Grassmannian Codes and Quasirandom Hypergraphs

Simon R. Blackburn

Jount work with Tuvi Etzion

Royal Holloway
University of London

9th July 2012

Grassmannian codes

The Grassmannian $\mathcal{G}_q(\ell, k)$ is the set of all k-dimensional subspaces of $\mathbb{F}_q^\ell$.

Grassmannian codes

The Grassmannian $\mathcal{G}_q(\ell, k)$ is the set of all k-dimensional subspaces of $\mathbb{F}_q^\ell$. For $U, V \in \mathcal{G}_q(\ell, k)$, define

$$d(U, V) = 2k - 2\dim(U \cap V).$$

Grassmannian codes

The Grassmannian $\mathcal{G}_q(\ell, k)$ is the set of all k-dimensional subspaces of $\mathbb{F}_q^\ell$. For $U, V \in \mathcal{G}_q(\ell, k)$, define

$$d(U, V) = 2k - 2\dim(U \cap V).$$

A set $\mathbb{C} \subseteq \mathcal{G}_q(\ell, k)$ is a Grassmannian code of minimum distance d if $d(U, V) \geq d$ for all $U, V \in \mathbb{C}$.

Grassmannian codes

The Grassmannian $\mathcal{G}_q(\ell, k)$ is the set of all k-dimensional subspaces of $\mathbb{F}_q^\ell$. For $U, V \in \mathcal{G}_q(\ell, k)$, define

$$d(U, V) = 2k - 2\dim(U \cap V).$$

A set $\mathbb{C} \subseteq \mathcal{G}_q(\ell, k)$ is a Grassmannian code of minimum distance d if $d(U, V) \geq d$ for all $U, V \in \mathbb{C}$.

Combinatorial problem

When ℓ, k and a distance d are fixed, find the size $\mathcal{A}_q(\ell, d, k)$ of the largest Grassmannian code of minimum distance d in $\mathcal{G}(\ell, k)$.

Grassmannian codes

The Grassmannian $\mathcal{G}_q(\ell, k)$ is the set of all k-dimensional subspaces of $\mathbb{F}_q^\ell$. For $U, V \in \mathcal{G}_q(\ell, k)$, define

$$d(U, V) = 2k - 2\dim(U \cap V).$$

A set $\mathbb{C} \subseteq \mathcal{G}_q(\ell, k)$ is a Grassmannian code of minimum distance d if $d(U, V) \geq d$ for all $U, V \in \mathbb{C}$.

Combinatorial problem

When ℓ, k and a distance d are fixed, find the size $\mathcal{A}_q(\ell, d, k)$ of the largest Grassmannian code of minimum distance d in $\mathcal{G}(\ell, k)$.

Koetter and Kschischang (2008) give applications to network coding.

Upper bounds

Important observation

A Grassmannian code $\mathcal{C}$ has minimum distance $2\delta + 2$ or more if and only if no subspace of dimension $k - \delta$ is contained in distinct $U, V \in \mathbb{C}$.

Upper bounds

Important observation

A Grassmannian code $\mathcal{C}$ has minimum distance $2\delta + 2$ or more if and only if no subspace of dimension $k - \delta$ is contained in distinct $U, V \in \mathbb{C}$.

Proof.

$$d(U, V) = 2k - 2\dim(U \cap V)$$

so $d(U, V) \leq 2\delta$ if and only if $\dim(U \cap V) \geq k - \delta$. $\square$

Upper bounds

Important observation

A Grassmannian code $\mathcal{C}$ has minimum distance $2\delta + 2$ or more if and only if no subspace of dimension $k - \delta$ is contained in distinct $U, V \in \mathbb{C}$.

Proof.

$$d(U, V) = 2k - 2\dim(U \cap V)$$

so $d(U, V) \leq 2\delta$ if and only if $\dim(U \cap V) \geq k - \delta$. $\square$

Define a hypergraph (V, E) where $V = \mathcal{G}_q(\ell, k - \delta)$ and $E = G_q(\ell, k)$. We say $V \in E$ contains those $U \in V$ with $U \subseteq V$. Then $\mathcal{C}$ corresponds to a packing by hyperedges.

Upper bounds

Write $\left[{\ell \atop k}\right]_q$ for the number of k-dimensional subspaces of an ℓ-dimensional vector space over $\mathbb{F}_q$.

Upper bounds

Write $\begin{bmatrix} \ell \\ k \end{bmatrix}_q$ for the number of k-dimensional subspaces of an ℓ-dimensional vector space over $\mathbb{F}_q$.

Corollary (The packing bound)

$$\mathcal{A}_q(\ell, 2\delta + 2, k) \leq \frac{\begin{bmatrix} \ell \\ k-\delta \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q}$$

Upper bounds

Write $\left[{\ell \atop k}\right]_q$ for the number of k-dimensional subspaces of an ℓ-dimensional vector space over $\mathbb{F}_q$.

