}(\mathcal{W}, \ell)$ is contained in two volumes, $\xi_\rho(s_i, s_j)$ and $\mathcal{P}(\mathcal{W}, \ell) - \mathcal{S}$ (not contained in $\mathcal{S}$). Then,

$$\bigcup_{\{i,j\} \in \binom{[|\mathcal{S}|]}{2}} E_{i,j} \tag{3}$$

is the event that the generated set $\mathcal{S}$ is a $(\rho, 2)$-list decodable code in accordance with Theorem 1.

Lemma 2: The probability of occurrence of event $E_{i,j}$ is independent of the particular choice of subspaces s_i and s_j. Moreover, the probability is bounded above as:

$$Pr[E_{i,j}] \leq \left[1 - \frac{|\mathcal{S}|}{|\mathcal{P}(\mathcal{W}, \ell)|}\right] \cdot \left[\frac{\sum_{k=1}^{\ell} \boldsymbol{P}(k).\zeta(k, 2\rho)}{|\mathcal{P}(\mathcal{W}, \ell)|}\right]$$

Proof: The probability of any random subspace $s \in \mathcal{P}(\mathcal{W}, \ell)$ turning out to be in $\xi_\rho(s_i, s_j)$, where s_i and s_j are two codewords of the randomly generated code $\mathcal{S}$ is dependent on the size of the set $\xi_\rho(s_i, s_j)$. Hence, we have:

$$Pr[E_{i,j}] = Pr[s \in \xi_\rho(s_i, s_j)] \times Pr[s \in \mathcal{P}(\mathcal{W}, \ell) - \mathcal{S}] \tag{4}$$

$$= \frac{|\xi_\rho(s_i, s_j)|}{|\mathcal{P}(\mathcal{W}, \ell)|} \cdot \left[1 - \frac{|\mathcal{S}|}{|\mathcal{P}(\mathcal{W}, \ell)|}\right] \tag{5}$$

Recall that the ℓ-dimensional projective geometry $\mathcal{P}(\mathcal{W}, \ell)$ constitutes a distance-regular graph. Hence, the above expression, dependent on cardinality of the set $\xi_\rho(s_i, s_j)$, is dependent only on the distance $d(s_i, s_j)$ between the subspaces s_i and s_j and not the subspaces themselves. Using conditional probabilities, we have:

$$Pr[E_{i,j}] \leq \sum_{k=1}^{\ell} \Big[Pr[E_{i,j} | d(s_i, s_j) = k] \times Pr[d(s_i, s_j) = k]\Big] \tag{6}$$

The expression for $Pr[d(s_i, s_j) = k]$ is given in (1). For the first part of the expression, using (4) we have:

$$Pr[E_{i,j} | d(s_i, s_j) = k] = \left[1 - \frac{|\mathcal{S}|}{|\mathcal{P}(\mathcal{W}, \ell)|}\right] \cdot \frac{|\xi_\rho(s_i, s_j)|}{|\mathcal{P}(\mathcal{W}, \ell)|} \Bigg|_{d(s_i, s_j) = k}$$

which, using Lemma 1, gives us:

$$Pr[E_{i,j} | d(s_i, s_j) = k] \leq \left[1 - \frac{|\mathcal{S}|}{|\mathcal{P}(\mathcal{W}, \ell)|}\right] \cdot \frac{\zeta(k, 2\rho)}{|\mathcal{P}(\mathcal{W}, \ell)|}$$

For the non-trivial case, combining these two expressions in (6), gives the expression of Lemma 2. ■

Proof of Theorem 3. For the probability of the event that a randomly generated set $\mathcal{S}$ of size $|\mathcal{S}|$ defines a $(\rho, 2)-$ list decodable code, we have:

$$Pr\left[\bigcup_{\{i,j\} \in \binom{[|\mathcal{S}|]}{2}} E_{i,j}\right] > 0 \tag{7}$$

