

eSeminar UGent-VUB

Constructing saturating sets in projective spaces

using subgeometries

Lins Denaux

14th of January 2021

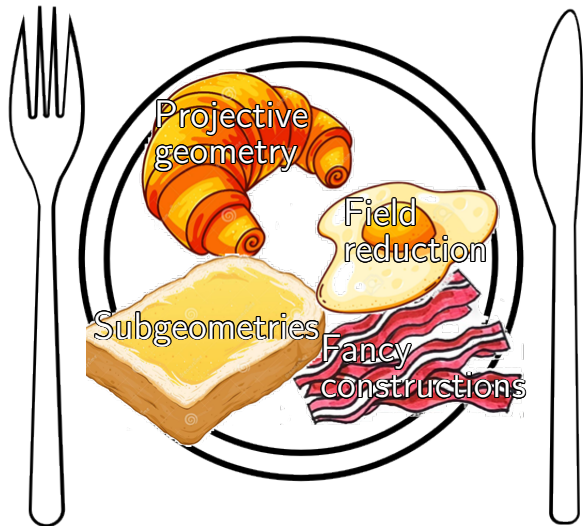


GHENT
UNIVERSITY

Overview

- 1 Introduction
- 2 Empty results from the past: a flashback
- 3 The mixed subgeometry approach
- 4 Subgeometries are affine lines
- 5 A construction for general n and q





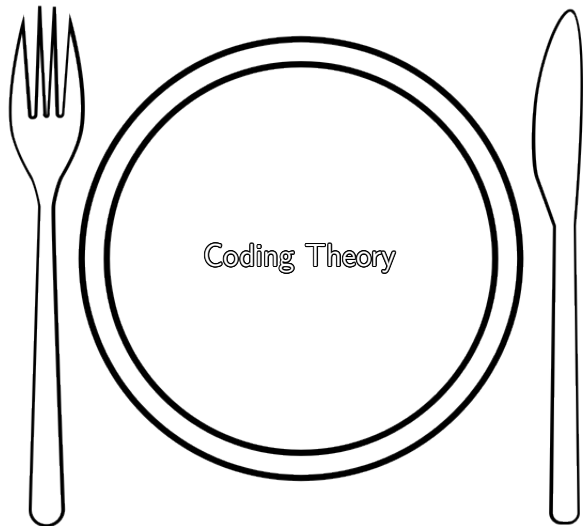
On the menu



1

Introduction

On the menu

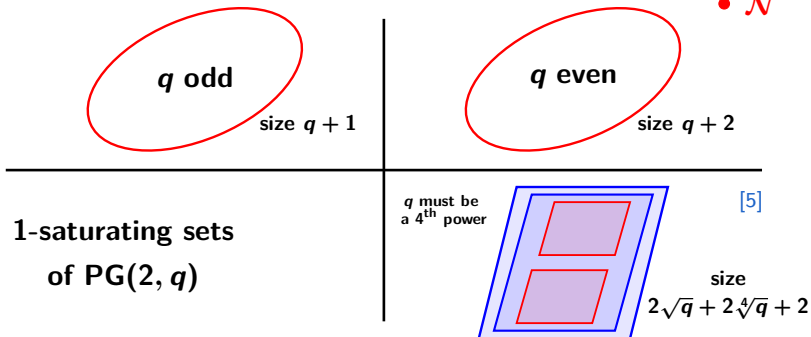


Let $n \in \mathbb{N}^\times$, q a prime power and $\varrho \in \{0, 1, \dots, n\}$.

A ϱ -*saturating set* \mathcal{S} of $\text{PG}(n, q)$: point set such that

- ▶ any point of $\text{PG}(n, q)$ lies in span of $\leq \varrho + 1$ points of \mathcal{S} .

