Combinatorial Bounds for List Decoding of Subspace Codes

(Extended Version)

Rachit Agarwal*

August 10th, 2009
(Earlier tech report: August 2008)

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 unconditionally secure authentication codes and 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.

In this paper, we initiate the study 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-packing (sphere-covering) conditions to volume-packing (volume-covering) conditions, which can be of independent interest.

*Coordinated Science Laboratory, Dept. of Electrical and Computer Engineering, University of Illinois, Urbana, IL 61801. Email: agarwal6@uiuc.edu. An extended version of the paper is available at http://www.ifp.uiuc.edu/~agarwal6/
1 Introduction

Consider a communication network modeled as a directed multi-graph with edges of unit capacity. For communication between a single-source and a single-destination, the min-cut max-flow theorem establishes that the maximum amount of information that the source can communicate to the destination per unit time is equal to the size of the min-cut between the source and the destination \[1\]. Moreover, this can be achieved by intermediate nodes in the network simply forwarding the incoming packets (referred to as routing) on well-defined paths between the source and the destination. However, if the source wishes to communicate the information to a set of receivers, there exist networks in which capacity cannot be achieved using such a routing scheme \[2\]. The theory of network coding \[2, 3\] establishes that if the nodes in the network are allowed to generate new packets by performing algebraic operations on the incoming information packets, then the achievable throughput is generally higher than what can be achieved by routing schemes. In fact, if each receiver has the same min-cut from the source, the intermediate nodes are only required to perform linear operations on the incoming packets in order to achieve the capacity of the network \[4\].

Of particular interest are so-called random network coding schemes \[5\], that allow intermediate nodes to generate linear combination of the incoming packets with randomly chosen coefficients, thus providing a completely distributed scheme that achieves optimal capacity with high probability. The standard assumption in these works is that no errors are introduced into the network. However, a number of error sources (e.g., malicious or malfunctioning nodes) cannot be neglected. Random network coding, due to its nature of random combination of packets at any given node, is highly susceptible to such error sources. Indeed, a single error introduced in the network may render the whole transmission useless when the erroneous packet is combined with other received packets. The problem of error control in random network coding, hence, is of particular importance.

Recently, Kötter and Kschischang developed the theory of subspace codes for error correction in random network coding \[6\]. Essentially, the idea of subspace codes is based on the observation that if the transmitted packets are represented as a matrix, the random linear operations at intermediate nodes preserve the row space of the transmitted matrix. Kötter and Kschischang, hence, consider the transmission of information not via choice of the transmitted matrix but by the choice of the vector space spanned by the rows of the transmitted matrix. Under this model, the network takes in a vector space \(U\) and puts out another vector space \(V\), possibly with erasures (deletion of vectors from the transmitted space) or errors (addition of vectors to the transmitted space). Kötter and Kschischang showed that correct decoding is possible with a Bounded Minimum Distance (BMD) decoder if the dimension of the space \(U \cap V\) is sufficiently large, or equivalently, if the distance (under an associated metric) between the transmitted and the received subspace is less than half the minimum distance of subspace code (defined shortly). The central trade-off in this theory, akin to the trade-off in standard coding theory literature, is the one between the amount of redundancy needed (captured in the size, or equivalently the rate, of the code) and the fraction of errors that can be corrected (captured in the minimum distance of the code).

Let \(S\) denote a subspace code and let \(D(S)\) be the minimum distance of the code. From the discussion above, it is desirable to have a subspace code with large minimum distance \(D(S)\) and large code size \(|S|\). It is easy to see that these are conflicting requirements, in that increasing the size of the code may possibly reduce the minimum distance of the code. However, this conflict is due to the fact that we are insisting on having an unique output: a BMD decoder for a subspace code \(S\) with a minimum distance \(D(S)\) is guaranteed to output an unique codeword (correct all errors in the received information) as long as the decoding radius (number of errors that can be corrected) \(\rho < [(D(S) - 1)/2]\). But this is an overly pessimistic estimate of the decoding radius, since the way subspaces pack in space, for most choices of the received word there will be at most one codeword within distance \(\rho\) from it even for \(\rho\) much greater than \([(D(S) - 1)/2]\). 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 roughly $\left\lfloor (D(S) - 1)/2 \right\rfloor$ from them. List decoding provides a clean way to get around this predicament, and yet deal with worst-case error patterns. In list decoding, the output of the decoder is a list of possible codewords. The decoding process is considered to be successful if the output list contains the transmitted codeword.