Corollary (The packing bound)

$$\mathcal{A}_q(\ell, 2\delta + 2, k) \leq \frac{\left[{\ell \atop k-\delta}\right]_q}{\left[{k \atop k-\delta}\right]_q}$$

Proof.

$|V| = \left[{\ell \atop k-\delta}\right]_q$, and each hyperedge contains $\left[{k \atop k-\delta}\right]_q$ vertices. □

Upper bounds

Write $\left[{\ell \atop k}\right]_q$ for the number of k-dimensional subspaces of an ℓ-dimensional vector space over $\mathbb{F}_q$.

Corollary (The packing bound)

$$\mathcal{A}_q(\ell, 2\delta + 2, k) \leq \frac{\left[{\ell \atop k-\delta}\right]_q}{\left[{k \atop k-\delta}\right]_q}$$

Proof.

$|V| = \left[{\ell \atop k-\delta}\right]_q$, and each hyperedge contains $\left[{k \atop k-\delta}\right]_q$ vertices. □

A version of the iterated Johnson bound for constant weight codes is a little better, but its asymptotics are the same.

Hypergraphs

Let V be a set of vertices, and E be a set of hyperedges.

- A hypergraph (V, E) is r-uniform if all hyperedges have cardinality r.

Hypergraphs

Let V be a set of vertices, and E be a set of hyperedges.

- A hypergraph (V, E) is r-uniform if all hyperedges have cardinality r. Our example: $r = \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q$.

Hypergraphs

Let V be a set of vertices, and E be a set of hyperedges.

- A hypergraph (V, E) is r-uniform if all hyperedges have cardinality r. Our example: $r = \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q$.
- The degree $\deg(v)$ of a vertex v is the number of hyperedges containing v.

Hypergraphs

Let V be a set of vertices, and E be a set of hyperedges.

- A hypergraph (V, E) is r-uniform if all hyperedges have cardinality r. Our example: $r = \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q$.
- The degree $\deg(v)$ of a vertex v is the number of hyperedges containing v.
- The hypergraph (V, E) is d-regular if $\deg(v) = d$ for all $v \in V$.

Hypergraphs

Let V be a set of vertices, and E be a set of hyperedges.

- A hypergraph (V, E) is r-uniform if all hyperedges have cardinality r. Our example: $r = \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q$.
- The degree $\deg(v)$ of a vertex v is the number of hyperedges containing v.
- The hypergraph (V, E) is d-regular if $\deg(v) = d$ for all $v \in V$. Our example: $d = \begin{bmatrix} \ell-k+\delta \\ \delta \end{bmatrix}_q$ (large).

Hypergraphs

Let V be a set of vertices, and E be a set of hyperedges.

- A hypergraph (V, E) is r-uniform if all hyperedges have cardinality r. Our example: $r = \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q$.
- The degree $\deg(v)$ of a vertex v is the number of hyperedges containing v.
- The hypergraph (V, E) is d-regular if $\deg(v) = d$ for all $v \in V$. Our example: $d = \begin{bmatrix} \ell-k+\delta \\ \delta \end{bmatrix}_q$ (large).
- The codegree $\mathrm{codeg}(u, v)$ of a pair of vertices is the number of hyperedges containing both u and v.

Hypergraphs

Let V be a set of vertices, and E be a set of hyperedges.

- A hypergraph (V, E) is r-uniform if all hyperedges have cardinality r. Our example: $r = \begin{bmatrix} k \\ k-\delta \end{bmatrix}_q$.
- The degree $\deg(v)$ of a vertex v is the number of hyperedges containing v.
- The hypergraph (V, E) is d-regular if $\deg(v) = d$ for all $v \in V$. Our example: $d = \begin{bmatrix} \ell-k+\delta \\ \delta \end{bmatrix}_q$ (large).
- The codegree $\mathrm{codeg}(u, v)$ of a pair of vertices is the number of hyperedges containing both u and v. Our example: number of k-dim subspaces containing u and v; small compared to degree.

Covers and packings of hypergraphs

Suppose we have a large r-uniform d-regular hypergraph Γ. Suppose the codegree of a pair of vertices is always much smaller than d. Then there is a covering of the vertices by hyperedges that is about as small as we could hope for (about $|V|/r$ hyperedges). Similarly there is a large hyperedge packing.

Covers and packings of hypergraphs

Suppose we have a large r-uniform d-regular hypergraph Γ. Suppose the codegree of a pair of vertices is always much smaller than d. Then there is a covering of the vertices by hyperedges that is about as small as we could hope for (about $|V|/r$ hyperedges). Similarly there is a large hyperedge packing.

