Conjectural upper bounds on the smallest size of a complete cap in $\mathrm{PG}(N, q)$, $N \geq 3$

Daniele Bartoli* Alexander A. Davydov@ Giorgio Faina*
Stefano Marcugini* Fernanda Pambianco*

@ Institute for Information Transmission Problems (Kharkevich Institute), Russian Academy of Science, Moscow, Russia
* Department of Mathematics and Informatics, Perugia University, Perugia, Italy

XV International Workshop on Algebraic and Combinatorial Coding Theory, ACCT2016,Albena, Bulgaria, June 18-24, 2016

Outline

INTRODUCTION NOTATION

$\mathrm{PG}(N, q)$ ⇔ projective space of dimension N over Galois field $\mathbb{F}_q$

***n*-cap** ⇔ a set of n points no three of which are collinear

tangent ⇔ a line meeting a cap in one point

bisecant ⇔ a line intersecting a cap in two points

a **point** A of $\mathrm{PG}(N, q)$ is **covered** by a cap ⇔
the point A lies on a **bisecant** of the cap

complete cap ⇔ all points of $\mathrm{PG}(N, q)$
are covered by bisecants of the cap
⇔ one may not add a new point to a complete cap

CONNECTIONS with CODING THEORY

complete n-cap in $\mathrm{PG}(N,q) \Leftrightarrow [n, n-(N+1), 4]_q 2$ code

point of the cap
$\Updownarrow$
column of a parity-check matrix of the code

LOWER BOUND

$t_2(N,q) \Leftrightarrow$ the smallest size of a complete cap in $\mathrm{PG}(N,q)$

exact values of $t_2(N,q)$ are known only for small q, N

LOWER BOUND: $t_2(N,q) > \sqrt{2}q^{\frac{N-1}{2}}$

results close to lower bound are known only for even q

$q=2$, N odd & N even:

E.M. Gabidulin, A.A. Davydov, L.M. Tombak **1991**

$q=2^h$, N odd: F. Pambianco, L. Storme **1996**; M. Giulietti **2007**

A.A. Davydov, M. Giulietti, S. Marcugini, F. Pambianco **2010**

PROBLEM: UPPER BOUND

$t_2(N,q) \Leftrightarrow$ the smallest size of a complete cap in $\mathrm{PG}(N,q)$

HARD OPEN CLASSICAL PROBLEM: **1950 $\rightarrow$**

upper bound on $t_2(N,q)$

$$t_2(N,q) < cq^{\frac{N-1}{2}} \ln^{300} q$$

c - constant independent of q

D. Bartoli, S. Marcugini, F. Pambianco **ACCT2014** &
http://arxiv.org/pdf/1406.5060.pdf **2014**

probabilistic methods based on J.H. Kim, V. Vu for plane $\mathrm{PG}(2,q)$
2003

GOAL and RESULT

GOAL ⇒ analytical (non-computer) bound

$t_2(N,q) < cq^{\frac{N-1}{2}}\sqrt{\ln q}.$ c - constant independent of q

RESULT ⇒ Under some reasonable probabilistic conjecture :(

$$t_2(N,q) \sim \sqrt{N+1}\cdot q^{\frac{N-1}{2}}\sqrt{\ln q}.$$

WAY and BASE

WAY $\Rightarrow$ analysis of step-by-step greedy algorithms

A greedy algorithm is an algorithm that makes the *locally optimal choice* at each stage with the hope of finding a global optimum or, at least, a global "good" solution.

"From the first day to this, sheer greed was the driving spirit of civilization" (F. Engels)

BASE D. Bartoli, A.A. Davydov, G. Faina, A.A. Kreshchuk, S. Marcugini, F. Pambianco bounds for $\mathrm{PG}(2, q)$
ACCT2014, Problems of Information Transmission 2014

Ensemble of random w-caps

The w-th step of Algorithm forms a w-cap W.

U_w $\Leftrightarrow$ the number of points not covered by W

$\mathbf{S}(U_w)$ $\Leftrightarrow$ the set of all w-caps in $\mathrm{PG}(N,q)$ each of which does not cover exactly U_w points.

Starting cap of the $(w+1)$-*th step* $\Leftrightarrow$ w-cap $\mathcal{K}_w$ randomly chosen from $\mathbf{S}(U_w)$.

For every cap of $\mathbf{S}(U_w)$ the probability to be chosen $= \frac{1}{\#\mathbf{S}(U_w)}$.

$\mathbf{S}(U_w)$ $\Leftrightarrow$ an ensemble of random objects with the uniform probability distribution.