List decoding has been studied for codes defined on Hamming spaces and dates back to the late 1950’s [7, 8]. For codes defined on Hamming space, it has been shown that list decoding allows increase in the decoding radius (code-rate) for a specified code-rate (decoding radius) [9, 10]. For carefully constructed codes like Reed-Solomon codes, the increase in decoding radius is quite significant [11, 10, 12] 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 [12].

1.1 Our Contribution

Motivated by the above discussion, we initiate the study of list decoding subspace codes. Similar to [6], we mainly work with subspace codes in which each codeword has the same dimension (referred to as constant-dimension codes or codes on finite-field Grassmannian). More so, because these codes have certain structural properties that allow the study of combinatorial bounds using literature from distance-regular graphs. In this paper, we restrict our attention to the first relaxation of BMD decoding, i.e., when the worst-case list size is restricted to two and present lower and upper bounds on the size of codes on finite-field Grassmannian under such a restriction. Our results are non-constructive, but present a first step towards the study of list decoding of codes in finite-field Grassmannian. At the heart of our construction is a generalization of the well-known Sphere-covering and Sphere-packing bounds to covering and packing of volumes. The conditions are easily generalizable to incorporate lists of larger sizes and a similar construction suffices to derive lower and upper bounds for any general list size, given that one can compute (or bound by above) “generalized intersection numbers” defined later.

1.2 Organization

The remainder of the paper is organized as follows. We briefly introduce codes on finite-field Grassmannian and recall some of the properties of these codes in Section 2. In Section 3, we give some definitions and notations that allow us to succinctly state our results. We formally state our results in Section 4 and provide an overview of the proof. Section 5 introduces the volume-covering and volume-packing conditions and covers basic lemmas that help us formulate the conditions to derive the bounds in the following sections. We derive a lower bound for decoding subspace codes beyond the minimum distance bound in Section 6. The upper bounds for the case of worst case list size restricted to two are derived in Section 7. We close the paper with some final remarks in Section 8.

2 Codes on Finite-Field Grassmannian [6]

Consider an information network given by a directed graph $G = (\mathcal{V} \cup s, \mathcal{E})$, where a source $s$ wishes to multicast some information to a set of terminals $T \subseteq \mathcal{V}$. 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 [5], these vectors are injected by $s$ into $G$. 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 $h_{j,i} \in \mathbb{F}_q$.
\( \mathbb{F}_q \). Now assume the injection of \( T \) erroneous packets by the network. In such a case, the model is extended to include error packets \( e_t, t = 1, \ldots, T \) to give \( y_j = \sum_{i=1}^{M} h_{i} p_i + \sum_{t=1}^{T} g_{j,t} e_t \), where again \( g_{j,t} \in \mathbb{F}_q \) are unknown random coefficients. The transmission model when written in a matrix form appears as \( y = H \cdot p + G \cdot e \), where \( H \) and \( G \) are random \( L \times M \) and \( L \times T \) matrices, respectively, \( p \) is the \( M \times N \) matrix whose rows are the transmitted vectors, \( y \) is the \( L \times N \) matrix whose rows are the received vectors, and \( e \) is the \( T \times N \) matrix whose rows are the error vectors. In absence of errors, since \( H \) is a random matrix, the product \( Hp \) conserves the row space of \( p \). In presence of errors, then, the network takes in a vector space \( U \) and puts out another vector space \( V \), possibly with erasures (deletion of vectors from the transmitted space) or errors (addition of vectors to the transmitted space).

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 \( \text{dim}(V) \). The sum of two subspaces \( U, V \) of \( \mathcal{W} \) is the smallest subspace of \( \mathcal{W} \) containing both \( U \) and \( V \). It was shown in [6] that the function \( d(A, B) := \text{dim}(A + B) - \text{dim}(A \cap B) = \text{dim}(A) + \text{dim}(B) - 2\text{dim}(A \cap B) \) is a metric for the space \( \mathcal{P}(\mathcal{W}) \). Of interest to us are those subsets of the projective geometry of \( \mathcal{W} \) that contains all subspaces of the same dimension.

