The minimum size of linear sets

Sam Adriaensen

Joint work with Paolo Santonastaso

RICCOTA '23

VRIJE
UNIVERSITEIT
BRUSSEL

What is a linear set?

Definition

Let $U \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}^d$. Define

$$L_U = \{\langle u \rangle_{\mathbb{F}_{q^n}} \parallel u \in U \setminus \{\mathbf{0}\}\}.$$

Then $L_U \subset \mathrm{PG}(d-1, q^n)$ is called an $\mathbb{F}_q$-*linear set*. Its *rank* is $\dim_{\mathbb{F}_q} U$.

The size

What is the size of an $\mathbb{F}_q$-linear set of rank k?

Motivation

Definition

A *blocking set* in $\mathrm{PG}(2, q^n)$ is a set of points that intersects every line.

Motivation

Definition

A *blocking set* in $\mathrm{PG}(2, q^n)$ is a set of points that intersects every line.

Choose $U \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}^3$ with $\dim_{\mathbb{F}_q} U = n + 1$.

Motivation

Definition

A *blocking set* in $\mathrm{PG}(2, q^n)$ is a set of points that intersects every line.

Choose $U \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}^3$ with $\dim_{\mathbb{F}_q} U = n+1$. A line ℓ in $\mathrm{PG}(2, q^n) \cong$ a subspace W of $\mathbb{F}_{q^n}^3$ with

- $\dim_{\mathbb{F}_{q^n}} W = 2$,

Motivation

Definition

A *blocking set* in $\mathrm{PG}(2, q^n)$ is a set of points that intersects every line.

Choose $U \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}^3$ with $\dim_{\mathbb{F}_q} U = n + 1$. A line ℓ in $\mathrm{PG}(2, q^n) \cong$ a subspace W of $\mathbb{F}_{q^n}^3$ with

- $\dim_{\mathbb{F}_{q^n}} W = 2$,
- $\dim_{\mathbb{F}_q} W = 2n$.

Motivation

Definition

A *blocking set* in $\mathrm{PG}(2, q^n)$ is a set of points that intersects every line.

Choose $U \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}^3$ with $\dim_{\mathbb{F}_q} U = n + 1$. A line ℓ in $\mathrm{PG}(2, q^n) \cong$ a subspace W of $\mathbb{F}_{q^n}^3$ with

- $\dim_{\mathbb{F}_{q^n}} W = 2$,
- $\dim_{\mathbb{F}_q} W = 2n$.

Grassmann's identity $\implies U \cap W > \mathbf{0} \implies \ell \cap L_U \neq \varnothing$.

Motivation

Definition

A *blocking set* in $\mathrm{PG}(2, q^n)$ is a set of points that intersects every line.

Choose $U \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}^3$ with $\dim_{\mathbb{F}_q} U = n + 1$. A line ℓ in $\mathrm{PG}(2, q^n) \cong$ a subspace W of $\mathbb{F}_{q^n}^3$ with

- $\dim_{\mathbb{F}_{q^n}} W = 2$,
- $\dim_{\mathbb{F}_q} W = 2n$.

Grassmann's identity $\implies U \cap W > \mathbf{0} \implies \ell \cap L_U \neq \varnothing$.

Lemma

Every $\mathbb{F}_q$-linear set of $\mathrm{PG}(2, q^n)$ of rank $n+1$ is a blocking set.

Motivation

Definition

A *blocking set* in $\mathrm{PG}(2, q^n)$ is a set of points that intersects every line.

Lemma

Every $\mathbb{F}_q$*-linear set of* $\mathrm{PG}(2, q^n)$ *of rank* $n + 1$ *is a blocking set.*

Conjecture

Every minimal blocking set in $\mathrm{PG}(2, q^n)$ *of size* $< 3\frac{q^n+1}{2}$ *is a linear set.*

Motivation

Definition

A *blocking set* in $\mathrm{PG}(2, q^n)$ is a set of points that intersects every line.

Lemma

Every $\mathbb{F}_q$-linear set of $\mathrm{PG}(2, q^n)$ of rank $n + 1$ is a blocking set.

Conjecture

Every minimal blocking set in $\mathrm{PG}(2, q^n)$ of size $< 3\frac{q^n+1}{2}$ is a linear set.

Linear sets are also linked to KM-arcs, rank-metric codes, few intersection sets, ...