Uniform distribution of uncovered points

$$\#\mathrm{PG}(N,q)=\theta_{N,q}=\frac{q^{N+1}-1}{q-1}=q^N+q^{N-1}+\ldots+q+1$$

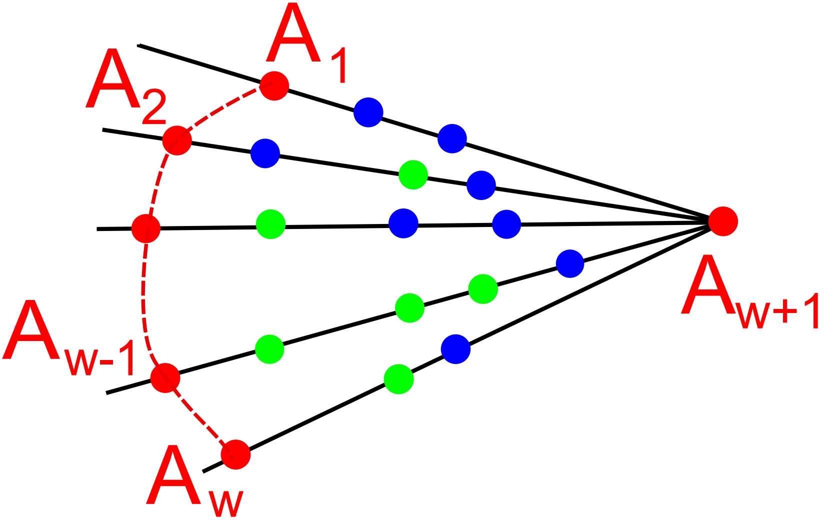
Lemma

Every point of $\mathrm{PG}(N,q)$ may be considered as a random object that can be uncovered by a randomly chosen w-arc $\mathcal{K}_w$ with some probability p_w. The probability p_w is the same for all points:

$$p_w=\frac{U_w}{\#\mathrm{PG}(N,q)}.$$

the **proportion** of uncovered points =
the **probability** that a point is uncovered

One step of a greedy algorithm



the number of new covered points on the $(w+1)$-th step

cap $\mathcal{K}_w = \{A_1, A_2, \ldots, A_w\}$. A_i – point of $\mathrm{PG}(N, q)$.

point A_{w+1} will be included in the cap on the $(w+1)$-th step

A_{w+1} defines a bundle $\mathcal{B}_w(A_{w+1})$ of w tangents to $\mathcal{K}_w$

$w(q-1)+1$ points of $\mathcal{B}_w(A_{w+1}) \setminus \{A_1, \ldots, A_w\}$ are candidates to be new covered points at the $(w+1)$-th step

$\Delta_w(A_{w+1})$ - the number of new covered points on $(w+1)$-th step

U_w uncovered points $\Rightarrow$ U_w distinct bundles

tools –> estimates of $\Delta_w(A_{w+1})$

the main idea for bounds

if events "a point is uncovered" are independent

the expected value of the number of new covered points among $w(q-1)+1$ random points is

$$\mathbf{E} = p_w \cdot (w(q-1)+1) = \frac{U_w}{\theta_{N,q}}(w(q-1)+1)$$

MAIN IDEA $\Rightarrow$ there exists an uncovered point A_{w+1} providing

$$\Delta_w(A_{w+1}) \geq \frac{\mathbf{E}}{D}, \quad D - \text{constant independent of q}$$

RIGOROUS PROOF — a part of steps of the iterative process

CONJECTURE — the rest of the steps

CONJECTURE

Conjecture

(i) (the generalized conjecture) *In* $\mathrm{PG}(N,q)$, *for* q *large enough, for every* $(w+1)$*-th step of the iterative process, there is a* w*-cap* $\mathcal{K}_w \in \mathbf{S}(U_w)$ *such that there exists an uncovered point* A_{w+1} *providing*

$$\Delta_w(A_{w+1}) \geq \frac{\mathbf{E}}{D}, \tag{1}$$

where $D \geq 1$ *is a constant independent of* q.

(ii) (the basic conjecture) *In* (1) *we have* $D = 1$.

new upper bound (under Conjecture)

Theorem

(i) *Under Conjecture (i), in* $\mathrm{PG}(N,q)$, $N \geq 3$, *it holds that*

$$t_2(N,q) < \frac{\sqrt{D}}{q-1}\sqrt{q^{N+1}(N+1)\ln q} + \frac{\sqrt{q^{N+1}}}{q-3},$$

$$t_2(N,q) \sim \sqrt{D(N+1)} \cdot q^{\frac{N-1}{2}}\sqrt{\ln q},$$

where $D \geq 1$ *is a constant independent of* q.