The \( \ell \)-dimensional projective geometry of \( \mathcal{W} \), denoted by \( \mathcal{P}(\mathcal{W}, \ell) \), is the set of all \( \ell \)-dimensional subspaces of \( \mathcal{W} \). For any two subspaces \( A, B \in \mathcal{P}(\mathcal{W}, \ell) \), we have that \( d(A, B) = 2(\ell - \text{dim}(A \cap B)) \). We will frequently drop the factor of 2 since it does not play any role in our formulation and say that the distance between \( A \) and \( B \) is \( (\ell - \text{dim}(A \cap B)) \) units. Codes defined on finite-field Grassmannian are nonempty subsets of \( \mathcal{P}(\mathcal{W}, \ell) \), i.e., nonempty collection of \( \ell \)-dimensional subspaces of \( \mathcal{W} \). The size of a code \( S \) is denoted by \( |S| \). A subspace code \( S \) is said to be of type \( [N, \ell, \log_q |S|, D(S)] \), where \( \ell \) is the dimension of the codewords of \( S \) and \( D(S) \) is the minimum distance of \( S \) defined as \( D(S) = \min_{s_1, s_2 \in S, s_1 \neq s_2} d(s_1, s_2) \). For subspace codes, transmitting a space \( V \in S \) would require the transmitter to inject up to \( \ell \) (basis) vectors from \( V \) into the network, corresponding to the transmission of \( N \ell q \)-ary symbols. Hence, the rate \( R \) of the code is defined by \( R = \log_q (|S|)/N \ell \).

Codes in finite-field Grassmannian are analogous to constant-weight codes in Hamming space (in which each codeword has constant Hamming weight) or to spherical codes in Euclidean space (in which each codeword has constant energy). They also exhibit interesting structural properties that allow borrowing tools from graph theory to study the performance and construction of these codes. In particular, we have the following fact:

**Fact 2.1 [13]** The \( \ell \)-dimensional projective geometry of an \( N \)-dimensional space \( \mathcal{W} \) constitutes a distance-regular graph \( G_{\mathcal{W}, \ell} \), known as Grassmann graph. \( G_{\mathcal{W}, \ell} \) 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 \( \ell \) dimensional subspaces of an \( N \)-dimensional ambient space over \( \mathbb{F}_q \) and is given by the so-called Gaussian coefficient \( \left| \mathcal{P}(\mathcal{W}, \ell) \right| = \left[ \begin{array}{c} N \\ \ell \end{array} \right]_q \).

We also recall the following result regarding Grassmannian graphs which will be useful in our analysis in the following sections:

**Fact 2.2 [13][6]** The number of subspaces \( V \) at distance \( k \) from a given subspace \( U \) is independent of the subspace \( U \) itself and is given by: \( \# \{ V \in \mathcal{P}(\mathcal{W}, \ell) : d(U, V) = k \} = q^{k^2 \left[ \begin{array}{c} N-\ell \\ k \end{array} \right]} \left[ \begin{array}{c} \ell \\ k \end{array} \right] \).
3 Definitions

In this section, we give definitions that allow us to succinctly state our results in the next section.

Denote by $P(k)$ the probability that any two randomly chosen subspaces $s_i, s_j \in \mathcal{P}(W, \ell)$ are at distance $k$. Using Fact 2.2, we have that:

$$P(k) = \Pr[d(s_i, s_j) = k] = \left[ \frac{q^k \binom{N-\ell}{\ell}}{|\mathcal{P}(W, \ell)|} \right]$$

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

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

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:

$$d(U, Z) = \min\{d(U, V) : U \in \mathcal{P}(W, \ell), V \in Z \subseteq \mathcal{P}(W, \ell) \}$$

**Definition 3.1 ($\rho, L$)-List-decodable Code** Let $\rho$ and $L$ be positive integers. A subspace code $S \subseteq \mathcal{P}(W, \ell)$ is said to be $(\rho, L)$-list-decodable if for every $U \in \mathcal{P}(W, \ell)$, the Grassmannian ball of radius $\rho$ centered at $U$ contains at most $L$ codewords of $S$. In other words, for a $(\rho, L)$-list-decodable code, we have:

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

The parameter $\rho$ is called the list decoding radius and the parameter $L$ is called the list size.