Theorem (Rödl)

Fix an integer r and a positive real number δ. Then there exists an integer n_0 and a positive real number δ' with the following property.
Let Γ be an r-uniform hypergraph on n vertices, where $n \geq n_0$. Suppose that all vertices of Γ have degree d for some integer d. Let $c = \max \operatorname{codeg}(u, v)$, where the maximum is taken over all pairs of distinct vertices $u, v \in \Gamma$. If $c \leq \delta' d$, then there exists a hyperedge cover consisting of at most $(1+\delta)n/r$ hyperedges, and a hyperedge packing consisting of at least $(1-\delta)n/r$ hyperedges.

An existence result

Theorem (SRB Etzion 2012)

Let q, k and δ be fixed integers, with $0 \leq \delta \leq k$ and such that q is a prime power. Then

$$\mathcal{A}_q(\ell, 2\delta + 2, k) \sim \frac{\begin{bmatrix} \ell \\ k-\delta \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q} \tag{1}$$

as $\ell \to \infty$.

An existence result

Theorem (SRB Etzion 2012)

Let q, k and δ be fixed integers, with $0 \leq \delta \leq k$ and such that q is a prime power. Then

$$\mathcal{A}_q(\ell, 2\delta + 2, k) \sim \frac{\begin{bmatrix} \ell \\ k-\delta \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q} \tag{1}$$

as $\ell \to \infty$.

Proof.

Upper bound from packing bound. Lower bound from Rödl's theorem on quasirandom hypergraphs.

An existence result

Theorem (SRB Etzion 2012)

Let q, k and δ be fixed integers, with $0 \leq \delta \leq k$ and such that q is a prime power. Then

$$\mathcal{A}_q(\ell, 2\delta + 2, k) \sim \frac{\begin{bmatrix} \ell \\ k-\delta \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q} \tag{1}$$

as $\ell \to \infty$.

Proof.

Upper bound from packing bound. Lower bound from Rödl's theorem on quasirandom hypergraphs. □

Explicit families are within a constant of the optimal size. Examples due to Koetter and Kschischang; larger codes by generalising these due to Etzion and Silberstein.

k-radius sequences

A 5-ary 2-radius sequence of length 7 is:

$$0, 1, 2, 3, 4, 0, 1$$

k-radius sequences

A 5-ary 2-radius sequence of length 7 is:

$$0, 1, 2, 3, 4, 0, 1$$

Definition (Jaromczyk, Lonc 2004)

Let $F = \{0, 1, \ldots, n-1\}$. An *$n$-ary k-radius sequence* is a finite sequence

$$a_0, a_1, \ldots, a_{m-1}$$

over the alphabet F with the following property:
For all $x, y \in F$, there exist $i, j \in \{0, 1, \ldots, m-1\}$ such that $a_i = x$, $a_j = y$ and $|i - j| \leq k$.

Another existence result

Let $f_k(q)$ be the shortest q-ary k-radius sequence.

Another existence result

Let $f_k(q)$ be the shortest q-ary k-radius sequence.

Theorem (SRB 2012)

Let k be fixed and $q \to \infty$. Then

$$f_k(q) \sim \frac{1}{k}\binom{q}{2}$$

Another existence result

Let $f_k(q)$ be the shortest q-ary k-radius sequence.

Theorem (SRB 2012)

Let k be fixed and $q \to \infty$. Then

$$f_k(q) \sim \frac{1}{k}\binom{q}{2}$$

Proof.

Upper bound: every position can be the left-hand entry of at most k pairs.

Another existence result

Let $f_k(q)$ be the shortest q-ary k-radius sequence.

Theorem (SRB 2012)

Let k be fixed and $q \to \infty$. Then

$$f_k(q) \sim \frac{1}{k}\binom{q}{2}$$

Proof.

Upper bound: every position can be the left-hand entry of at most k pairs.
Lower bound: from quasirandom hypergraph argument. □

Another existence result

Let $f_k(q)$ be the shortest q-ary k-radius sequence.

Theorem (SRB 2012)

Let k be fixed and $q \to \infty$. Then

$$f_k(q) \sim \frac{1}{k}\binom{q}{2}$$

Proof.

Upper bound: every position can be the left-hand entry of at most k pairs.
Lower bound: from quasirandom hypergraph argument. □

Remark: Jaromczyk,Lonc,Truszczyński (2012) have recently given an explicit asymptotically tight construction.

Some Links

This talk will appear soon on my home page:

`http://www.ma.rhul.ac.uk/sblackburn`

S.R. Blackburn and T. Etzion, 'The asymptotic behavior of Grassmannian codes', *IEEE Trans. Information Theory*, to appear. See:

`http://arxiv.org/abs/1111.2713`

S.R. Blackburn, 'The existence of k-radius sequences', *J. Comb. Theory - Series A*, Vol. 119 (2012), pp. 212-217. See:

`http://arxiv.org/abs/1101.1172`.