Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in DISCRETE MATHEMATICS

Electronic Notes in Discrete Mathematics 57 (2017) 21–26

www.elsevier.com/locate/endm

Upper bounds on the smallest size of a complete cap in PG$(3, q)$ and PG$(4, q)$

Daniele Bartoli[a, 1,3], Alexander A. Davydov[b, 2,4], Alexey A. Kreshchuk[b, 2,4], Stefano Marcugini[a, 1,3], Fernanda Pambianco[a, 1,3]

[a] *Dipartimento di Matematica e Informatica*
Università degli Studi di Perugia
Perugia, Italy

[b] *Institute for Information Transmission Problems (Kharkevich institute)*
Russian Academy of Sciences
Moscow, Russia

Abstract

In this work we summarize some recent results to be included in a forthcoming paper [2]. We present and analyze computational results concerning small complete caps in the projective spaces PG(N, q) of dimension $N = 3$ and $N = 4$ over the finite field of order q. The results have been obtained using randomized greedy algorithms and the algorithm with fixed order of points (FOP). The new complete caps are the smallest known. Based on them, we obtained new upper bounds on the minimum size $t_2(N, q)$ of a complete cap in PG(N, q), $N = 3, 4$. Our investigations and results allow to conjecture that these bounds hold for all q.

Keywords: Projective spaces, small complete caps, upper bounds

http://dx.doi.org/10.1016/j.endm.2017.02.005

1 Introduction. The main results

Let $\mathrm{PG}(N,q)$ be the N-dimensional projective space over the Galois field $\mathbb{F}_q$ of order q. A cap $\mathcal{K}$ in $\mathrm{PG}(N,q)$ is a set of points no three of which are collinear. A cap $\mathcal{K}$ is complete if it is not contained in a larger cap. Caps in $\mathrm{PG}(2,q)$ are also called arcs and they have been widely studied, see e.g. [6,8]. If $N>2$ only few constructions and bounds are known, see e.g. [1, 4, 6, 7, 9].

Caps are connected with Coding Theory. Points of an n-cap in $\mathrm{PG}(N,q)$ form columns of a parity-check matrix of a linear q-ary code of length n, dimension $n-N-1$, and minimum distance 4 (exceptions are given by the 5-cap in $\mathrm{PG}(3,2)$ and the 11-cap in $\mathrm{PG}(4,3)$). For $N=2$ this code is maximum distance separable (MDS); if $N=3$ it is Almost MDS code. Complete caps correspond to non-extendable quasi-perfect codes with covering radius 2.

A central problem concerning caps is to determine the spectrum of the possible sizes of complete caps in a given space. Of particular interest for applications to Coding Theory is the lower part of the spectrum; in fact, small complete caps correspond to codes with small covering density [6].

We denote by $t_2(N,q)$ *the minimum size of a complete cap* in $\mathrm{PG}(N,q)$. The exact values of $t_2(N,q)$ are known only for very small q.

The trivial lower bound for $t_2(N,q)$ is $\sqrt{2}q^{(N-1)/2}$. General constructions of complete caps whose size is close to this lower bound are only known for q even [6]. Using a modification of the approach of [8], the probabilistic upper bound $t_2(N,q) < cq^{\frac{N-1}{2}}\log^{300} q$, with c constant, has been obtained in [5]. Computer assisted results on small complete caps in $\mathrm{PG}(N,q)$ and $\mathrm{AG}(N,q)$ are given in [4,6,7,9]. Here $\mathrm{AG}(N,q)$ is the N-dimensional affine space over $\mathbb{F}_q$.

In this paper we obtain by computer search [5] results concerning upper bounds on $t_2(3,q)$ and $t_2(4,q)$. This search requested a huge of memory and execution time. We constructed small complete caps in $\mathrm{PG}(3,q)$ and $\mathrm{PG}(4,q)$ using two approaches: *the algorithm with fixed order of points (FOP)*, for $q\in L_N$ in $\mathrm{PG}(N,q)$, and *randomized greedy algorithms*, for $q\in G_N$ in $\mathrm{PG}(N,q)$,

[1] The research of D. Bartoli, S. Marcugini and F. Pambianco was supported in part by Ministry for Education, University and Research of Italy (MIUR) (Project "Geometrie di Galois e strutture di incidenza") and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INDAM).

