Grassmannian Codes and Quasirandom Hypergraphs

Simon R. Blackburn

Joint work with Tuvi Etzion

9th July 2012
Grassmannian codes

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

Combinatorial problem

When $\ell$, $k$, and a distance $d$ are fixed, find the size $A_q(\ell, d, k)$ of the largest Grassmannian code of minimum distance $d$ in $G(\ell, k)$. 

Grassmannian codes

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

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

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

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

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

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

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

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

Combinatorial problem

When $\ell$, $k$ and a distance $d$ are fixed, find the size $A_q(\ell, d, k)$ of the largest Grassmannian code of minimum distance $d$ in $G(\ell, k)$.
Grassmannian codes

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

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

A set $C \subseteq G_q(\ell, k)$ is a Grassmannian code of minimum distance $d$ if $d(U, V) \geq d$ for all $U, V \in C$.

Combinatorial problem

When $\ell, k$ and a distance $d$ are fixed, find the size $A_q(\ell, d, k)$ of the largest Grassmannian code of minimum distance $d$ in $G(\ell, k)$.

Important observation

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

Proof.

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

Define a hypergraph $(V, E)$ where $V = G_{q}(\ell, k - \delta)$ and $E = G_{q}(\ell, k)$. We say $V \in E$ contains those $U \in V$ with $U \subseteq V$. Then $C$ corresponds to a packing by hyperedges.
A Grassmannian code $C$ 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 $\dim(U \cap V) \geq k - \delta$. \qed
**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 $U, V \in \mathcal{C}$.

**Proof.**

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

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

Define a **hypergraph** $(V, E)$ where $V = G_q(\ell, k - \delta)$ 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 $\binom{\ell}{k}_q$ for the number of $k$-dimensional subspaces of an $\ell$-dimensional vector space over $\mathbb{F}_q$.
Upper bounds

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

Corollary (The packing bound)

$$A_q(\ell, 2\delta + 2, k) \leq \frac{\binom{\ell}{k-\delta}_q}{\binom{k}{k-\delta}_q}$$
Upper bounds

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

**Corollary (The packing bound)**

$$A_q(\ell, 2\delta + 2, k) \leq \frac{\left[ \begin{array}{c} \ell \\ k-\delta \end{array} \right]_q}{\left[ \begin{array}{c} k \\ k-\delta \end{array} \right]_q}$$

**Proof.**

$|V| = \left[ \begin{array}{c} \ell \\ k-\delta \end{array} \right]_q$, and each hyperedge contains $\left[ \begin{array}{c} k \\ k-\delta \end{array} \right]_q$ vertices.

\qed
Upper bounds

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

**Corollary (The packing bound)**

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

**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: $r = \binom{k}{k-\delta}_q$.

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: $d = \ell - k + \delta_q$ (large).

The codegree $\text{codeg}(u, v)$ 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.
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: \( r = \left[ \frac{k}{k-\delta} \right]_q \).
- The degree \( \deg(v) \) of a vertex \( v \) is the number of hyperedges containing \( v \).
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: $d = \begin{bmatrix} \ell \end{bmatrix} - k + \delta$ (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: $r = \binom{k}{k-\delta} q$.
- 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: $d = \binom{\ell-k+\delta}{\delta} q$ (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: $r = \binom{k}{k-\delta}_q$.
- The degree $\text{deg}(v)$ of a vertex $v$ is the number of hyperedges containing $v$.
- The hypergraph $(V, E)$ is $d$-regular if $\text{deg}(v) = d$ for all $v \in V$. Our example: $d = \binom{\ell-k+\delta}{\delta}_q$ (large).
- The codegree $\text{codeg}(u, v)$ 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: $r = \left[ \frac{k}{k-\delta} \right]_q$.
- 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: $d = \left[ \frac{\ell-k+\delta}{\delta} \right]_q$ (large).
- The codegree $\text{codeg}(u, v)$ 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 $\Gamma$. 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 $\frac{|V|}{r}$ hyperedges). Similarly there is a large hyperedge packing.

Theorem (Rödl)

Fix an integer $r$ and a positive real number $\delta$. Then there exists an integer $n_0$ and a positive real number $\delta'$ with the following property. Let $\Gamma$ be an $r$-uniform hypergraph on $n$ vertices, where $n \geq n_0$. Suppose that all vertices of $\Gamma$ have degree $d$ for some integer $d$. Let $c = \max \text{codeg}(u, v)$, 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 $(1 + \delta) \frac{n}{r}$ hyperedges, and a hyperedge packing consisting of at least $(1 - \delta) \frac{n}{r}$ hyperedges.
Covers and packings of hypergraphs

Suppose we have a large $r$-uniform $d$-regular hypergraph $\Gamma$. 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 $\delta$. Then there exists an integer $n_0$ and a positive real number $\delta'$ with the following property. Let $\Gamma$ be an $r$-uniform hypergraph on $n$ vertices, where $n \geq n_0$. Suppose that all vertices of $\Gamma$ have degree $d$ for some integer $d$. Let $c = \max \text{codeg}(u, v)$, 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 \( \delta \) be fixed integers, with \( 0 \leq \delta \leq k \) and such that \( q \) is a prime power. Then

\[
\mathcal{A}_q(\ell, 2\delta + 2, k) \sim \frac{\binom{\ell}{k-\delta} q}{\binom{k}{k-\delta} q}
\]

(1)

as \( \ell \to \infty \).
An existence result

Theorem (SRB Etzion 2012)

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

$$A_q(\ell, 2\delta + 2, k) \sim \frac{\left[ \frac{\ell}{k-\delta} \right] q}{\left[ \frac{k}{k-\delta} \right] q}$$

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

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

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

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

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, Truszczynski (2012) have recently given an explicit asymptotically tight construction.
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, Truszczynski (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


http://arxiv.org/abs/1111.2713