We introduce two volumes generated by the intersection of Grassmannian balls of certain specified radius with centers as two subspaces $U, V \in \mathcal{P}(W, \ell)$. These volumes, referred to as set functions $\chi_z(U, V)$ and $\xi_z(U, V)$, are defined as follows:

**Definition 3.2** Given two subspaces $U, V \in \mathcal{P}(W, \ell)$ and a non-negative integer $z$, the set $\chi_z(U, V)$ is simply the volume generated by the intersection of the Grassmannian Balls of radius $z$ centered at $U$ and $V$, i.e.,

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

**Definition 3.3** Given a pair of subspaces $U, V \in \mathcal{P}(W, \ell)$ and a non-negative integer $z$, $\xi_z(U, V)$ is defined as:

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

The set $\chi_z(U, V)$ is non-empty as long as the Grassmannian balls $B(U, z)$ and $B(V, z)$ are not disjunct, i.e., $\exists s \in \mathcal{P}(W, \ell)$, such that $d(s, U) \leq z$ and $d(s, V) \leq z$. 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 $\mathcal{P}(W, \ell)$ 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 $(U, V)$.

**Definition 3.4 (Intersection Number, Intersection Size)** For any pair of subspaces $U, V \in \mathcal{P}(W, \ell)$ with $d(U, V) = \delta$, their intersection number is defined as:

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

We define the Intersection size $\zeta$ as:

$$\zeta(\delta, z) = \sum_{i=1}^{z} \sum_{j=1}^{z} \lambda_{i,j}(\delta) = |B(U, z) \cap B(V, z)|$$
**Fact 3.1** ([13]) 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 \( \delta \) between \( u \) and \( v \) and not the specific choice of vertices.

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

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.

### 4 Our Results

We give a formal statement of our results below:

**Theorem 4.1 (Volume-Covering Condition)** The collection of subspaces \( S = \{ s_i : s_i \in \mathcal{P}(W, \ell) \} \) of length \(|S|\) defines a subspace code that is \((\rho, 2)\)-list decodable if \( \forall t \in [|S|/\{i, j\}], \) we have \( s_t \notin \xi_\rho(s_i, s_j), \forall \{i, j\} \in \binom{[|S|]}{2} \).

**Theorem 4.2 (Volume-Packing Condition)** The collection of subspaces \( S = \{ s_i : s_i \in \mathcal{P}(W, \ell) \} \) of length \(|S|\) defines a subspace code that is \((\rho, 2)\)-list decodable if for every \( i, j, m \in [|S|], \) we have:

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

**Theorem 4.3 (Lower Bound)** There exists a subspace code of size \(|S|\) that is \((\rho, 2)\)-list decodable, if the following condition is satisfied:

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

**Theorem 4.4 (Upper Bound)** There exists a code defined on finite-field Grassmannian of size \(|S|\) that is \((\rho, 2)\)-list decodable, if the following condition is satisfied:

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

Bounds on the size of the subspace codes for the case of BMD decoding are presented in [6]. Fig. 1 compares the performance of our bounds to the bounds for BMD decoding for a certain set of parameters. For all parameters, the lower bound of Theorem 4.3 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 (see appendix).
5 Volume Covering and Volume Packing Conditions

Theorem 4.1 and Theorem 4.2 give generalizations of standard sphere-covering and sphere-packing conditions for the case of BMD decoding [14] to volume-covering and volume-packing conditions for $(\rho, 2)$-list decodability. In this section, we provide formal proofs of correctness of Theorem 4.1 and Theorem 4.2. 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.

Volume Covering Conditions

Proof of Theorem 4.1. We first show that the set $S$ actually defines a code, which when decoded up to radius $\rho$ outputs a list of no more than two codewords. From the definition of list-decodability, this requires that a Grassmannian ball of radius $\rho$ around any space in $P(W, \ell)$ must contain at most two codewords. Intuitively, recall that for any two subspaces $s_i, s_j$ in the set $S$, 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 $S$, then the code $S$ 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 $S$ and a subspace $s_t \in S$ such that $s_t \in \xi_\rho(s_i, s_j)$ for some $s_i, s_j \in S$. 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 $S$ is a $(\rho, 2)$-list-decodable code.

Finally, we note that for any set $S$ that complies with the theorem, $s_i, i \in |S|$ will be distinct. To see this, assume that $s_i = s_j$ for some $i, j \in |S|$. Let $s_t \in S, t \in |S|$. 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 $S$ are distinct and so, $S$ defines a code of size $|S|$.