[2] The research of A.A. Davydov and A.A. Kreshchuk was carried out at the IITP RAS at the expense of the Russian Foundation for Sciences (project 14-50-00150).

[3] Email: {daniele.bartoli,stefano.marcugini,fernanda.pambianco}@unipg.it

[4] Email: {adav,krsch}@iitp.ru

[5] Calculations were performed using computational resources of Multipurpose Computing Complex of National Research Centre "Kurchatov Institute", http://computing.kiae.ru

where $N = 3, 4$ and $L_3 := \{\text{prime } q \leq 4673\} \cup \{5003, 6007, 7001, 8009\}$, $G_3 := \{\text{prime } q \leq 3701\} \cup \{3803, 3907, 4001, 4289\}$, $L_4 := \{\text{prime } q \leq 1361\} \cup \{1409\}$, $G_4 := \{\text{prime } q \leq 463\}$. Such relatively wide regions of q values are not considered in the literature for $\mathrm{PG}(3, q)$ and $\mathrm{PG}(4, q)$.

Sizes of new small complete caps obtained by computer search give rise to the following theorem.

Theorem 1.1 *Let $t_2(N, q)$ be the minimum size of a complete cap in the projective space $\mathrm{PG}(N, q)$. The following upper bounds on $t_2(N, q)$ hold.*

A. *Upper bounds with the constant multiplier $\sqrt{N+2}$:*

$$t_2(N, q) < \sqrt{N+2} \cdot q^{\frac{N-1}{2}} \sqrt{\ln q}, \quad q \in L_N, \quad N = 3, 4. \tag{1}$$

B. *Upper bounds with a decreasing multiplier $\beta_N(q)$:*

$$t_2(N, q) < \beta_N(q) \cdot q^{\frac{N-1}{2}} \sqrt{\ln q}, \; \beta_N(q) = \sqrt{N+1} + \frac{1.3}{\ln(2q)}, \; q \in L_N, \; N = 3, 4.$$

Conjecture 1.2 *In $\mathrm{PG}(N, q)$, $N = 3, 4$, the bounds (1) hold for all q.*

Complete caps obtained in this work are *the smallest known in the literature* for prime q with $61 \leq q \in L_3$ in $\mathrm{PG}(3, q)$ and $17 \leq q \in L_4$ in $\mathrm{PG}(4, q)$.

2 Algorithms for small caps in $\mathrm{PG}(N, q)$. Graphics

Algorithm with fixed order of points (FOP). We fix a particular order on the points of $\mathrm{PG}(N, q)$ [1]. The algorithm builds a complete cap step by step adding a new point at each step. Let $K^{(i-1)}$ be the cap obtained at the $(i-1)$-th step. Among the points not lying on bisecants of $K^{(i-1)}$, the first point in the fixed order is added to $K^{(i-1)}$ to obtain $K^{(i)}$.

Algorithm FOP with lexicographical order of points. The points of $\mathrm{PG}(N, q)$ are ordered as $A_1, A_2, \ldots, A_{\frac{q^{N+1}-1}{q-1}}$. For simplicity, we considered only q prime. The number i of a point A_i of $\mathrm{PG}(N, q)$ is defined as follows. The elements of the field $\mathbb{F}_q = \{0, 1, \ldots, q-1\}$ are treated as integers modulo q. A point A_i is represented in homogenous coordinates so that $A_i = (x_0^{(i)}, x_1^{(i)}, \ldots, x_N^{(i)})$, $x_j^{(i)} \in \mathbb{F}_q$, where the leftmost non-zero element is 1. The points of $\mathrm{PG}(N, q)$ are sorted according to the lexicographic order on the $(N+1)$-tuples of their coordinates; it means that $i = \sum_{j=0}^{N} q^{N-j} x_j^{(i)}$. This order is called a *lexicographical order of points*. We call *lexicap* a cap obtained by the algorithm FOP with the lexicographical order of points.

We denote by $t_2^L(N,q)$ *the size of a complete lexicap* in $\mathrm{PG}(N,q)$.

