Asymptotically Good Strong Blocking Sets

Finite Geometries 2022 – Sixth Irsee Conference

Alessandro Neri

29 August 2022

Joint work with Anurag Bishnoi and Shagnik Das

Max Planck Institute for Mathematics in the Sciences

Contents

Coding Theory

"Coding theory is the theory of subsets (subspaces) of a metric space"

- Finite field $\mathbb{F}_q$ with q elements.
- $\mathbb{F}_q^n$ vector space.
- The (Hamming) **support** of $v \in \mathbb{F}_q^n$ is the set

$$\sigma(v) := \{i \,:\, v_i \neq 0\} \subseteq [n].$$

- $\mathrm{wt}(v) := |\sigma(v)|$ is the (Hamming) **weight**.
- $\delta : \mathbb{F}_q^n \times \mathbb{F}_q^b \to \mathbb{R}_{\geq 0}$, $\delta(u, v) := \mathrm{wt}(u - v)$ is the (Hamming) **distance**.

Linear Codes and Minimal Linear Codes

Definition

An $[n, k, d]_q$ code $\mathcal{C}$ is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$.

- n is the **length** of $\mathcal{C}$.
- k is the **dimension** of $\mathcal{C}$.
- $d := \min\{\mathrm{wt}(u) \, : \, u \in \mathcal{C} \setminus \{0\}\}$ is the **minimum distance** of $\mathcal{C}$.

Linear Codes and Minimal Linear Codes

Definition

An $[n, k, d]_q$ code $\mathcal{C}$ is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$.

- n is the **length** of $\mathcal{C}$.
- k is the **dimension** of $\mathcal{C}$.
- $d := \min\{\mathrm{wt}(u) : u \in \mathcal{C} \setminus \{0\}\}$ is the **minimum distance** of $\mathcal{C}$.

- $\mathcal{C}$ possesses a **generator matrix** $G \in \mathbb{F}_q^{k \times n}$ whose rows are a basis:

$$\mathcal{C} = \{uG : u \in \mathbb{F}_q^k\},$$

Linear Codes and Minimal Linear Codes

Definition

An $[n, k, d]_q$ code $\mathcal{C}$ is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$.

- n is the **length** of $\mathcal{C}$.
- k is the **dimension** of $\mathcal{C}$.
- $d := \min\{\mathrm{wt}(u) \,:\, u \in \mathcal{C} \setminus \{0\}\}$ is the **minimum distance** of $\mathcal{C}$.

- $\mathcal{C}$ possesses a **generator matrix** $G \in \mathbb{F}_q^{k \times n}$ whose rows are a basis:

$$\mathcal{C} = \{uG \,:\, u \in \mathbb{F}_q^k\},$$

- $v \in \mathcal{C} \setminus \{0\}$ is a **minimal codeword** if $\sigma(v)$ is minimal w.r.t $\subseteq$ in

$$\sigma(\mathcal{C}) := \{\sigma(c) \,:\, c \in \mathcal{C} \setminus \{0\}\}.$$

Linear Codes and Minimal Linear Codes

Definition

An $[n, k, d]_q$ code $\mathcal{C}$ is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$.

- n is the **length** of $\mathcal{C}$.
- k is the **dimension** of $\mathcal{C}$.
- $d := \min\{\mathrm{wt}(u) \,:\, u \in \mathcal{C} \setminus \{0\}\}$ is the **minimum distance** of $\mathcal{C}$.

- $\mathcal{C}$ possesses a **generator matrix** $G \in \mathbb{F}_q^{k\times n}$ whose rows are a basis:

$$\mathcal{C} = \{uG \,:\, u \in \mathbb{F}_q^k\},$$

- $v \in \mathcal{C} \setminus \{0\}$ is a **minimal codeword** if $\sigma(v)$ is minimal w.r.t $\subseteq$ in

$$\sigma(\mathcal{C}) := \{\sigma(c) \,:\, c \in \mathcal{C} \setminus \{0\}\}.$$

- $\mathcal{C}$ is a **minimal (linear) code** if every $v \in \mathcal{C} \setminus \{0\}$ is minimal.

