Combinatorial lower bound for list decoding of codes in finite-field Grassmannian

Rachit Agarwal

University of Illinois at Urbana-Champaign
ISIT 2011
Randomized network coding
Randomized network coding

Source injects a number of packets
Randomized network coding

Source injects a number of packets

Each intermediate node generates a random linear combination of the incoming packets
Randomized network coding

Source injects a number of packets

Each intermediate node generates a random linear combination of the incoming packets

Collectively seen, operations at intermediate nodes are vector space preserving (in absence of failures)
Randomized network coding

Source injects a number of packets

Each intermediate node generates a random linear combination of the incoming packets

Collectively seen, operations at intermediate nodes are vector space preserving (in absence of failures)

Operator channel: models networks as channels that transmit and receive vector spaces
Subspace codes [KK’08]
Subspace codes [KK’08]

Network error correction
Subspace codes [KK’08]

Network error correction

\( \mathcal{W} \) - A fixed N-dimensional space over \( \mathbb{F}_q \)
Subspace codes [KK’08]

Network error correction

\( \mathcal{W} \) - A fixed N-dimensional space over \( \mathbb{F}_q \)

Projective geometry \( \mathcal{P}(\mathcal{W}) \) - the set of all subspaces of \( \mathcal{W} \)
Subspace codes [KK’08]

\(\mathcal{W}\) - A fixed N-dimensional space over \(\mathbb{F}_q\)

Projective geometry \(\mathcal{P}(\mathcal{W})\) - the set of all subspaces of \(\mathcal{W}\)

A subspace code \(\mathcal{C}\) is a non-empty subset of \(\mathcal{P}(\mathcal{W})\)
Codes on finite-field Grassmannian
Codes on finite-field Grassmannian

Dimension of each codeword is a fixed integer $\ell$
Codes on finite-field Grassmannian

Dimension of each codeword is a fixed integer $\ell$

$\mathcal{P}(\mathcal{W}, \ell)$ - $\ell$-dimensional Projective geometry
Codes on finite-field Grassmannian

Dimension of each codeword is a fixed integer $\ell$

$P(W, \ell)$ - $\ell$-dimensional Projective geometry

A code $\mathcal{C}$ on finite-field Grassmannian
is a non-empty subset of $P(W, \ell)$
Codes on finite-field Grassmannian

Dimension of each codeword is a fixed integer $\ell$

$\mathcal{P}(\mathcal{W}, \ell)$ - $\ell$-dimensional Projective geometry

A code $\mathcal{C}$ on finite-field Grassmannian is a non-empty subset of $\mathcal{P}(\mathcal{W}, \ell)$

Codes on finite-field Grassmannian possess a nice algebraic structure
Grassmannian graph
Codes on finite-field Grassmannian form a subset of vertices of the Grassmannian graph.
Grassmannian graph

Codes on finite-field Grassmannian form a subset of vertices of the Grassmannian graph

Grassmannian graph is a distance-regular graph

interesting algebraic properties that one could exploit
This talk

List decoding of codes on finite-field Grassmannian
This talk

List decoding of codes on finite-field Grassmannian

Focus on list size 2
This talk

List decoding of codes on finite-field Grassmannian

Focus on list size 2

Compute bounds on size of codes that are list decodable
This talk

List decoding of codes on finite-field Grassmannian

Focus on list size 2

Compute bounds on size of codes that are list decodable

Technique
This talk

List decoding of codes on finite-field Grassmannian

Focus on list size 2

Compute bounds on size of codes that are list decodable

Technique

Generalization of sphere-covering condition
This talk

List decoding of codes on finite-field Grassmannian

Focus on list size 2

Compute bounds on size of codes that are list decodable

Technique

Generalization of sphere-covering condition

Exploiting algebraic properties of the Grassmannian graph
Sphere-covering condition
Sphere-covering condition
Sphere-covering condition

Informally

If we draw balls $B(s, \rho)$ of radius $\rho$ around each codeword, any subspace must be contained in at most one sphere.
A code of size $|\mathcal{C}|$ exists if one can pack $|\mathcal{C}|$ spheres without violating the above condition.

Sphere-covering condition

Informally

If we draw balls $\mathcal{B}(s, \rho)$ of radius $\rho$ around each codeword, any subspace must be contained in at most one sphere.