By the inclusion exclusion principle, we get the expression as in (8). Notice that given the random choice of elements in the set $\mathcal{S}$, the expression in (8) can be simplified to the expression of (9). Using condition (7) over the expression of (9), we have that the randomly generated set $\mathcal{S}$ defines a $(\rho, 2)$-list-decodable code of maximal size $|\mathcal{S}|$ if it satisfies:

$$\sum_{\{i,j\} \in \binom{[|\mathcal{S}|]}{2}} \Big[Pr\big[E_{i,j}\big]\Big] - \sum_{\substack{\{i,j\},\{m,n\} \in \binom{[|\mathcal{S}|]}{2}; \\ \{i,j\} \neq \{m,n\}}} \Big[Pr\big[E_{i,j}\big]\Big]^2 > 0$$

The first summation sign in the above expression is simply the choice of two indices among $|\mathcal{S}|$ possible indices and the second summation sign is the choice of pairs of indices among all possible pairs. Hence, the expression can be written as:

$$\binom{|\mathcal{S}|}{2} \Big[Pr\big[E_{i,j}\big]\Big] - \binom{\binom{|\mathcal{S}|}{2}}{2} \Big[Pr\big[E_{i,j}\big]\Big]^2 > 0$$

$$Pr\left[\bigcup_{\{i,j\}\in\binom{[|\mathcal{S}|]}{2}} E_{i,j}\right] \geq \sum_{\{i,j\}\in\binom{[|\mathcal{S}|]}{2}} \Big[Pr\big[E_{i,j}\big]\Big] - \sum_{\{i,j\},\{m,n\}\in\binom{[|\mathcal{S}|]}{2};\{i,j\}\neq\{m,n\}} \Big[Pr\big[E_{i,j}\cap E_{m,n}\big]\Big] \tag{8}$$

$$Pr\left[\bigcup_{\{i,j\}\in\binom{[|\mathcal{S}|]}{2}} E_{i,j}\right] \geq \sum_{\{i,j\}\in\binom{[|\mathcal{S}|]}{2}} \Big[Pr\big[E_{i,j}\big]\Big] - \sum_{\{i,j\},\{m,n\}\in\binom{[|\mathcal{S}|]}{2};\{i,j\}\neq\{m,n\}} \Big[Pr\big[E_{i,j}\big]\Big]^2 \tag{9}$$

which, after simplification and using Lemma 2 becomes:

$$\frac{1}{2}\left[\binom{|\mathcal{S}|}{2}-1\right]\left[1-\frac{|\mathcal{S}|}{|\mathcal{P}(\mathcal{W},\ell)|}\right]\cdot\left[\frac{\sum_{k=1}^{\ell}\boldsymbol{P}(k).\zeta(k,2\rho)}{|\mathcal{P}(\mathcal{W},\ell)|}\right]\leq 1$$

The above condition is slightly weaker than:

$$\frac{1}{2}\binom{|\mathcal{S}|}{2}\left[\frac{\sum_{k=1}^{\ell}\boldsymbol{P}(k).\zeta(k,2\rho)}{|\mathcal{P}(\mathcal{W},\ell)|}\right]<1$$

which by using the fact that:

$$\binom{|\mathcal{S}|}{2}<\frac{(|\mathcal{S}|-0.5)^2}{2}$$

shows the existence of a subspace code that is $(\rho,2)$- list decodable and is of size given by the expression in Theorem 3, thereby establishing a lower bound on the size of $(\rho,2)$- list decodable codes. □

VII. Proof for Theorem 4 (Sketch)

Given a triple of indices $\{i,j,m\}\in\binom{[|\mathcal{S}|]}{3}$ of elements from set $\mathcal{S}$, let $E_{i,j,m}$ be the event that the created set $\mathcal{S}$ is such that there exists a subspace s such that $s\in\chi_\rho(s_i,s_j)\bigcap\chi_\rho(s_m,s_m)$. Let $E^c_{i,j,m}$ denote the complement of the event $E_{i,j,m}$. Then, from Theorem 2, the event:

$$\bigcap_{\{i,j,m\}\in\binom{[|\mathcal{S}|]}{3}} E^c_{i,j,m}$$

is the event that the generated set $\mathcal{S}$ is a $(\rho,2)$- list decodable code. The existence of a $(\rho,2)$- list-decodable code of size $|\mathcal{S}|$ then amounts to showing that:

$$Pr\left[\bigcap_{\{i,j,m\}\in\binom{[|\mathcal{S}|]}{3}} E^c_{i,j,m}\right]>0$$