Brief Explanation

- Minimal codewords were first studied for decoding pruposes by Hwang ('78).
- Renovated interest due to Massey ('93). He proposed an application to Secret Sharing Schemes.
- Many (many!) constructions of **long** minimal codes
- Really interesting from a Combinatorial point of view
- Supports of the nonzero codewords are a **Sperner family**: i.e. they form an antichain with respect to "$\subseteq$"
- This does not say everything: we have an underlying $\mathbb{F}_q$-linear structure. We can talk of of **$\mathbb{F}_q$-linear Sperner family**
- There is a Geometric point of view that leads new interesting results

Geometric Interpretation of Linear Codes

Consider an $[n, k]_q$ code $\mathcal{C}$ with generator matrix $G = (g_{i,j})$. A basis for $\mathcal{C}$ is given by the rows of G.

$$\begin{matrix} \downarrow & \downarrow & & \downarrow \\ \end{matrix}$$

$$\begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix}$$

We can instead consider the columns as projective points

$$\mathcal{P} = \{\{P_1, \ldots, P_n\}\} \subseteq \mathrm{PG}(k-1, q)$$

Geometric Interpretation of Linear Codes

Consider an $[n, k]_q$ code $\mathcal{C}$ with generator matrix $G = (g_{i,j})$. A basis for $\mathcal{C}$ is given by the rows of G.

$$\begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix}$$

We can instead consider the columns as projective points

$$\mathcal{P} = \{\{P_1, \ldots, P_n\}\} \subseteq \mathrm{PG}(k-1, q)$$

Transform metric properties of codes in geometric properties.

Geometric Interpretation of Linear Codes

Consider an $[n, k]_q$ code $\mathcal{C}$ with generator matrix $G = (g_{i,j})$. A basis for $\mathcal{C}$ is given by the rows of G.

$$\begin{array}{cccc} \downarrow & \downarrow & & \downarrow \end{array}$$
$$\begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix}$$

We can instead consider the columns as projective points

$$\mathcal{P} = \{\{P_1, \ldots, P_n\}\} \subseteq \mathrm{PG}(k-1, q)$$

Transform metric properties of codes in geometric properties.

$$G \longleftrightarrow \mathcal{P}$$

Geometric interpretation of Minimal Codes

Theorem 1

(a) uG is minimal if and only if $\langle \mathcal{P} \cap u^{\perp} \rangle = u^{\perp}$.

(b) $\mathcal{C}$ is minimal if and only if $\langle \mathcal{P} \cap H \rangle = H$ for every hyperplane $H \subseteq \mathrm{PG}(k-1, q)$ ($\mathcal{P}$ is a **strong (cutting) blocking set**).

Geometric interpretation of Minimal Codes

Theorem 1

(a) uG is minimal if and only if $\langle \mathcal{P} \cap u^\perp \rangle = u^\perp$.

(b) $\mathcal{C}$ is minimal if and only if $\langle \mathcal{P} \cap H \rangle = H$ for every hyperplane $H \subseteq \mathrm{PG}(k-1, q)$ ($\mathcal{P}$ is a **strong (cutting) blocking set**).

- Long linear codes are very likely minimal (they correspond to large subsets of $\mathrm{PG}(k-1, q)$)

Geometric interpretation of Minimal Codes

Theorem 1

(a) uG is minimal if and only if $\langle \mathcal{P} \cap u^\perp \rangle = u^\perp$.

(b) $\mathcal{C}$ is minimal if and only if $\langle \mathcal{P} \cap H \rangle = H$ for every hyperplane $H \subseteq \mathrm{PG}(k-1, q)$ ($\mathcal{P}$ is a **strong (cutting) blocking set**).

- Long linear codes are very likely minimal (they correspond to large subsets of $\mathrm{PG}(k-1, q)$)

Questions

(1) What can we say about the parameters of a minimal linear code?

(2) Can we construct families of short minimal linear codes?

G.N. Alfarano, M. Borello, A. Neri. "A geometric characterization of minimal codes and their asymptotic performance", 2020.

C. Tang, Y. Qiu, Q. Liao, Z. Zhou. "Full Characterization of Minimal Linear Codes as Cutting Blocking Sets", 2021.

Geometric interpretation of Minimal Codes

Theorem 1

(a) uG is minimal if and only if $\langle \mathcal{P} \cap u^{\perp} \rangle = u^{\perp}$.

(b) $\mathcal{C}$ is minimal if and only if $\langle \mathcal{P} \cap H \rangle = H$ for every hyperplane $H \subseteq \mathrm{PG}(k-1, q)$ ($\mathcal{P}$ is a **strong (cutting) blocking set**).

- Long linear codes are very likely minimal (they correspond to large subsets of $\mathrm{PG}(k-1, q)$)

Questions

(1) What can we say about the parameters of a strong blocking sets?

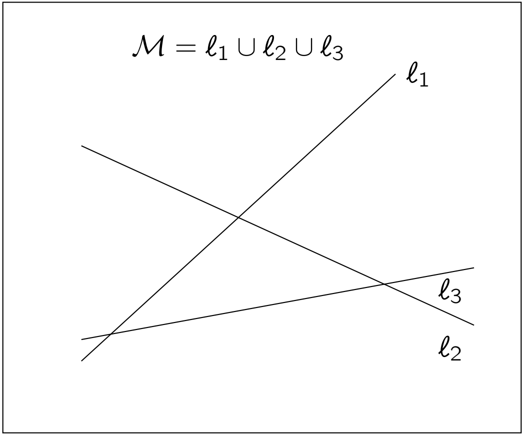
(2) Can we construct families of small strong blocking sets?