• \mathcal{N}



Correspondence with covering codes

 \mathcal{S} ϱ -saturating set of $PG(n, q)$, $\mathcal{S} := \{P_1, P_2, P_3, \dots, P_{|\mathcal{S}|}\}$.

$$\begin{array}{ccccccc}
 P_1 & P_2 & P_3 & \cdots & P_i & \cdots & P_{|\mathcal{S}|} \\
 \left(\begin{array}{ccccccc}
 x_{10} & x_{20} & x_{30} & \cdots & x_{i0} & \cdots & x_{|\mathcal{S}|0} \\
 x_{11} & x_{21} & x_{31} & \cdots & x_{i1} & \cdots & x_{|\mathcal{S}|1} \\
 \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
 x_{1n} & x_{2n} & x_{3n} & \cdots & x_{in} & \cdots & x_{|\mathcal{S}|n}
 \end{array} \right)
 \end{array}$$


coordinates of P_i

PC-matrix of a $[|\mathcal{S}|, |\mathcal{S}| - n - 1]_q$ $(\varrho + 1)$ -covering code!

Any vector of $\mathbb{F}_q^{|\mathcal{S}|}$ lies within Hamming distance $\varrho + 1$ of a codeword.

Goal: Finding good upper bounds for $s_q(n, \varrho)$.

PG(2, q): LOTS of research!

- ▶ Strongly \sim to complete caps.
- ▶ Often computer searches.
- ▶ Nice survey in [7]. (Davydov & Östergård, 2000)

Keep in mind

$$s_q(n, \varrho) \gtrsim \varrho \cdot q^{\frac{n-\varrho}{\varrho+1}}.$$

Hypothesis (LD, 2019)

Desperate wish (LD, 2020)

$$s_q(n, \varrho) \lesssim \varrho \cdot q^{\frac{n-\varrho}{\varrho+1}},$$

for all $n, \varrho \leq n$ and ∞ -many q .

The jungle of known results

PG(n, q): quite a lot of research

- ▶ Davydov et al., 2011 [5]

$$s_q(n, \varrho) \lesssim \binom{n+1}{\varrho} q^{\frac{n-\varrho}{\varrho+1}}$$

if q is a $(\varrho + 1)^{\text{th}}$ power.

- ▶ Bartoli et al., 2017, 2019 [1, 2]

$$s_q(n, 1) \lesssim 2q^{\frac{n-1}{2}} \sqrt{\ln(q)}$$

if n is even and n, q are large.

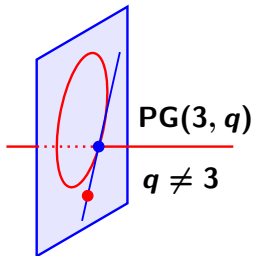
- ▶ A few more, see later.

Empty results from the past: a flashback

An inductive fiasco

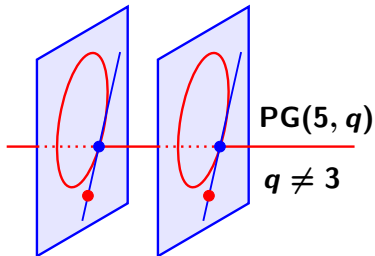
Corollary

$$s_q(2\varrho + 1, \varrho) \leq (\varrho + 1)(q + 1).$$



Keep in mind

$$s_q(n, \varrho) \gtrsim \varrho \cdot q^{\frac{n-\varrho}{\varrho+1}}.$$



Theorem (Davydov [3])

$$s_q(3, 1) \leq 2(q + 1) - 1.$$

Theorem (Davydov & Östergård, 2000 [7])

$$s_q(5, 2) \leq 3(q + 1) - 2.$$



Empty results from the past: a flashback

An inductive fiasco

Theorem (LD, 2019)

Let $k \in \mathbb{N}$, $(k, q) \neq (1, 3)$, $q \neq 2$ if k is even and $\varrho < \theta_k$. Then

$$s_q\left(k(\varrho + 1) + \varrho, \varrho\right) \leq (\varrho + 1)\theta_k - \varrho.$$

Keep in mind

$$s_q(n, \varrho) \gtrsim \varrho \cdot q^{\frac{n-\varrho}{\varrho+1}}.$$

Hypothesis (LD, 2019)

Desperate wish (LD, 2020)

$$s_q(n, \varrho) \lesssim \varrho \cdot q^{\frac{n-\varrho}{\varrho+1}},$$

for all n , $\varrho \leq n$ and ∞ -many q .