Upper bound

Let U be a k-dim. $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^d$. Then U has $\dfrac{q^k-1}{q-1}$ $\mathbb{F}_q$-lin. indep. vectors. $\implies$ U has at most $\dfrac{q^k-1}{q-1}$ $\mathbb{F}_{q^n}$-lin. indep. vectors.

Upper bound

Let U be a k-dim. $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^d$. Then U has $\dfrac{q^k-1}{q-1}$ $\mathbb{F}_q$-lin. indep. vectors. $\implies$ U has at most $\dfrac{q^k-1}{q-1}$ $\mathbb{F}_{q^n}$-lin. indep. vectors.

Proposition (Blokhuis-Lavrauw)

$$|L_U| \leq \frac{q^k-1}{q-1} = q^{k-1} + q^{k-2} + \ldots + q + 1.$$

Upper bound

Let U be a k-dim. $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^d$. Then U has $\dfrac{q^k-1}{q-1}$ $\mathbb{F}_q$-lin. indep. vectors. $\implies$ U has at most $\dfrac{q^k-1}{q-1}$ $\mathbb{F}_{q^n}$-lin. indep. vectors.

Proposition (Blokhuis-Lavrauw)

$$|L_U| \leq \frac{q^k-1}{q-1} = q^{k-1} + q^{k-2} + \ldots + q + 1.$$

Linear sets attaining equality are called *scattered* and have been investigated a lot.

Obstacles for a lower bound

Let U be a k-dim. $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^d$.

Obstacles for a lower bound

Let U be a k-dim. $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^d$.

- What if U has "extra linearities"?
  Suppose that $n = st$ and U is an $\mathbb{F}_{q^s}$-subspace. Then $L_U = L_{U'}$ for every $(k - s + 1)$-dim. $\mathbb{F}_q$-subspace $U' \leq U$.

Obstacles for a lower bound

Let U be a k-dim. $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^d$.

- What if U has "extra linearities"?
  Suppose that $n = st$ and U is an $\mathbb{F}_{q^s}$-subspace. Then $L_U = L_{U'}$ for every $(k-s+1)$-dim. $\mathbb{F}_q$-subspace $U' \leq U$.

Definition

Let L_U be a linear set and $\pi \subseteq \mathrm{PG}(d-1, q^n)$ the subspace corresponding to $W \leq_{\mathbb{F}_{q^n}} \mathbb{F}_{q^n}^d$. The *weight* of π w.r.t. L_U is

$$w_{L_U}(\pi) = \dim_{\mathbb{F}_q}(W \cap U).$$

Obstacles for a lower bound

Let U be a k-dim. $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^d$.

Definition

Let L_U be a linear set and $\pi \subseteq \mathrm{PG}(d-1, q^n)$ the subspace corresponding to $W \leq_{\mathbb{F}_{q^n}} \mathbb{F}_{q^n}^d$. The *weight* of π w.r.t. L_U is

$$w_{L_U}(\pi) = \dim_{\mathbb{F}_q}(W \cap U).$$

Theorem (Csajbók-Marino-Pepe, last month!)

Suppose $k \leq (d-1)n$. If L_U has no points of weight 1, then $L_U = L_{U'}$ for some $\mathbb{F}_{q^m}$-subspace U' of $\mathbb{F}_{q^n}^d$, with $1 < m | n$.

Lower bound

Theorem (Bonoli-Polverino)

If L_U is an $\mathbb{F}_q$-linear set on $\mathrm{PG}(1, q^n)$ with

- *rank $n - 1$,*
- *at least one point of weight 1,*

$$|L_U| \geq q^{n-1} + 1.$$

Lower bound

Theorem (Bonoli-Polverino, De Beule-Van de Voorde)

If L_U is an $\mathbb{F}_q$-linear set on $\mathrm{PG}(1, q^n)$ with

- *rank $k \leq n - 1$,*
- *at least one point of weight 1,*

$$|L_U| \geq q^{k-1} + 1.$$

Lower bound

Theorem (Bonoli-Polverino, De Beule-Van de Voorde)

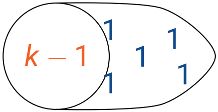
If L_U is an $\mathbb{F}_q$-linear set on $\mathrm{PG}(1, q^n)$ with

- *rank $k \leq n-1$,*
- *at least one point of weight 1,*

$$|L_U| \geq q^{k-1} + 1.$$

Example

The bound is tight. Take $U = U_1 \times \mathbb{F}_q$ for some $U_1 \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$ of dimension $k-1$.