Lemma 3: The probability of occurrence of event $E_{i,j,m}$ is independent of the particular choice of subspaces s_i, s_j and s_m. Moreover, the probability is bounded above as:

$$Pr[E_{i,j,m}]\leq\left[\frac{\sum_{k=1}^{\ell}\boldsymbol{P}(k)\cdot\zeta(k,\rho)}{|\mathcal{P}(\mathcal{W},\ell)|}\right]\times\left[\sum_{k=1}^{\rho}\boldsymbol{P}(k)\right]$$

Proof of Theorem 4 (Sketch, see [10] for complete proof). For the probability of the event that a randomly selected set $\mathcal{S}$ of size $|\mathcal{S}|$ defines a $(\rho,2)-$ list decodable code, we have:

$$Pr\left[\bigcap_{\{i,j,m\}\in\binom{[|\mathcal{S}|]}{3}} E^c_{i,j,m}\right]=1-Pr\left[\bigcup_{\{i,j,m\}\in\binom{[|\mathcal{S}|]}{3}} E_{i,j,m}\right]$$

Hence, an equivalent existence condition for a $(\rho,2)-$ list decodable code of size $|\mathcal{S}|$ is:

$$Pr\left[\bigcup_{\{i,j,m\}\in\binom{[|\mathcal{S}|]}{3}} E_{i,j,m}\right]<1$$

Furthermore, by application of the union bound and using Lemma 3 with algebraic manipulation leads to the resulting expression. □

VIII. Conclusion

In this paper, we have considered the problem of characterizing combinatorial bounds for list decoding of subspace codes. In particular, we have derived lower and upper bounds on the size of subspace codes for the first relaxation of bounded minimum distance decoding, *i.e.*, when the worst-case list size is restricted to two. The main technique used to characterize the bounds is generalization of sphere-covering and sphere-packing coditions to volume-covering and volume packing conditions respectively. The resulting bounds have been compared to the bounds for unique decoding, demonstrating a significant increase in the decoding radius even for the first relaxation.

References

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

[2] R. Koetter and F. Kschischang, “Coding for errors and erasures in random network coding,” *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, August 2008.

[3] P. Elias, “List decoding for noisy channels,” Research Laboratory of Electronics, Massachusetts Institute of Technology, MA, USA, Tech. Rep. 335, pp. 94-104, 1957.

[4] J. M. Wozencraft, “List decoding,” Research Laboratory of Electronics, Massachusetts Institute of Technology, Quarterly Progress Report 48:90-95, 1958.

[5] V. Guruswami, *List Decoding of Error-Correcting Codes*. USA: PhD Thesis, Massachusetts Institute of Technology (Lecture Notes in Computer Science, Vol. 3282), 2005.

[6] V. Guruswami and M. Sudan, “Improved decoding of Reed-Solomon and algebraic-geometric codes,” *IEEE Transactions Information Theory*, vol. 45, no. 6, pp. 1757–1767, September 1999.

[7] R. J. McEliece. (2003) The Guruswami-Sudan decoding algorithm for Reed-Solomon codes. [Online]. Available: http://www.systems.caltech.edu/EE/Faculty/rjm/papers/RSD-JPL.pdf

[8] J. H. van Lint, *Introduction to Coding Theory*. New York, NY: Springer Verlag, 1999.

[9] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*. New York, NY: Springer Verlag, 1989.

[10] R. Agarwal, “Combinatorial bounds for decoding of codes in finite-field Grassmannian beyond the minimum distance bound,” University of Illinois at Urbana-Champaign, IL, USA, Tech. Rep., 2009. [Online]. Available: http://www.ifp.illinois.edu/~agarwa16/pubs/bounds.pdf