So... whatya think!?

Took some work! 😊

Very nice construction. 😊

Your upper bound doesn't improve ours, though.

... say what now?



Empty results from the past: a flashback

An inductive fiasco

Theorem (LD, 2019)

Let $k \in \mathbb{N}$, $(k, q) \neq (1, 3)$, $q \neq 2$ if k is even and $\varrho < \theta_k$. Then

$$s_q(k(\varrho + 1) + \varrho, \varrho) \leq (\varrho + 1)\theta_k - \varrho.$$

Theorem (Davydov, Marcugini & Pambianco, 2019 [6])

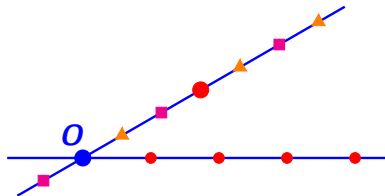
Let $k \in \mathbb{N}$ be large enough, $q \geq 7$ and $\varrho \geq 3$. Then

$$s_q(k(\varrho + 1) + \varrho, \varrho) \leq (\varrho + 1)q^k + 2q^{k-1} + \mathcal{O}(q^{k-2}).$$



A better but bitter start

- ▶ Let $n = 2$ and $\rho = 1$.
- ▶ Let q be square.

**Keep in mind**

$$s_q(2, 1) \gtrsim \sqrt{q}.$$

- ▶ 1-sat. set of $PG(2, q)$.
- ▶ Davydov: algebraic proof.
- ▶ Combinatorial proof?
 - ▶ $\sqrt{q}(\sqrt{q} + 1)$ collinear Baer sublines through O .

$$\sqrt{q}(\sqrt{q} + 1) = q + q - \sqrt{q}(\sqrt{q} - 1).$$

Theorem (Davydov, 1995 [3])

Let q be square. Then

$$s_q(2, 1) \leq 3\sqrt{q} - 1.$$

Theorem (Davydov et al., 2011 [5])

Let q be a fourth power. Then



$$s_q(2, 1) \leq 2\sqrt{q} + 2\sqrt[4]{q} + 2.$$

Empty results from the past: a flashback

A better but bitter start

Theorem (LD, 2019)

Let n be even and q be square. Then

$$s_q(n, 1) \leq 3q^{\frac{n-1}{2}} + 3q^{\frac{n-3}{2}} + \cdots + 3q^{\frac{1}{2}} - \frac{n}{2}.$$

Keep in mind

$$s_q(n, 1) \gtrsim q^{\frac{n-1}{2}}.$$

► Davydov et al., 2011 [5]

$$s_q(n, \varrho) \lesssim \binom{n+1}{\varrho} q^{\frac{n-\varrho}{\varrho+1}}$$

if q is a $(\varrho + 1)^{\text{th}}$ power.

Phew, found myself another construction! 🤔

Thoughts?

Nice one! 😊

But a better bound was already known in 1999.



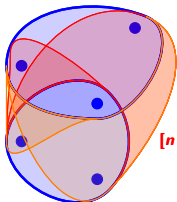
Theorem (Davydov et al., 2011 [5])

Any $(\varrho + 1)$ -fold strong blocking set in $\text{PG}(n, \sqrt[e+1]{q})$ is a ϱ -saturating set of $\text{PG}(n, q)$.

A $(\varrho + 1)$ -fold strong blocking set \mathcal{B} of $\text{PG}(n, q)$:

- ▶ Any ϱ -space is spanned by $\varrho + 1$ points of \mathcal{B} .

How did they obtain the coefficient $\binom{n+1}{\varrho}$?