G.N. Alfarano, M. Borello, A. Neri. "A geometric characterization of minimal codes and their asymptotic performance", 2020.

C. Tang, Y. Qiu, Q. Liao, Z. Zhou. "Full Characterization of Minimal Linear Codes as Cutting Blocking Sets", 2021.

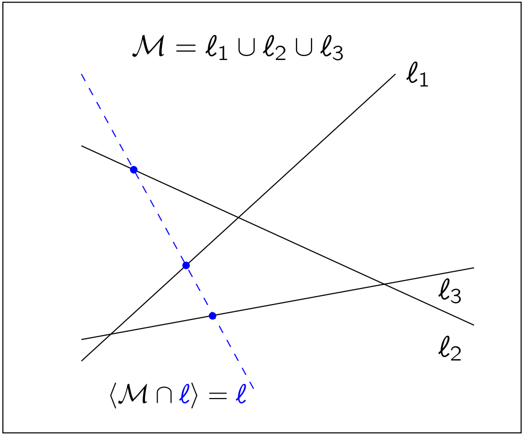
Constructing Strong Blocking Sets: an Example

In PG(2, q) hyperplanes are lines



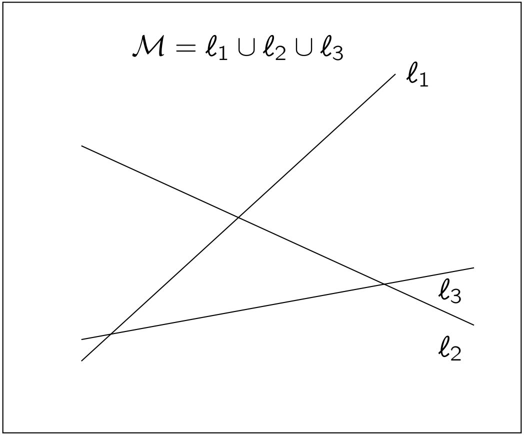
Constructing Strong Blocking Sets: an Example

In PG(2, q) hyperplanes are lines



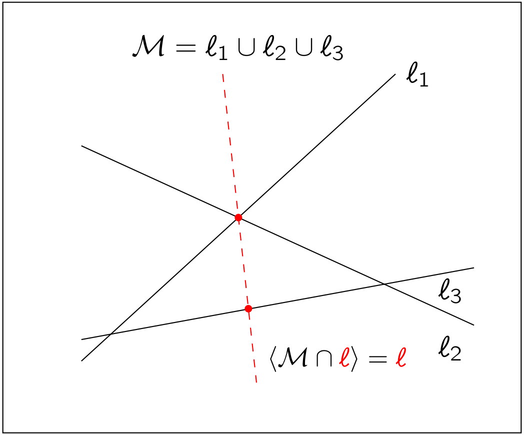
Constructing Strong Blocking Sets: an Example

In PG$(2, q)$ hyperplanes are lines



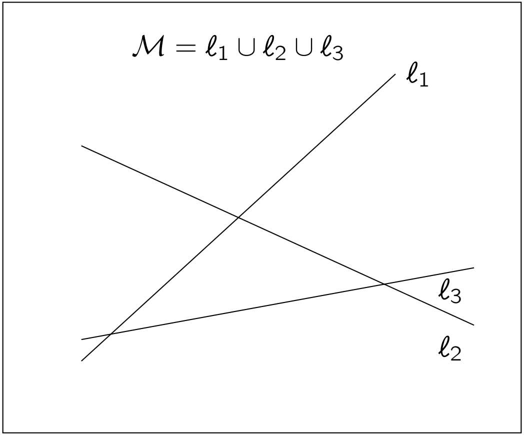
Constructing Strong Blocking Sets: an Example

In PG(2, q) hyperplanes are lines



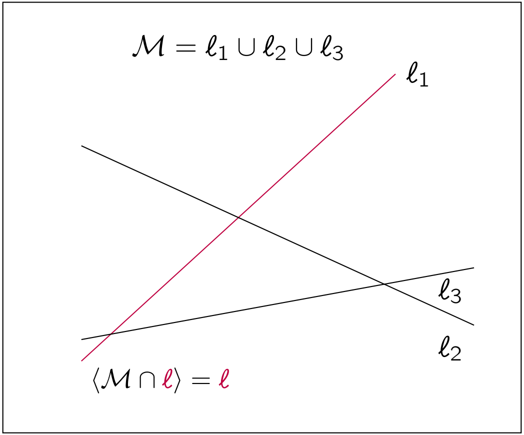
Constructing Strong Blocking Sets: an Example