Volume Packing Condition

**Proof of Theorem 4.2** Assume that there exists some $s_m \in S$ such that $\chi_\rho(s_i, s_j) \cap \chi_\rho(s_m, s_m) \neq \phi$. Then, there will exist a received subspace $s_r \in \mathcal{P}(W, \ell)$ 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 $\rho$. This contradicts the condition that the worst-case list size is restricted to two. Hence the proof.

**Remark 5.1** Notice the equivalence of conditions for sphere covering bound for unique decoding and for decoding under list size two restriction in Theorem 4.1. Indeed, if $s_i$ and $s_j$ in the condition of Theorem 4.1 coincide, the condition states that the projective geometry must be contained in the union of all Grassmannian Balls of radius $2\rho = D(C) - 1$, where $D(C) = 2\rho + 1$ 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 4.2 for the upper bound, the condition states that all the spheres of radius $\rho$ in the projective geometry must be disjoint, precisely the sphere-packing bound condition.

Hence, the conditions used for deriving the upper and lower bounds for decoding of codes on finite-field Grassmannian are natural extensions of the sphere-covering and sphere-packing bounds for BMD decoding.

More on the two volumes

Using the intersection number $\lambda_{i,j}(\delta)$, we can bound $|\chi_z(U, V)|$ for any pair of subspaces $U, V \in \mathcal{P}(W, \ell)$ such that $d(U, V)$ satisfies $0 < k \leq 2\rho$.

**Claim 5.2** For any pair of subspaces $U, V \in \mathcal{P}(W, \ell)$ and a positive integer $z$, the size of the set $\chi_z(U, V)$ is given by

$$|\chi_z(U, V)| \big|_{d(U,V) = \delta} = \sum_{i=1}^{\zeta} \sum_{j=1}^{\zeta} \lambda_{i,j}(\delta)$$

**Lemma 5.3** For any pair of subspaces $U, V \in \mathcal{P}(W, \ell)$ and a non-negative integer $z$, the following holds:

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

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

\[
d(U, X) \leq d(U, X') + d(X', X) \leq z + z = 2 \cdot z
\]

\[
d(V, X) \leq d(V, X') + d(X', X) \leq z + z = 2 \cdot z
\]

Hence, every subspace \(X \in \xi(U, V)\) is also a member of \(\chi_{2z}(U, V)\). In other words, \(\xi(U, V) \subseteq \chi_{2z}(U, V)\), or, \(|\xi(U, V)| \leq |\chi_{2z}(U, V)|\). The correctness of the lemma follows by using Claim 5.2 and Definition 3.4.

\[\] 6 Lower Bound

Let \(E_{i,j}\) be the event that the created set \(S\) is such that a randomly selected subspace from the set \(\mathcal{P}(W, \ell)\) is contained in two volumes, \(\xi_s(s_i, s_j)\) and \(\mathcal{P}(W, \ell) - S\) (not contained in \(S\)). Then, the event:

\[
\bigcup_{\{i,j\} \in \binom{[M]}{2}} E_{i,j}
\]

(3)

generates a set \(S\) such that if a randomly selected subspace from \(\mathcal{P}(W, \ell)\) is contained in any of the \(\xi(s_i, s_j), \{i, j\} \in \binom{[M]}{2}\), then it is contained in \(\mathcal{P}(W, \ell) - S\) (and hence, not contained in \(S\), in accordance with Theorem 4.1).

\[\]

**Lemma 6.1** 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:

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

(4)

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

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

(5)

\[
= \frac{\xi_s(s_i, s_j)}{|\mathcal{P}(W, \ell)|} \cdot \left[1 - \frac{M}{|\mathcal{P}(W, \ell)|}\right]
\]

Recall that the \(\ell\)-dimensional projective geometry \(\mathcal{P}(W, \ell)\) constitutes a distance-regular graph. Hence, the above expression, dependent on cardinality of the set \(\xi(s_i, s_j)\), 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:

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

(6)

The expression for \(\Pr[d(s_i, s_j) = k]\) is given in (1). For the first part of the expression, using (5) we have:

\[
\Pr[E_{i,j} | d(s_i, s_j) = k] = \left[1 - \frac{M}{|\mathcal{P}(W, \ell)|}\right] \cdot \frac{\xi(s_i, s_j)}{|\mathcal{P}(W, \ell)|} \cdot d(s_i, s_j) = k
\]
which, using Lemma 5.3, gives us:

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

For the non-trivial case, combining these two expressions in (6), we get:

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

Hence, the proof.