Existence of a code

A code of size $|\mathcal{C}|$ exists if one can pack $|\mathcal{C}|$ spheres without violating the above condition.
Can we generalize Sphere-covering condition in a meaningful way to derive bounds on size of list-decodable codes?
\[ \lambda_{i,j}(\delta) = \left| \{ x \in \mathcal{P}(\mathcal{W}, \ell) : d(x, s) = i ; d(x, s') = j \} \right| \]
Intersection numbers

$$\lambda_{i,j}(\delta) = \left| \{ x \in \mathcal{P}(W, \ell) : d(x, s) = i ; \ d(x, s') = j \} \right|$$

Informally

The number of subspaces that are at distance $i$ from $s$ and at distance $j$ from $s'$.
Intersection numbers

\[ \lambda_{i,j}(\delta) = \left| \left\{ x \in \mathcal{P}(\mathcal{W}, \ell) : d(x, s) = i \ ; \ d(x, s') = j \right\} \right| \]

Informally

The number of subspaces that are at distance \( i \) from \( s \) and at distance \( j \) from \( s' \).
Intersection numbers

\[ \lambda_{i,j}(\delta) = \left| \{ x \in \mathcal{P}(W, \ell) : d(x, s) = i ; d(x, s') = j \} \right| \]

Informally

The number of subspaces that are at distance \( i \) from \( s \) and at distance \( j \) from \( s' \)
Intersection numbers

\[ \lambda_{i,j}(\delta) = \left| \{ x \in \mathcal{P}(\mathcal{W}, \ell) : d(x, s) = i ; d(x, s') = j \} \right| \]

Informally

The number of subspaces that are at distance i from s and at distance j from s'
Intersection numbers

\[ \lambda_{i,j}(\delta) = \left| \{ x \in \mathcal{P}(\mathcal{W}, \ell) : d(x, s) = i ; d(x, s') = j \} \right| \]

Informally:

The number of subspaces that are at distance i from s and at distance j from s'.

Intersection numbers

\[ \lambda_{i,j}(\delta) = \left| \{ x \in \mathcal{P}(W, \mathcal{L}) : d(x, s) = i ; d(x, s') = j \} \right| \]

Informally:

The number of subspaces that are at distance \( i \) from \( s \) and at distance \( j \) from \( s' \).
Intersection numbers

\[ \lambda_{i,j}(\delta) = \left| \{ x \in \mathcal{P}(\mathcal{W}, \ell) : d(x, s) = i ; d(x, s') = j \} \right| \]

Informally

The number of subspaces that are at distance \(i\) from \(s\) and at distance \(j\) from \(s'\)

Can be computed efficiently for distance-regular graphs
\[ \chi_z(s, s') = \mathcal{B}(s, z) \cap \mathcal{B}(s', z) \]
Intersection space

\[ \chi_z(s, s') = \mathcal{B}(s, z) \cap \mathcal{B}(s', z) \]

Informally:

The set of subspaces in the intersection of spheres of radius \( z \) around \( s \) and \( s' \).
Intersection space

\[ \chi_z(s, s') = B(s, z) \cap B(s', z) \]

Informally

The set of subspaces in the intersection of spheres of radius \( z \) around \( s \) and \( s' \)
Intersection space

\[ \chi_z(s, s') = B(s, z) \cap B(s', z) \]

Informally

The set of subspaces in the intersection of spheres of radius \( z \) around \( s \) and \( s' \)
The set of subspaces in the intersection of spheres of radius $z$ around $s$ and $s'$. 

\[ \chi_z(s, s') = B(s, z) \cap B(s', z) \]
Intersection space

\[ \chi_z(s, s') = \mathcal{B}(s, z) \cap \mathcal{B}(s', z) \]

Informally

The set of subspaces in the intersection of spheres of radius \( z \) around \( s \) and \( s' \).
Intersection space

\[ \chi_z(s, s') = \mathcal{B}(s, z) \cap \mathcal{B}(s', z) \]