In PG$(2, q)$ hyperplanes are lines



Constructing Strong Blocking Sets: an Example

In PG$(2, q)$ hyperplanes are lines



Bounds on the Size

Theorem (Alfarano, Borello, N, Ravagnani, '21)

Let $\mathcal{P} \subseteq \mathrm{PG}(k-1, q)$ be a strong blocking set. Then

$$|\mathcal{P}| \geq (q+1)(k-1).$$

G.N. Alfarano, M. Borello, A. Neri, A. Ravagnani. "Three combinatorial perspectives on minimal codes", 2021.

Theorem (Heger, Nagy '21)

The size of the smallest strong blocking set in $\mathrm{PG}(k-1, q)$

$$\leq \begin{cases} \frac{2k-1}{\log_2(4/3)} & \text{if } q = 2 \\ (q+1)\left(\frac{2}{1+\frac{1}{(q+1)^2 \log q}}(k-1)\right) & \text{otherwise} \end{cases}$$

T. Heger, Z. L. Nagy. "Short minimal codes and covering codes via strong blocking sets in projective spaces", 2021.

Rational Normal Tangents

For fixed k and large q we have a quasi-optimal construction:

Theorem (Fancsali, Sziklai, '14)

- $q \geq 2k-3$
- $\mathcal{X}$ rational normal curve of degree $k-1$ in $\mathrm{PG}(k-1,q)$
- $P_1, \ldots, P_{2k-3} \in \mathcal{X}$.
- ℓ_i tangent line to $\mathcal{X}$ in P_i.

$$\bigcup_{i=1}^{2k-3} \ell_i \qquad \text{is a strong blocking set}$$

S. Fancsali, P. Sziklai. "Lines in higgledy-piggledyarrangement", The electronic journal of combinatorics 21, 2014.

Question

What if we fix q and let k grow? **Asymptotically good constructions**

Tetrahedron

Tetrahedron

- $P_1, \dots, P_k$ be points in $\mathrm{PG}(k-1, q)$ in general position.
- $\ell_{i,j} = \langle P_i, P_j \rangle$.

Then, the following is a strong blocking set:

$$\mathcal{P}_k = \bigcup_{1 \leq i < j \leq k} \ell_{i,j} \subseteq \mathrm{PG}(k-1, q)$$

We have

$$|\mathcal{P}_k| = \binom{k}{2}(q-1) + k = \mathcal{O}(k^2)$$

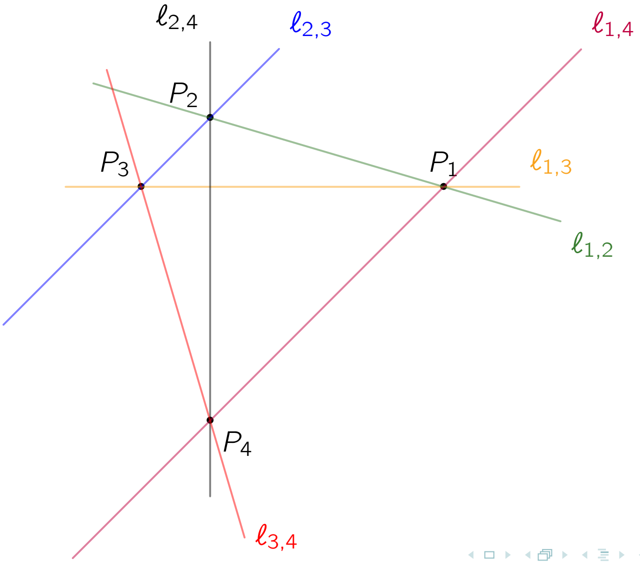
A. Davydov, M. Giulietti, S. Marcugini, F. Pambianco. "Linear nonbinary covering codes and saturating sets in projective spaces", 2011.

G.N. Alfarano, M. Borello, A. Neri. "A geometric characterization of minimal codes and their asymptotic performance", 2020.

D. Bartoli, M. Bonini, B. Gunes. "An inductive construction of minimal codes", 2021.

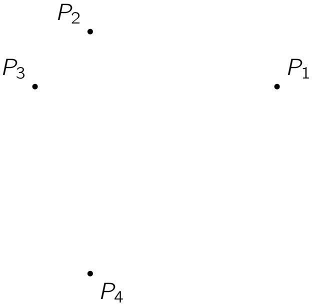
W. Lu, X. Wu, X. Cao. "The parameters of minimal linear codes", 2021.