- ▶ Choose $n + 1$ independent points.
- ▶ Consider span of each $(n - \varrho)$ -subset.
- ▶ Add the $\varrho + 1$ 'extensions' to saturating set \mathcal{S} .

$$|\mathcal{S}| \leq \binom{n+1}{\varrho+1} (\varrho+1) q^{\frac{n-\varrho}{e+1}}.$$

$[n - \varrho - 1]$



The mixed subgeometry approach

Two different approaches

If q is a $(\varrho + 1)^{\text{th}}$ power: two possible paths to take

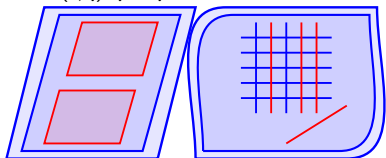
Path of the single subgeometry
Strong blocking set approach



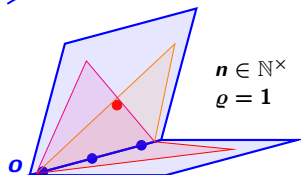
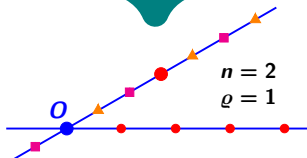
- ▶ $(\varrho + 1)$ -fold strong blocking sets in $\text{PG}(n, q)$.

$\text{PG}(2, q)$, q 4th power

$\text{PG}(3, q)$



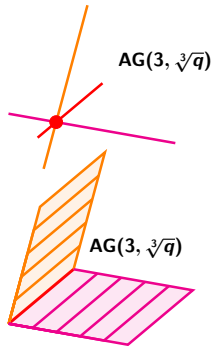
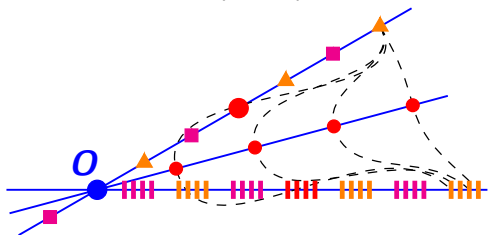
Path of the mixed subgeometries
Mixed subgeometry approach



The mixed subgeometry approach

The spark

Let q be cube ($\varrho = 2$).



"This last construction looks promising!" - LD, 2019

Theorem (LD, 2019)

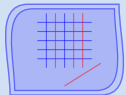
Let q be cube. Then

$$s_q(3, 2) \leq 6\sqrt[3]{q} - 3.$$

Theorem (Davydov et al., 2011 [5])

Let q be cube. Then

$$s_q(3, 2) \leq 4\sqrt[3]{q} + 4.$$



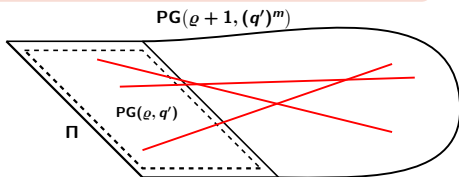
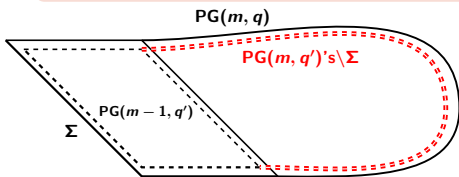
Subgeometries are affine lines

Two isomorphic point-line geometries

Suppose $q = (q')^{\varrho+1}$.

Let $m \in \mathbb{N}^\times$, Σ hyperplane of $\text{PG}(m, q)$. $\mathbf{Y}(\varrho, m, q') := (\mathcal{P}_{\text{sub}}, \mathcal{L}_{\text{sub}})$.

- ▶ $\mathcal{P}_{\text{sub}} := \text{PG}(m, q) \setminus \Sigma$.
- ▶ $\mathcal{L}_{\text{sub}} :=$ all $\text{PG}(m, q')$'s $\setminus \Sigma$ through fixed $\text{PG}(m-1, q') \subseteq \Sigma$.



Let $m \in \mathbb{N}^\times$, Π hyperpl. of $\text{PG}(\varrho+1, (q')^m)$. $\mathbf{T}^*(\text{PG}(\varrho, q')) := (\mathcal{P}_{\text{aff}}, \mathcal{L}_{\text{aff}})$.

- ▶ $\mathcal{P}_{\text{aff}} := \text{PG}(\varrho+1, (q')^m) \setminus \Pi$.
- ▶ $\mathcal{L}_{\text{aff}} :=$ all affine parts of lines outside of Π intersecting $\text{PG}(\varrho, q') \subseteq \Pi$.

Subgeometries are affine lines

Suppose $q = (q')^{\rho+1}$.