Subgeometries and higher dim. bound

Definition

A *subgeometry* of $\mathrm{PG}(d, q^n)$ is a linear set L_U of rank $d+1$ spanning $\mathrm{PG}(d, q^n)$. The standard example is

$$L_{\mathbb{F}_q^{d+1}} = \left\{ \langle x \rangle_{\mathbb{F}_{q^n}} \parallel x \in \mathbb{F}_q^{d+1} \right\}.$$

The other examples are $\mathrm{PGL}(d+1, q^n)$-images of $L_{\mathbb{F}_q^{d+1}}$.

Subgeometries and higher dim. bound

Definition

A *subgeometry* of $\mathrm{PG}(d, q^n)$ is a linear set L_U of rank $d+1$ spanning $\mathrm{PG}(d, q^n)$. The standard example is

$$L_{\mathbb{F}_q^{d+1}} = \left\{ \langle x \rangle_{\mathbb{F}_{q^n}} \parallel x \in \mathbb{F}_q^{d+1} \right\}.$$

The other examples are $\mathrm{PGL}(d+1, q^n)$-images of $L_{\mathbb{F}_q^{d+1}}$.

Every point in a subgeometry has weight 1.

Subgeometries and higher dim. bound

Definition

A *subgeometry* of $\mathrm{PG}(d, q^n)$ is a linear set L_U of rank $d+1$ spanning $\mathrm{PG}(d, q^n)$.

Every point in a subgeometry has weight 1.

Theorem (De Beule-Van de Voorde)

Let L_U be an $\mathbb{F}_q$-linear set in $\mathrm{PG}(d, q^n)$ such that

- *its rank is $k > d$,*
- *it intersects some hyperplane in a subgeometry.*

$$|L_U| \geq q^{k-1} + \ldots + q^{k-d} + 1.$$

“Conjecture”

Theorem (De Beule-Van de Voorde)

Let L_U *be an* $\mathbb{F}_q$*-linear set in* $\mathrm{PG}(d, q^n)$ *such that*

- *its rank is* $k > d$,
- *it intersects some hyperplane in a subgeometry.*

$$|L_U| \geq q^{k-1} + \ldots + q^{k-d} + 1.$$

Conjecture (Jena-Van de Voorde)

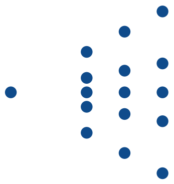
Let L_U *be an* $\mathbb{F}_q$*-linear set in* $\mathrm{PG}(d, q^n)$ *such that*

- n *is prime,*
- *its rank is* $k \leq d + n$,
- L_U *spans* $\mathrm{PG}(d, q^n)$.

$$|L_U| \geq q^{k-1} + \ldots + q^{k-d} + 1.$$

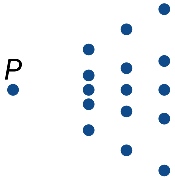
Projection of a linear set

Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(d-1, q^n)$.



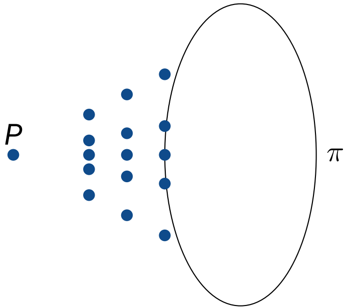
Projection of a linear set

Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(d-1, q^n)$. Let P be a point of weight $w > 0$.



Projection of a linear set

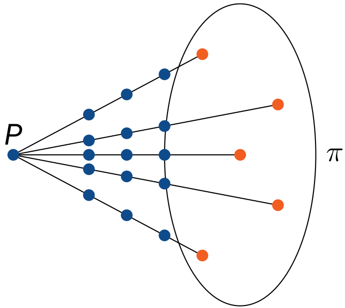
Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(d-1, q^n)$. Let P be a point of weight $w > 0$. Choose a hyperplane $\pi \not\ni P$.