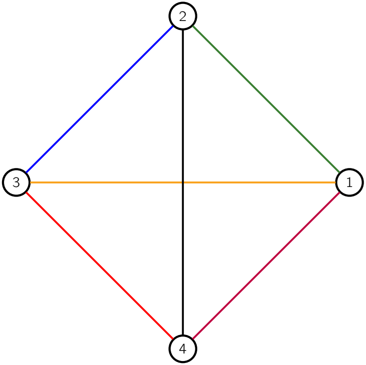
Tetrahedron in PG$(3, q)$



Tetrahedron in PG(3, q)

$\mathcal{P} \subseteq \mathrm{PG}(3, q)$ $+$ $G = K_4$





Let us Generalize!

Lambda Construction

Let us start with

- A set of points $\mathcal{P} = \{P_1, \dots, P_m\}$;
- A graph $G = (V, E)$ on $V = [m] := \{1, \dots, m\}$;

Define

$$\Lambda(\mathcal{P}, G) := \bigcup_{(i,j)\in E} \langle P_i, P_j \rangle.$$

Let us Generalize!

Lambda Construction

Let us start with

- A set of points $\mathcal{P} = \{P_1, \ldots, P_m\}$;
- A graph $G = (V, E)$ on $V = [m] := \{1, \ldots, m\}$;

Define

$$\Lambda(\mathcal{P}, G) := \bigcup_{(i,j) \in E} \langle P_i, P_j \rangle.$$

Tetrahedron in $\mathrm{PG}(k-1, q)$:

$$\cong \Lambda(\{[e_1], \ldots, [e_k]\}, K_k)$$

Let us Generalize!

Lambda Construction

Let us start with

- A set of points $\mathcal{P} = \{P_1, \ldots, P_m\}$;
- A graph $G = (V, E)$ on $V = [m] := \{1, \ldots, m\}$;

Define

$$\Lambda(\mathcal{P}, G) := \bigcup_{(i,j)\in E} \langle P_i, P_j \rangle.$$

Tetrahedron in $\mathrm{PG}(k-1, q)$:

$$\cong \Lambda(\{[e_1], \ldots, [e_k]\}, K_k)$$

Question

When is $\Lambda(\mathcal{P}, G)$ a strong blocking set?

A Connectivity Parameter

Let $G = (V, E)$. For a subset $S \subset V$, define

- $G[S]$: the induced subgraph on the vertices in S;
- $t(S)$: the maximum cardinality of a connected component in $G[S]$;

A Connectivity Parameter

Let $G = (V, E)$. For a subset $S \subset V$, define

- $G[S]$: the induced subgraph on the vertices in S;
- $t(S)$: the maximum cardinality of a connected component in $G[S]$;

Connectivity factor

$$s(G) := \min_{S \subseteq V} \left(|V| - |S| + t(S)\right).$$

A Connectivity Parameter

Let $G = (V, E)$. For a subset $S \subset V$, define

- $G[S]$: the induced subgraph on the vertices in S;
- $t(S)$: the maximum cardinality of a connected component in $G[S]$;

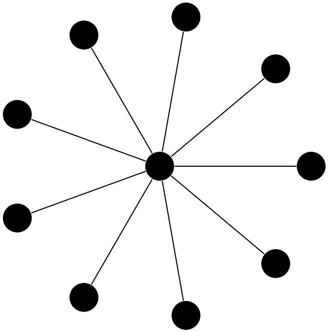
Connectivity factor

$$s(G) := \min_{S \subseteq V} \left(|V| - |S| + t(S)\right).$$

We say that the graph G is **of type** (m, e, s) if

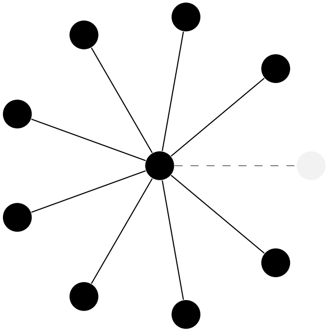
- $m = |V|$, number of **vertices**,
- $e = |E|$, number of **edges**,
- $s = s(G)$, **connectivity factor**.