Two isomorphic point-line geometries

Theorem (LD, 2020 [9])

$$Y(\varrho, m, q') \cong T^*(\text{PG}(\varrho, q')).$$

Proof.

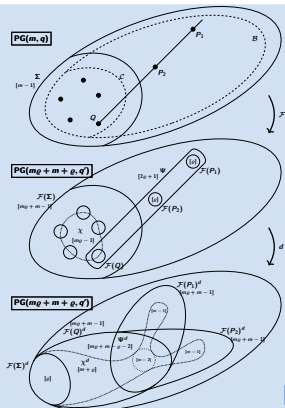
- ▶ Coordinates.
- ▶ Field reduction.

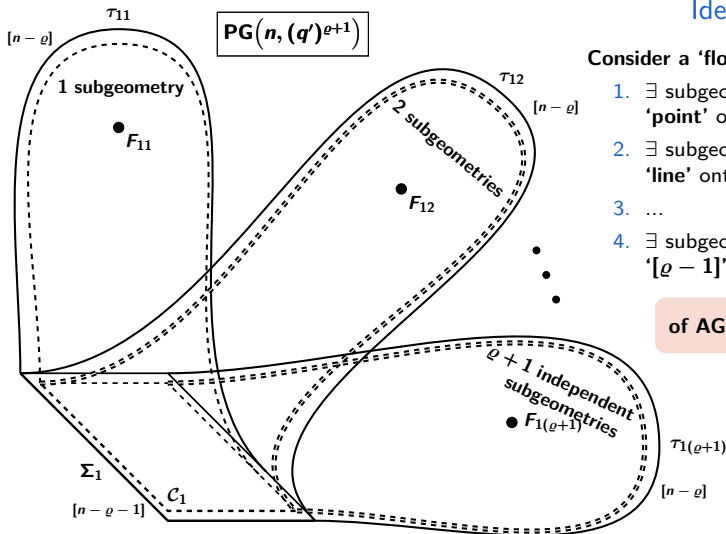
Theorem (LD, 2020 [9])

$$Y(\varrho, m, q') \cong X(\varrho, m, q').$$

Theorem (De Winter, Rottey & Van de Voorde, 2015 [8])

$$X(\varrho, m, q') \cong T^*(\text{PG}(\varrho, q')).$$



A construction for general n and ϱ 

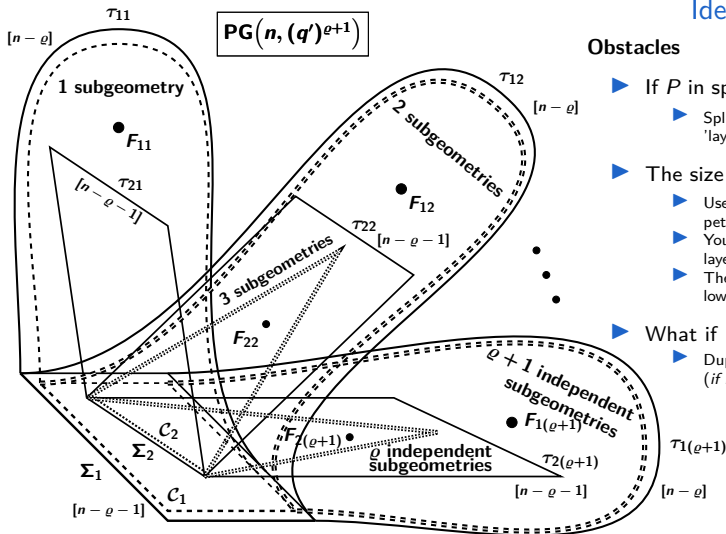
Ideas and obstacles

Consider a 'flower'.

1. \exists subgeom. in τ_{11} that projects 'point' onto 'line',
2. \exists subgeom. in τ_{12} that projects 'line' onto 'plane',
3. ...
4. \exists subgeom. in $\tau_{1\varrho}$ that projects ' $[\varrho - 1]$ ' onto 'hyperplane'

of $\text{AG}(\varrho + 1, (q')^{n-\varrho})$.