Before going to the proof of Theorem 4.3, we give a strictly tighter bound which approaches the bound of Theorem 4.3 asymptotically:

**Theorem 6.2** There exists a subspace code of size \(|S|\) that is \((\rho, 2)\)-list decodable, if the following condition is satisfied:

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

**Proof**: For the probability of the event that our experiment produces a \((\rho, 2)\)-list decodable code of maximal size \(M\), we have:

\[
\Pr \left[ \bigcup_{\{i,j\} \in \binom{[M]}{2}} E_{i,j} \right] > 0
\]  

(7)

By the inclusion exclusion principle, we get the following expression:

\[
\Pr \left[ \bigcup_{\{i,j\} \in \binom{[M]}{2}} E_{i,j} \right] \geq \sum_{\{i,j\} \in \binom{[M]}{2}} \Pr[E_{i,j}] - \sum_{\{i,j\}, \{m,n\} \in \binom{[M]}{2}: \{i,j\} \neq \{m,n\}} \Pr[E_{i,j} \cap E_{m,n}]
\]

Notice that given the random choice of elements in the set \(S\), the above expression can be simplified to:

\[
\Pr \left[ \bigcup_{\{i,j\} \in \binom{[M]}{2}} E_{i,j} \right] \geq \sum_{\{i,j\} \in \binom{[M]}{2}} \Pr[E_{i,j}] - \sum_{\{i,j\}, \{m,n\} \in \binom{[M]}{2}: \{i,j\} \neq \{m,n\}} \left[ \Pr[E_{i,j}] \right]^2
\]

Using condition (7) over the above expression, we have that the randomly generated set \(S\) defines a \((\rho, 2)\)-list-decodable code of maximal size \(M\) if it satisfies:

\[
\sum_{\{i,j\} \in \binom{[M]}{2}} \left[ \Pr[E_{i,j}] \right] - \sum_{\{i,j\}, \{m,n\} \in \binom{[M]}{2}: \{i,j\} \neq \{m,n\}} \left[ \Pr[E_{i,j}] \right]^2 > 0
\]

The first summation sign in the above expression is simply the choice of two indices among \(M\) 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:

\[
\binom{M}{2} \left[ \Pr[E_{i,j}] \right] - \binom{M}{2} \left[ \Pr[E_{i,j}] \right]^2 > 0
\]
which is same as:
\[
\binom{M}{2} \left[ \Pr[E_{i,j}] \right] - \frac{1}{2} \binom{M}{2} \left( \binom{M}{2} - 1 \right) \left[ \Pr[E_{i,j}] \right]^2 > 0
\]  
(8)

and can be simplified to:
\[
\frac{1}{2} \left( \binom{M}{2} - 1 \right) \left[ \Pr[E_{i,j}] \right] < 1
\]  
(9)

which from Lemma 6.1 is:
\[
\frac{1}{2} \left( \binom{M}{2} - 1 \right) \left[ \Pr[E_{i,j}] \right] < 1
\]  
(10)

We obtain the proof of Theorem 4.3 as a corollary of Theorem 6.2.

**Proof of Theorem 4.3** We use two facts in the result of Theorem 4.3. First,
\[
\left[ 1 - \frac{M}{|\mathcal{P}(W, \ell)|} \right] < 1
\]
and second:
\[
\binom{|\mathcal{S}|}{2} < \frac{(|\mathcal{S}| - 0.5)^2}{2}
\]

Hence, Theorem 4.3 implies the existence of a code defined on finite-field Grassmannian of size \(|\mathcal{S}|\) that is \((\rho, 2)\)-list-decodable if
\[
\frac{1}{2|\mathcal{P}(W, \ell)|} \left[ \frac{(|\mathcal{S}| - 0.5)^2}{2} \right] \left[ \sum_{k=1}^{\ell} P(k) \zeta(k, \rho) \right] < 1
\]

which is same as:
\[
|\mathcal{S}| < 0.5 + \sqrt{\frac{4 \cdot |\mathcal{P}(W, \ell)|}{\sum_{k=1}^{\ell} P(k) \zeta(k, \rho)}}
\]

shows the existence of a subspace code that is \((\rho, 2)\)-list decodable and is of size given by the expression in Theorem 4.3, thereby establishing a lower bound on the size of \((\rho, 2)\)-list decodable codes.