An Example: the Star Graph



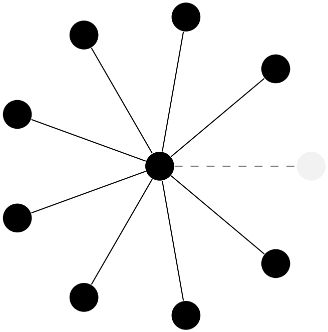
$K_{1,9}$

An Example: the Star Graph



$K_{1,9}$

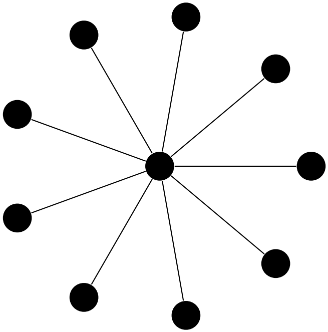
An Example: the Star Graph



$K_{1,9}$

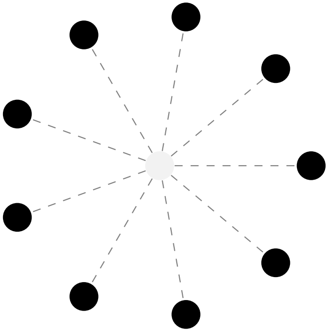
$$(|V| - |S|) + t(S) = 1 + 9 = 10$$

An Example: the Star Graph



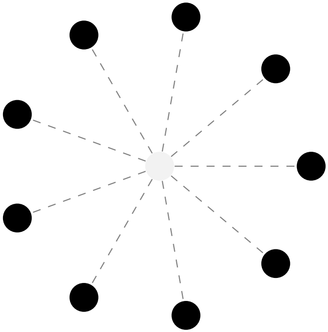
$K_{1,9}$

An Example: the Star Graph



$K_{1,9}$

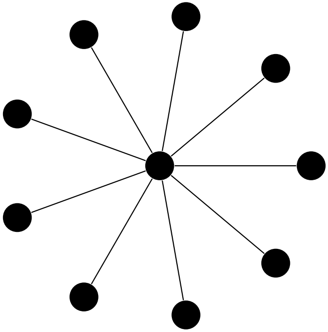
An Example: the Star Graph



$K_{1,9}$

$$(|V| - |S|) + t(S) = 1 + 1 = 2$$

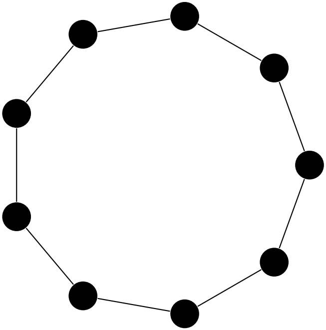
An Example: the Star Graph



$K_{1,9}$

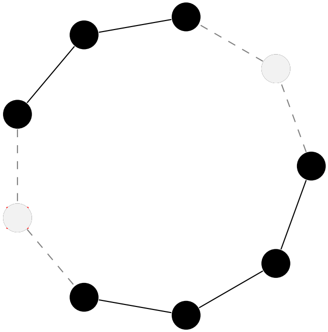
$$s(K_{1,9}) = 2$$

Another Example: the Cycle Graph



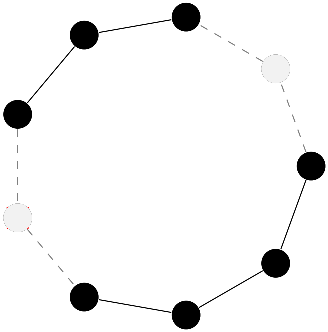
C_9

Another Example: the Cycle Graph



C_9

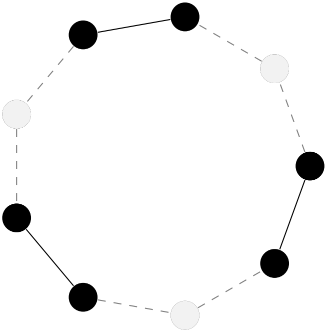
Another Example: the Cycle Graph



C_9

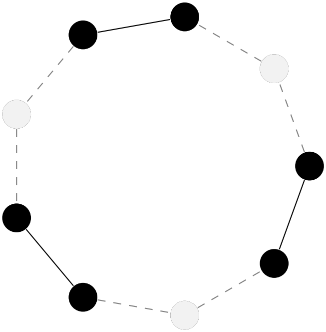
$$(|V| - |S|) + t(S) = 2 + 4 = 6$$

Another Example: the Cycle Graph



C_9

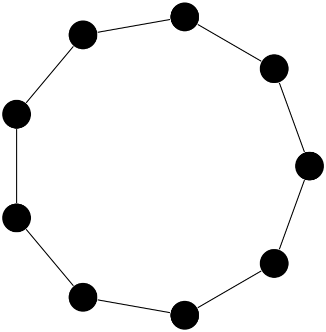
Another Example: the Cycle Graph



C_9

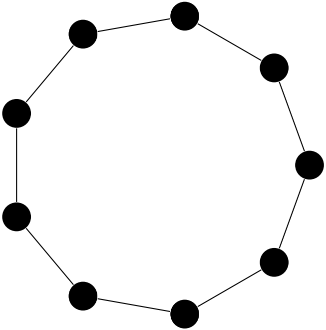
$$(|V| - |S|) + t(S) = 3 + 2 = 5$$

Another Example: the Cycle Graph



C_9

Another Example: the Cycle Graph



C_9

$s(C_9) = 5$

Main Theorem

Let

- $\mathcal{P} = \{P_1, \ldots, P_m\}$ from an $[m, k, d]_q$ code,
- $G = (V, E)$ be a graph of type (m, e, s).