Informally

The set of subspaces in the intersection of spheres of radius \( z \) around \( s \) and \( s' \)
The set of subspaces in the intersection of spheres of radius $z$ around $s$ and $s'$

$$\chi_z(s, s') = \mathcal{B}(s, z) \cap \mathcal{B}(s', z)$$
Size of Intersection space
Size of Intersection space

\[ \zeta(\delta, z) = |B(s, z) \cap B(s', z)| \bigg|_{d(s, s') = \delta} \]
\[ \zeta(\delta, z) = |\mathcal{B}(s, z) \cap \mathcal{B}(s', z)| \quad \text{if} \quad d(s, s') = \delta \]
The size of intersection space be computed efficiently

$$\zeta(\delta, z) = |B(s, z) \cap B(s', z)| \bigg|_{d(s, s')=\delta}$$

$$|B(s, z) \cap B(s', z)| \bigg|_{d(s, s')=\delta} = \sum_{i=1}^{z} \sum_{j=1}^{z} \lambda_{i,j}(\delta)$$
Another geometric volume
Another geometric volume

$$\xi_z(s, s') = \{x \in \mathcal{P}(W, \ell) : d(x, \chi_z(s, s')) \leq z\}$$
Another geometric volume

\[ \xi_z(s, s') = \{ x \in \mathcal{P}(\mathcal{W}, \ell) : d(x, \chi_z(s, s')) \leq z \} \]
Another geometric volume

\[ \xi_z(s, s') = \{ x \in \mathcal{P}(\mathcal{W}, \ell) : d(x, \chi_z(s, s')) \leq z \} \]
\[ \xi_z(s, s') = \{ x \in \mathcal{P}(\mathcal{W}, \ell) : d(x, \chi_z(s, s')) \leq z \} \]
Another geometric volume

\[ \xi_z(s, s') = \{ x \in \mathcal{P}(W, \ell) : d(x, \chi_z(s, s')) \leq z \} \]
Another geometric volume

\[ \xi_z(s, s') = \{ x \in \mathcal{P}(\mathcal{W}, \ell) : d(x, \chi_z(s, s')) \leq z \} \]

Collection of all subspaces that are within distance \( \rho \) from a subspace in \( \chi_z(s, s') \)
Another geometric volume

\[ \xi_z(s, s') = \{ x \in \mathcal{P}(W, \ell) : d(x, \chi_z(s, s')) \leq z \} \]

**Interpretation**

Collection of all subspaces that are within distance \( \rho \) from a subspace in \( \chi_z(s, s') \)

**Interpretation - II**

Collection of all spheres of radius \( \rho \) that contain the pair of codewords \( s, s' \)
Generalizing sphere-covering condition
The collection of subspaces $\mathcal{S} = \{s_i : s_i \in \mathcal{P}(\mathcal{W}, \ell)\}$ defines a code on finite-field Grassmannian that is $(\rho, 2)$–list decodable if for each pair of $s_i, s_j \in \mathcal{S}$,
$$\xi_\rho(s_i, s_j) \cap \mathcal{S} \leq 2$$
Generalizing sphere-covering condition

The collection of subspaces \( S = \{ s_i : s_i \in \mathcal{P}(W, \ell) \} \) defines a code on finite-field Grassmannian that is \((\rho, 2) - \) list decodable if for each pair of \( s_i, s_j \in S \),

\[
\xi_\rho(s_i, s_j) \cap S \leq 2
\]
The collection of subspaces $\mathcal{S} = \{s_i : s_i \in \mathcal{P}(\mathcal{W}, \ell)\}$ defines a code on finite-field Grassmannian that is $(\rho, 2)$-list decodable if for each pair of $s_i, s_j \in \mathcal{S}$,

$$\xi_\rho(s_i, s_j) \cap \mathcal{S} \leq 2$$

**Informal statement**

The shaded area, corresponding to each pair of codewords, must not contain any other codeword.
For any non-negative integers $z, \delta,$ and any pair of subspaces $s, s' \in \mathcal{P}(\mathcal{W}, \ell)$, with $d(s, s') = \delta$, the size of $\xi_z(s, s')$ is upper bounded as: $|\xi_z(s, s')| \leq \zeta(\delta, 2z)$.
For any non-negative integers $z, \delta$, and any pair of subspaces $s, s' \in \mathcal{P}(W, \ell)$, with $d(s, s') = \delta$, the size of $\xi_z(s, s')$ is upper bounded as: $|\xi_z(s, s')| \leq \zeta(\delta, 2z)$
For any non-negative integers $z, \delta$, and any pair of subspaces $s, s' \in \mathcal{P}(\mathcal{W}, \ell)$, with $d(s, s') = \delta$, the size of $\xi_z(s, s')$ is upper bounded as:

$$|\xi_z(s, s')| \leq \zeta(\delta, 2z)$$
For any non-negative integers $z, \delta$, and any pair of subspaces $s, s' \in \mathcal{P}(\mathcal{W}, \ell)$, with $d(s, s') = \delta$, the size of $\xi_z(s, s')$ is upper bounded as: \[ |\xi_z(s, s')| \leq \zeta(\delta, 2z) \]
Lower Bound
Strategy

Generate a code by randomly selecting $|S|$ subspaces
Generate a code by randomly selecting $|S|$ subspaces.