A construction for general n and ϱ

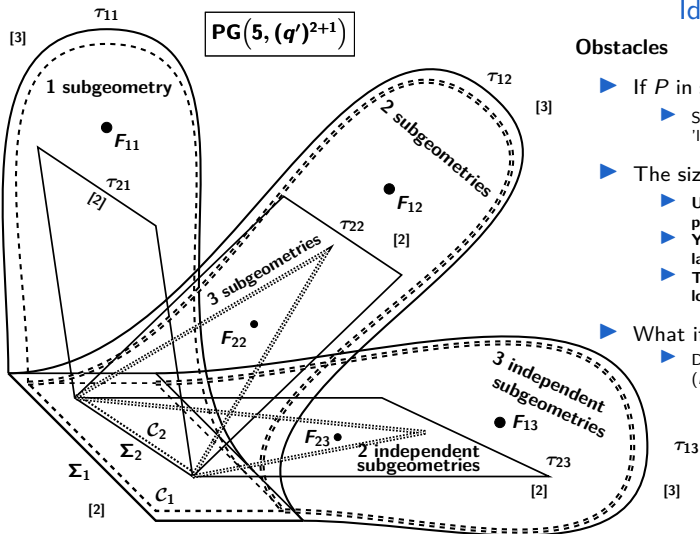


Ideas and obstacles

Obstacles

- ▶ If P in span of $< (\varrho + 1)$ petals?
 - ▶ Split petals and add multiple 'layers' in each petal!
- ▶ The size will get expon. **big...**
 - ▶ Use the subgeometries from the petal above!
 - ▶ You only need $\min\{\varrho, n - \varrho\}$ layers, and not in *all* petals!
 - ▶ The number of subgeometries in lower layers can be reduced!
- ▶ What if $P \in \Sigma_1$?
 - ▶ Duplicate construction! (if necessary)

A construction for general n and q



Ideas and obstacles

Obstacles

- ▶ If P in span of $< (q+1)$ petals?
 - ▶ Split petals and add multiple 'layers' in each petal!
- ▶ The size will get expon. **big...**
 - ▶ Use the subgeometries from the petal above!
 - ▶ You only need $\min\{q, n - q\}$ layers, and not in *all* petals!
 - ▶ The number of subgeometries in lower layers can be reduced!
- ▶ What if $P \in \Sigma_1$?
 - ▶ Duplicate construction! (if necessary)

A construction for general n and ϱ

One bound to rule them all

Theorem (LD, 2020 [9])

Let $0 < \varrho < n$ and let $q = (q')^{\varrho+1}$ for any prime power q' . Then

$$s_q(n, \varrho) \leq \sum_{i=1}^{k(n, \varrho)} \left(\frac{(\varrho+1)(\varrho+2)}{2} (q')^{n+1-i(\varrho+1)} \right) + \sum_{i=1}^{k(n, \varrho)-1} \sum_{j=1}^{\varrho-1} \tilde{a}(\varrho, j) (q')^{n+1-i(\varrho+1)-j}$$

$$+ \sum_{j=1}^{\ell(n, \varrho)-1} \tilde{a}(n, \varrho, j) (q')^{\ell(n, \varrho)-j} - \tilde{c}(n, \varrho) - \bar{c}(n, \varrho) + \delta_{q'=2} \cdot \left((2^{\varrho-1} - 1) \cdot \sum_{i=1}^{k(n, \varrho)-1} (2^{n-\varrho+2-i(\varrho+1)}) + 2^{\ell(n, \varrho)} - 2 \right),$$

▶ $k(n, \varrho) := \left\lceil \frac{n-\varrho}{\varrho+1} \right\rceil,$

▶ $\ell(n, \varrho) := (n \bmod \varrho + 1) + 1,$

▶ $\tilde{a}(\varrho, j) := \frac{\varrho(\varrho+2j+1)-j(3j+1)}{2},$

▶ $\tilde{a}(n, \varrho, j) := \frac{\ell(n, \varrho)(2\varrho - \ell(n, \varrho) + 2j + 1) - j(3j + 1)}{2},$