Main Theorem

Let

- $\mathcal{P} = \{P_1, \dots, P_m\}$ from an $[m, k, d]_q$ code,
- $G = (V, E)$ be a graph of type (m, e, s).

Theorem (Bishnoi, Das, N., 202+)

If

$$m - d + 1 \leq s$$

then $\Lambda(\mathcal{P}, G)$ is a **strong blocking set** in $\mathrm{PG}(k-1, q)$ of size

$$|\Lambda(\mathcal{P}, G)| = (q-1)e + m$$

Asymptotically Consequence

Theorem (Bishnoi, Das, N., 202+)

If there exists a family $\{G_m\}_{m\in\mathbb{N}}$ of connected graphs of type (m, e_m, s_m) with

- $e_m = \Theta(m^\alpha)$
- $s_m = \mu m + o(m)$

then we can explicitly construct a family of strong blocking sets of the form $\Lambda(\mathcal{P}_{m,q}, G_m)$ of size (approx.)

$$e_m(q+1) = \mathcal{O}(k^\alpha)$$

provided that $\mu > 1/(\sqrt{q}-1)$.

Open Problem at Combinatorics 2022

(1) Explicit construction of a family $\{G_m\}_{m\in\mathbb{N}}$ of connected graphs of type (m, e_m, s_m) with

$$e_m = \Theta(m), \qquad s_m = \Theta(m)$$

implies

Explicit construction of a family $\{C_{k,q}\}_{k\in\mathbb{N}}$ of $[n_k, k]_q$ minimal codes of length

$$n_k = \mathcal{O}(k)$$

Open Problem at Combinatorics 2022

(1) Explicit construction of a family $\{G_m\}_{m\in\mathbb{N}}$ of connected graphs of type (m, e_m, s_m) with

$$e_m = \Theta(m), \qquad s_m = \Theta(m)$$

implies

Explicit construction of a family $\{\mathcal{P}_{k,q}\}_{k\in\mathbb{N}}$ of strong blocking sets in $\mathrm{PG}(k-1, q)$ of size

$$\mathcal{O}(k)$$

Open Problem at Combinatorics 2022

(1) Explicit construction of a family $\{G_m\}_{m\in\mathbb{N}}$ of connected graphs of type (m, e_m, s_m) with

$$e_m = \Theta(m), \qquad s_m = \Theta(m)$$

implies

Explicit construction of a family $\{\mathcal{P}_{k,q}\}_{k\in\mathbb{N}}$ of strong blocking sets in $\mathrm{PG}(k-1, q)$ of size

$$\mathcal{O}(k)$$

Not anymore!

t-Regular Graphs

t-Regular Graphs

Lemma (Bishnoi, Das, N., 202+)

Let

- G be a t-regular graph on m vertices
- λ its second largest eigenvalue in absolute value.

t-Regular Graphs

Lemma (Bishnoi, Das, N., 202+)

Let

- G be a t-regular graph on m vertices
- λ its second largest eigenvalue in absolute value.

Then

$$s(G) \geq \frac{t-\lambda}{3t-\lambda}\, m$$

Margulis Graphs

- $G_{a^2} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}$ $\qquad m := a^2$

Margulis Graphs

- $G_{a^2} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}$ $\quad m := a^2$
- (x, y) is adjacent to

$$\{(x \pm 2y, y), (x \pm (2y+1), y), (x, y \pm 2x), (x, y \pm (2x+1))\}$$

Margulis Graphs

- $G_{a^2} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}$ $\qquad m := a^2$
- (x, y) is adjacent to

$$\{(x \pm 2y, y), (x \pm (2y+1), y), (x, y \pm 2x), (x, y \pm (2x+1))\}$$

- For each a the graph G_{a^2} is 8-regular.
- $\lambda \leq 5\sqrt{2}$

Margulis Graphs

- $G_{a^2} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}$ $\qquad m := a^2$
- (x, y) is adjacent to

$$\{(x \pm 2y, y), (x \pm (2y+1), y), (x, y \pm 2x), (x, y \pm (2x+1))\}$$

- For each a the graph G_{a^2} is 8-regular.
- $\lambda \leq 5\sqrt{2}$

$$s_m \geq \frac{8 - 5\sqrt{2}}{24 - 5\sqrt{2}} m \geq \frac{1}{19} m.$$

Margulis Graphs

- $G_{a^2} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}$ $\qquad m := a^2$
- (x, y) is adjacent to