\[\square\]

### 7 Upper Bound

Given a triple of indices \(\{i, j, m\} \in \binom{[M]}{3}\) 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 \(s \in \chi_\rho(s_i, s_j) \cap \chi_\rho(s_m, s_m)\). Let \(E_{i,j,m}^c\) denote the complement of the event \(E_{i,j,m}\). Then, from Theorem 4.2, the event:
\[
\bigcap_{\{i,j,m\} \in \binom{[M]}{3}} E_{i,j,m}^c
\]
is the event that the random experiment generates a set \(\mathcal{S}\) which defines a \((\rho, 2)\)-list decodable code of size \(M\). The existence of a \((\rho, 2)\)-list-decodable code of size \(M\) then amounts to showing that:
\[
\Pr \left[ \bigcap_{\{i,j,m\} \in \binom{[M]}{3}} E_{i,j,m}^c \right] > 0
\]  
(10)
Lemma 7.1 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:

$$\Pr[E_{i,j,m}] \leq \left[ \frac{\sum_{k=1}^{\ell} \mathcal{P}(k) \cdot \zeta(k, \rho)}{|\mathcal{P}(W, \ell)|} \right] \times \left[ \sum_{k=1}^{\rho} \mathcal{P}(k) \right]$$  \hspace{1cm} (11)

**Proof:** Given the random choice of elements of the set $\mathcal{S}$ out of all possible subspaces in $\mathcal{P}(W, \ell)$, the probability of an element $s \in \mathcal{P}(W, \ell)$ turning up to be in $\chi_\rho(s_i, s_j) \cap \chi_\rho(s_m, s_m)$ is dependent on the cardinality of the space $\chi_\rho(s_i, s_j) \cap \chi_\rho(s_m, s_m)$. Since all of $s_i, s_j, s_m$ are chosen independently, this in turn depends on cardinalities of individual sets $\chi_\rho(s_i, s_j)$ and $\chi_\rho(s_m, s_m)$.

$$\Pr[E_{i,j,m}] = \Pr[\{s \in \chi_\rho(s_i, s_j) \cap \chi_\rho(s_m, s_m)\}]$$

$$= \Pr[\{s \in \chi_\rho(s_i, s_j)\} \cap \{s \in \chi_\rho(s_m, s_m)\}]$$

$$= \Pr[\{s \in \chi_\rho(s_i, s_j)\}] \cdot \Pr[\{s \in \chi_\rho(s_m, s_m)\}]$$

$$= \frac{|\chi_\rho(s_i, s_j)|}{|\mathcal{P}(W, \ell)|} \cdot \frac{|\chi_\rho(s_m, s_m)|}{|\mathcal{P}(W, \ell)|}$$

for all $s \in \mathcal{P}(W, \ell)$ and all $\{i, j, m\} \in (|M|_3)$. Notice that $\chi_\rho(s_m, s_m)$ contains all the codewords that are at distance $\rho$ or less from subspace $s_m$. Recall that this expression is independent of the subspace $s_m$ and can be computed using the expression of (1).

Moreover, using an argument similar to that of Lemma 6.1 it is easy to show that the above expression reduces to:

$$\Pr[E_{i,j,m}] \leq \left[ \sum_{k=1}^{\ell} \mathcal{P}(k) \cdot \frac{\zeta(k, \rho)}{|\mathcal{P}(W, \ell)|} \right] \times \left[ \sum_{k=1}^{\rho} \mathcal{P}(k) \right]$$  \hspace{1cm} (12)

**Proof of Theorem 4.4** For the probability of the event that our experiment produces a $(\rho, 2)$-list decodable code of maximal size $M$, we have:

$$\Pr \left[ \bigcap_{\{i,j,m\} \in (|M|_3)} E_{i,j,m}^c \right] = 1 - \Pr \left[ \bigcup_{\{i,j,m\} \in (|M|_3)} E_{i,j,m} \right]$$

Hence, an equivalent existence condition for a $(\rho, 2)$-list decodable code of size $M$ is:

$$\Pr \left[ \bigcup_{\{i,j,m\} \in (|M|_3)} E_{i,j,m} \right] < 1$$  \hspace{1cm} (13)