▶ $\tilde{c}(n, \varrho) := (k(n, \varrho) - 1) \frac{\varrho^2(\varrho+1)}{2},$

▶ $\bar{c}(n, \varrho) := \frac{\varrho(\varrho+1) + \ell(n, \varrho)(\ell(n, \varrho) - 1)(2\varrho - \ell(n, \varrho) + 1)}{2},$

▶ $\delta_{q'=2} := \begin{cases} 1 & \text{if } q' = 2, \\ 0 & \text{if } q' \neq 2. \end{cases}$

with

A construction for general n and ϱ

One bound to rule them all

Corollary (LD, 2020 [9])

Let $1 < \varrho < n$ and let $q = (q')^{\varrho+1}$ for any prime power q' . Then

$$s_q(n, \varrho) \leq \frac{(\varrho + 1)(\varrho + 2)}{2} (q')^{n-\varrho} + \varrho(\varrho + 1) ((q')^{n-\varrho-1} + \dots + q' + 1).$$

Keep in mind

$$s_q(n, \varrho) \gtrsim \varrho \cdot q^{\frac{n-\varrho}{\varrho+1}}.$$

Davydov et al., 2011 [5]

Hypothesis (LD, 2019)

Desperate wish (LD, 2020)

$$s_q(n, \varrho) \lesssim \varrho \cdot q^{\frac{n-\varrho}{\varrho+1}},$$

for all n , $\varrho \leq n$ and ∞ -many q .

$$s_q(n, \varrho) \lesssim \binom{n+1}{\varrho} q^{\frac{n-\varrho}{\varrho+1}}$$

if q is a $(\varrho + 1)^{\text{th}}$ power.

A construction for general n and ϱ

One bound to rule them all

Corollary (LD, 2020 [9])

Let $1 < \varrho < n$ and let $q = (q')^{\varrho+1}$ for any prime power q' . Then

$$s_q(n, \varrho) \leq \frac{(\varrho + 1)(\varrho + 2)}{2} (q')^{n-\varrho} + \varrho(\varrho + 1) ((q')^{n-\varrho-1} + \dots + q' + 1).$$

Coincidental example found in the wild:

Theorem (Davydov et al., 2011 [5])

Let $q = (q')^3$ for any prime power q' . Then

$$s_q(4, 2) \leq 9(q')^2 - 8q' + 4.$$

Corollary (LD, 2020 [9])

Let $q = (q')^3$ for any prime power q' . Then

$$s_q(4, 2) \leq 6(q')^2 + 3q' - 6 \quad (+2 \text{ if } q = 8).$$

arXiv:2008.13459

Slides: <https://users.ugent.be/~ldnaux>

Thank you for listening

Any questions?

Suggestions?

Funny anecdotes?



References

- [1] **D. Bartoli, A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco.** *New bounds for linear codes of covering radius 2*, volume 10495 of *Lecture Notes in Comput. Sci.* Springer, Cham, 2017.
- [2] **D. Bartoli, A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco.** *New bounds for linear codes of covering radii 2 and 3*, volume 11. 2019.
- [3] **A. A. Davydov.** *Constructions and families of covering codes and saturated sets of points in projective geometry*, volume 41. 1995.
- [4] **A. A. Davydov.** Constructions and families of nonbinary linear codes with covering radius 2. *IEEE Trans. Inform. Theory*, 45(5):1679–1686, 1999.
- [5] **A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco.** *Linear nonbinary covering codes and saturating sets in projective spaces*, volume 5. 2011.
- [6] **A. A. Davydov, S. Marcugini, and F. Pambianco.** New covering codes of radius R , codimension tR and $tR + \frac{R}{2}$, and saturating sets in projective spaces. *Des. Codes Cryptogr.*, 87(12):2771–2792, 2019.
- [7] **A. A. Davydov and P. R. J. Östergård.** *On saturating sets in small projective geometries*, volume 21. 2000.
- [8] **S. De Winter, S. Rottey, and G. Van de Voorde.** Linear representations of subgeometries. *Des. Codes Cryptogr.*, 77(1):203–215, 2015.
- [9] **L. Denaux.** Constructing saturating sets in projective spaces using subgeometries. [arXiv:2008.13459](https://arxiv.org/abs/2008.13459), 2020.