Projection of a linear set

Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(d-1,q^n)$. Let P be a point of weight $w > 0$. Choose a hyperplane $\pi \not\ni P$. Define the set $L' \subset \pi$ by

$$R \in L' \iff \langle P, R\rangle \cap L_U \supsetneq \{P\}.$$

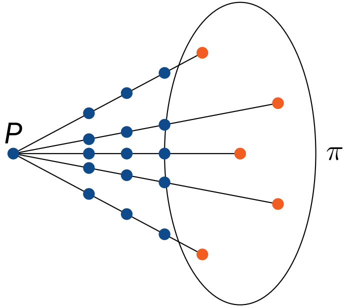


Projection of a linear set

Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(d-1, q^n)$. Let P be a point of weight $w > 0$. Choose a hyperplane $\pi \not\ni P$. Define the set $L' \subset \pi$ by

$$R \in L' \iff \langle P, R \rangle \cap L_U \supsetneq \{P\}.$$

Then L' is an $\mathbb{F}_q$-linear set of rank $k - w$ in $\pi \cong \mathrm{PG}(d-2, q^n)$.



Recursive bound

Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(d-1, q^n)$.

Recursive bound

Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(d-1, q^n)$.

Case 1: L_U has no point of weight 1.

By Csajbók-Marino-Pepe either

Recursive bound

Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(d-1, q^n)$.

Case 1: L_U has no point of weight 1.
By Csajbók-Marino-Pepe either

- $k > (d-1)n$ (and $L_U = \mathrm{PG}(d-1, q^n)$),

Recursive bound

Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(d-1, q^n)$.

Case 1: L_U has no point of weight 1.
By Csajbók-Marino-Pepe either

- $k > (d-1)n$ (and $L_U = \mathrm{PG}(d-1, q^n)$),
- or L_U is equal to an $\mathbb{F}_{q^m}$-linear set with $1 < m | n$.

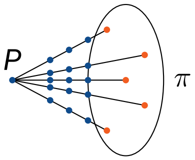
Recursive bound

Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(d-1, q^n)$.

Case 1: L_U has no point of weight 1.
By Csajbók-Marino-Pepe either

- $k > (d-1)n$ (and $L_U = \mathrm{PG}(d-1, q^n)$),
- or L_U is equal to an $\mathbb{F}_{q^m}$-linear set with $1 < m|n$.

Case 2: L_U has some point P of weight 1.
Project from P. Apply the De Beule-Van de Voorde bound on all the lines through P.



$$|L_U| \geq q^{k-1} + |L'|.$$

Recursive bound

Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(d-1, q^n)$.

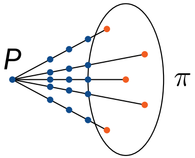
<u>Case 1: L_U has no point of weight 1.</u>
By Csajbók-Marino-Pepe either

- $k > (d-1)n$ (and $L_U = \mathrm{PG}(d-1, q^n)$),
- or L_U is equal to an $\mathbb{F}_{q^m}$-linear set with $1 < m | n$.
  If n is prime, this implies $m = n$.

<u>Case 2: L_U has some point P of weight 1.</u>

Project from P. Apply the De Beule-Van de Voorde bound on all the lines through P.

$$|L_U| \geq q^{k-1} + |L'|.$$



Bounds

Suppose that L_U is an $\mathbb{F}_q$-linear set of rank k, spanning $\mathrm{PG}(d-1, q^n)$ containing a point of weight 1. Then

$$q^{k-1} + |L'| \leq |L_U| \leq q^{k-1} + \ldots + q + 1.$$

Here L' is an $\mathbb{F}_q$-linear set of rank $k-1$ spanning $\mathrm{PG}(d-2, q^n)$.

Bounds

Suppose that L_U is an $\mathbb{F}_q$-linear set of rank k, spanning $\mathrm{PG}(d-1, q^n)$ containing a point of weight 1. Then

$$q^{k-1} + |L'| \leq |L_U| \leq q^{k-1} + \ldots + q + 1.$$

Here L' is an $\mathbb{F}_q$-linear set of rank $k-1$ spanning $\mathrm{PG}(d-2, q^n)$.

Corollary

If n is prime and $k < d + n$, then

$$|L_U| \geq q^{k-1} + q^{k-2} + \ldots + q^{k-d} + 1.$$

This proves the “conjecture” of Jena-Van de Voorde

Finite Geometry & Friends

Summer school at Vrije Universiteit Brussel

18-22 September 2023.

- Code-based cryptography,
- quantum walks on graphs,
- algebraic graph theory,
- tensors, semifields, rank metric codes.

`http://summerschool.fining.org`