(ii) *Under Conjecture (ii), the bound above holds for* $D = 1$ *, i.e.*

$$t_2(N,q) \sim \sqrt{N+1} \cdot q^{\frac{N-1}{2}}\sqrt{\ln q}.$$

$\sim$ for q large enough

Estimate of average of $\Delta_w(A_{w+1})$: tool for rigorous proof

Δ_w^{aver} - the average value of $\Delta_w(A_{w+1})$ over all U_w uncovered points A_{w+1}

$$\max_{A_{w+1}} \Delta_w(A_{w+1}) \geq \Delta_w^{\text{aver}} = \frac{1}{U_w} \sum_{A_{w+1}} \Delta_w(A_{w+1}) \geq 1$$

Lemma

$$\Delta_w^{aver} \geq \max\{1, \frac{wU_w}{\theta_{N-1,q} + 1 - w} - w + 1\}$$

equality holds if every tangent contains:

the same number of uncovered points;

at most one uncovered point

rigorous proof for a part of the iterative process

Theorem

Let one of the following conditions hold:

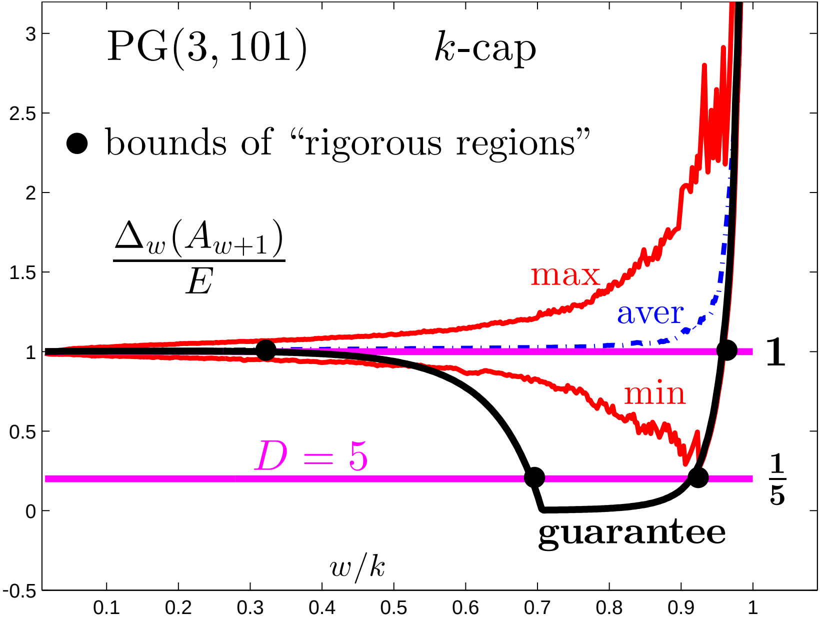
$$\frac{D(w-1)\theta_{N,q}(\theta_{N-1,q}+1-w)}{Dw\theta_{N,q}-(\theta_{N-1,q}+1-w)(w(q-1)+1)},$$

$$\frac{D\theta_{N,q}}{w(q-1)+1} \geq U_w.$$

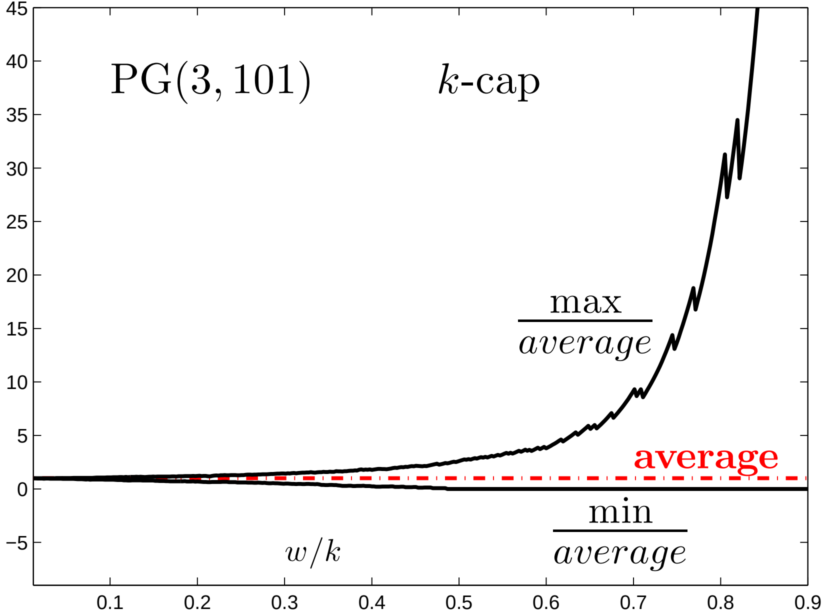
Then there exists an uncovered point A_{w+1} providing the inequality $\Delta_w(A_{w+1}) \geq \frac{\mathbf{E}}{D}$.

$D \geq 1$ *- constant independent of* q.

RIGOROUS proof vs CONJECTURE



the number of uncovered points on tangents



Thank you Spasibo

Premnogo blagodarya

Mille grazie

!'Muchas gracias

Toda raba

Merci beaucoup

Dankeschön

Dank u wel

Domo arigato