$E_{i,j} := \text{Event that a randomly selected subspace is contained in } \xi_{\rho}(s_i, s_j) \text{ and not in } S$
Generate a code by randomly selecting $|S|$ subspaces

$E_{i,j} := \text{Event that a randomly selected subspace is contained in } \xi_{\rho}(s_i, s_j) \text{ and not in } S$
Lower Bound

Strategy

Generate a code by randomly selecting $|S|$ subspaces

$E_{i,j} :=$ Event that a randomly selected subspace is contained in $\xi_\rho(s_i, s_j)$ and not in $S$

The code is list decodable if

$$\Pr \left[ \bigcup_{\{i,j\} \in \left( \frac{|S|}{2} \right)} E_{i,j} \right] > 0$$
Lower bound ..
$$Pr[E_{i,j}] \leq \sum_{k=1}^{\ell} \left[ Pr[E_{i,j} | d(s_i, s_j) = k] \times Pr[d(s_i, s_j) = k] \right]$$
Lower bound ..

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

Easy, call it P(k)
Lower bound ..

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

Easy, call it \( P(k) \)
Lower bound ..

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

Easy, call it \( P(k) \)

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

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

Easy, call it \( P(k) \)

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

\[ \Pr[E_{i,j} \mid d(s_i, s_j) = k] \leq \left[ 1 - \frac{|S|}{|P(W, \ell)|} \right] \cdot \frac{\zeta(k, 2\rho)}{|P(W, \ell)|} \]
Lower bound on code size
There exists a code on finite-field Grassmannian $\mathcal{S}$, of size $|\mathcal{S}|$, that is $(\rho, 2)$–list decodable, such that $|\mathcal{S}|$ is lower bounded by:

$$|\mathcal{S}| > 0.5 + \sqrt{\frac{4 \cdot |\mathcal{P}(\mathcal{W}, \ell)|}{\sum_{k=1}^{\ell} P(k) \cdot \zeta(k, 2\rho)}}$$
There exists a code on finite-field Grassmannian $S$, of size $|S|$, that is $(\rho, 2)$ – list decodable, such that $|S|$ is lower bounded by:

$$|S| > 0.5 + \sqrt{\frac{4 \cdot |\mathcal{P}(W, \ell)|}{\sum_{k=1}^{\ell} P(k) \cdot \zeta(k, 2\rho)}}$$
There exists a code on finite-field Grassmannian $\mathcal{S}$, of size $|\mathcal{S}|$, that is $(\rho, 2)$ – list decodable, such that $|\mathcal{S}|$ is lower bounded by:

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

Intersection numbers
Summary

Intersection numbers

Intersection volume
Summary

- Intersection numbers
- Intersection volume
- Generalization of sphere-covering condition
Intersection numbers

Intersection volume

Generalization of sphere-covering condition

Used intersection size to approximate size of the new volume
Summary

Intersection numbers
Intersection volume
Generalization of sphere-covering condition
Used intersection size to approximate size of the new volume

Random coding argument to establish the lower bound on size of list-decodable codes
Open problems
Open problems

Combinatorial side
- Closed form expression, asymptotic analysis
- generalizing to larger list sizes
- design of “good” list decodable codes
Open problems

Combinatorial side
- Closed form expression, asymptotic analysis
- generalizing to larger list sizes
- design of “good” list decodable codes

Algorithmic side
- design of list decoding algorithms
(Mahdavifar & Vardy, ISIT 2010)
Open problems

Combinatorial side
- Closed form expression, asymptotic analysis
- Generalizing to larger list sizes
- Design of “good” list decodable codes

Algorithmic side
- Design of list decoding algorithms
  (Mahdavifar & Vardy, ISIT 2010)

Generalization to general subspace codes - do they possess interesting list decodability properties?