By the union bound, we have:

$$\Pr \left[ \bigcup_{\{i,j,m\} \in (|M|_3)} E_{i,j,m} \right] \leq \sum_{\{i,j,m\} \in (|M|_3)} \Pr[E_{i,j,m}]$$
which using Lemma 7.1 gives (14).

$$\Pr \left[ \bigcup_{\{i,j,m\} \in \binom{[M]}{3}} E_{i,j,m} \right] \leq \sum_{\{i,j,m\} \in \binom{[M]}{3}} \left[ \frac{\sum_{k=1}^\ell P(k) \cdot \zeta(k, \rho)}{|\mathcal{P}(W, \ell)|} \right] \times \left[ \sum_{k=1}^\rho P(k) \right]$$

(14)

The first summation sign in (14) is simply the choice of three indices among $M$ possible indices. This gives us (15).

$$\Pr \left[ \bigcup_{\{i,j,m\} \in \binom{[M]}{3}} E_{i,j,m} \right] \leq \binom{M}{3} \left[ \frac{\sum_{k=1}^\ell P(k) \cdot \zeta(k, \rho)}{|\mathcal{P}(W, \ell)|} \right] \times \left[ \sum_{k=1}^\rho P(k) \right]$$

(15)

Using the expression in (13), this leads to the following expression for the upper bound on rate for list decoding of codes on finite field Grassmannian for list size restricted to two:

$$\binom{M}{3} \left[ \frac{\sum_{k=1}^\ell P(k) \cdot \zeta(k, \rho)}{|\mathcal{P}(W, \ell)|} \right] \times \left[ \sum_{k=1}^\rho P(k) \right] \leq 1$$

(16)

We get the resulting expression using the fact that: $\binom{M}{3} = \frac{1}{6} M(M-1)(M-2) < \frac{1}{6} (M-1)^3$. □

8 Open Problems

Motivated by the shared secret channel model frequently encountered in message authentication systems and information networks, we have initiated the study of list decoding recently proposed subspace codes. In particular, we have presented lower and upper bounds on achievable code rates for the first relaxation of bounded minimum distance decoding, i.e., when the worst case list size is restricted to two.

At the heart of our construction are generalizations of conditions for sphere-covering and sphere-packing bounds to volume-covering and volume-packing bounds. Our constructions are conceptually simple, present insights on constructing good list decodable subspace codes and is easily generalizable to lists of larger sizes, given that one could bound the generalized intersection numbers for the Grassmannian graph, defined as follows:

**Definition 8.1 (Generalized Intersection Number)** For any $n$ subspaces $s_1, s_2, \ldots, s_n \in \mathcal{P}(W, \ell)$ with $d(s_i, s_j) = \delta_{ij}$, let $\delta$ denote the collection of all the mutual distances between the $n$ subspaces (i.e., $|\delta| = \binom{n}{2}$). Then, the generalized intersection number is defined as:

$$\lambda_{d_1, d_2, \ldots, d_n}(\delta) = \#\{s \in \mathcal{P}(W, \ell) : d(s, s_i) = d_i, \forall i; d(s_i, s_j) = \delta_{ij} \forall \{i, j\} \in \binom{[n]}{2}\}$$
References


Comparison of Gilbert–Varshamov and Non-Asymptotic Lower bound (list size 2) for finite field $F_2$ and $\lambda = \frac{1}{2}$ for $N = 18, 24$

Comparison of Gilbert–Varshamov and Non-Asymptotic Lower bound (list size 2) for finite field $F_4$ and $\lambda = \frac{1}{2}$ for $N = 18, 24$

Comparison of Gilbert–Varshamov and Non-Asymptotic Lower bound (list size 2) for finite field $F_8$ and $\lambda = \frac{1}{2}$ for $N = 18, 24$
Figure 7: Comparison of Gilbert–Varshamov and Non-Asymptotic Packing bound (list size 2) for finite field $\mathbb{F}_8$ and $N = 24$ for $\lambda = \frac{1}{2}, \frac{1}{3}$.

Figure 8: Comparison of Lower and Upper bounds (list size 2) for $\lambda = 1/2$, $N = 24$ for finite field sizes $\mathbb{F}_4, \mathbb{F}_8$. 