$$\{(x \pm 2y, y), (x \pm (2y+1), y), (x, y \pm 2x), (x, y \pm (2x+1))\}$$

- For each a the graph G_{a^2} is 8-regular.
- $\lambda \leq 5\sqrt{2}$

$$s_m \geq \frac{8 - 5\sqrt{2}}{24 - 5\sqrt{2}} m \geq \frac{1}{19} m.$$

Margulis Graphs

- $G_{a^2} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}$ $\qquad m := a^2$
- (x, y) is adjacent to

$$\{(x \pm 2y, y), (x \pm (2y+1), y), (x, y \pm 2x), (x, y \pm (2x+1))\}$$

- For each a the graph G_{a^2} is 8-regular.
- $\lambda \leq 5\sqrt{2}$

$$s_m \geq \frac{8 - 5\sqrt{2}}{24 - 5\sqrt{2}} m \geq \frac{1}{19} m.$$

Corollary (Bishnoi, Das, N., 202+)

For every square $q > 19^2$, we can construct a family of strong blocking sets in $\mathrm{PG}(k-1, q)$ of size approx.

$$8k(q+1)\left(\frac{19(\sqrt{q}-1)}{\sqrt{q}-20}\right)$$

Margulis Graphs

- $G_{a^2} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}$ $\qquad m := a^2$
- (x, y) is adjacent to

$$\{(x \pm 2y, y), (x \pm (2y+1), y), (x, y \pm 2x), (x, y \pm (2x+1))\}$$

- For each a the graph G_{a^2} is 8-regular.
- $\lambda \leq 5\sqrt{2}$

$$s_m \geq \frac{8 - 5\sqrt{2}}{24 - 5\sqrt{2}} m \geq \frac{1}{19} m.$$

Corollary (Bishnoi, Das, N., 202+)

For every square $q > 19^2$, we can construct a family of strong blocking sets in $\mathrm{PG}(k-1, q)$ of size approx.

$$8k(q+1)\left(\frac{19(\sqrt{q}-1)}{\sqrt{q}-20}\right)$$

Margulis Graphs

- $G_{a^2} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}$ $\qquad m := a^2$
- (x, y) is adjacent to

$$\{(x \pm 2y, y), (x \pm (2y+1), y), (x, y \pm 2x), (x, y \pm (2x+1))\}$$

- For each a the graph G_{a^2} is 8-regular.
- $\lambda \leq 5\sqrt{2}$

$$s_m \geq \frac{8 - 5\sqrt{2}}{24 - 5\sqrt{2}} m \geq \frac{1}{19} m.$$

Corollary (Bishnoi, Das, N., 202+)

For every square $q > 19^2$, we can construct a family of strong blocking sets in $\mathrm{PG}(k-1, q)$ of size approx.

$$8k(q+1)\left(\frac{19(\sqrt{q}-1)}{\sqrt{q}-20}\right)$$

Margulis Graphs

- $G_{a^2} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}$ $\qquad m := a^2$
- (x, y) is adjacent to

$$\{(x \pm 2y, y), (x \pm (2y+1), y), (x, y \pm 2x), (x, y \pm (2x+1))\}$$

- For each a the graph G_{a^2} is 8-regular.
- $\lambda \leq 5\sqrt{2}$

$$s_m \geq \frac{8 - 5\sqrt{2}}{24 - 5\sqrt{2}} m \geq \frac{1}{19} m.$$

Corollary (Bishnoi, Das, N., 202+)

For every square $q > 19^2$, we can construct a family of strong blocking sets in $\mathrm{PG}(k-1, q)$ of size approx.

$$8k(q+1)\left(\frac{19(\sqrt{q}-1)}{\sqrt{q}-20}\right)$$

Margulis Graphs

- $G_{a^2} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}$ $\quad m := a^2$
- (x, y) is adjacent to

$$\{(x \pm 2y, y), (x \pm (2y+1), y), (x, y \pm 2x), (x, y \pm (2x+1))\}$$

- For each a the graph G_{a^2} is 8-regular.
- $\lambda \leq 5\sqrt{2}$

$$s_m \geq \frac{8 - 5\sqrt{2}}{24 - 5\sqrt{2}} m \geq \frac{1}{19} m.$$

Corollary (Bishnoi, Das, N., 202+)

For every square $q > 19^2$, we can construct a family of strong blocking sets in $\mathrm{PG}(k-1, q)$ of size approx.

$$8k(q+1)\left(\frac{19(\sqrt{q}-1)}{\sqrt{q}-20}\right)$$

The End

Thank you! Danke!

Grazie!