Remark 2.1 For the lexicographical order with prime q, *the size* $t_2^L(N,q)$ *of a complete lexicap and its set of points depend on* N *and* q *only.*

Randomized greedy (RG) algorithm. It is a step by step algorithm. At every step an RG algorithm maximizes the number of points lying on bisecants of the running cap; but some steps are executed in a random manner. RG algorithms obtain complete caps smaller than lexicaps, but their computer time is essentially greater than for the algorithm FOP.

Let $t_2^G(N,q)$ denote *the smallest size of a complete cap* in $\mathrm{PG}(N,q)$ obtained using *randomized greedy algorithms.*

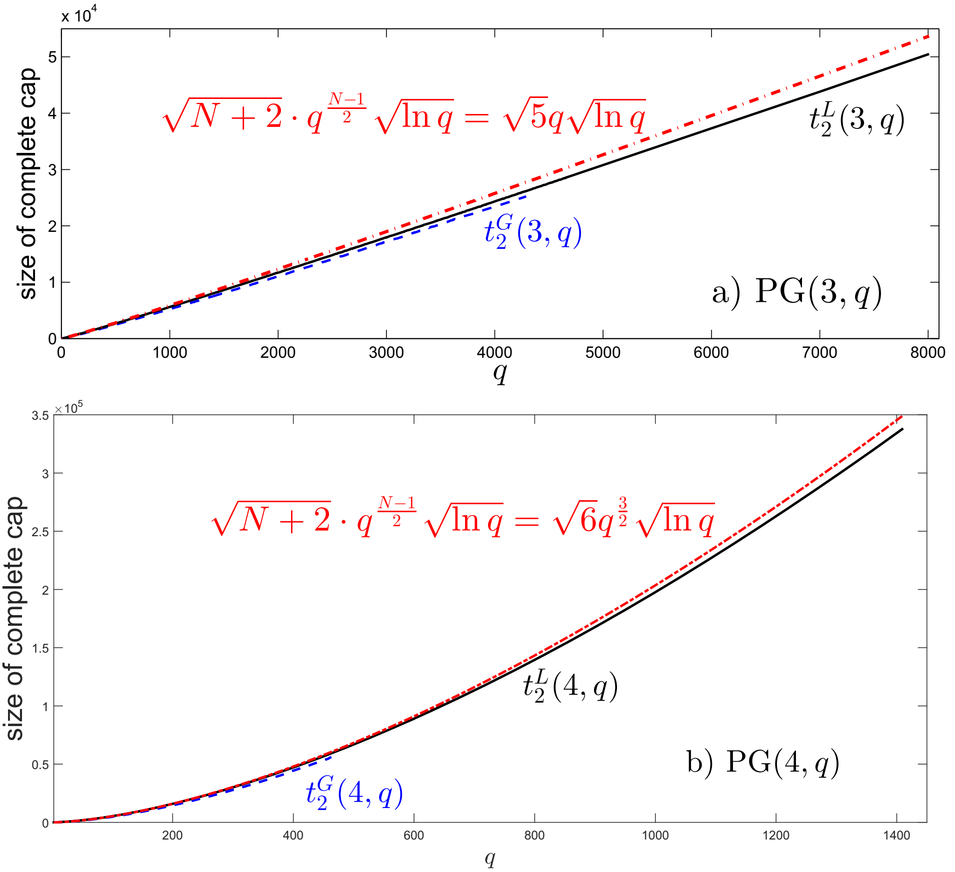

Fig. 1. **Upper bound** $\sqrt{N+2}\cdot q^{\frac{N-1}{2}}\sqrt{\ln q}$ (*top dashed-dotted red curve*) **vs values** $t_2^L(N,q)$, $q \in L_N$ (*the 2-nd solid black curve*) and $t_2^G(N,q)$, $q \in G_N$(*bottom dashed blue curve*). a) $N=3$, $\mathrm{PG}(3,q)$; b) $N=4$, $\mathrm{PG}(4,q)$

The bounds of Theorem 1.1 are shown in Figures 1, 2. In the scale of Fig. 1 the curves $t_2^L(N,q)$ and $t_2^G(N,q)$ are close to each other.

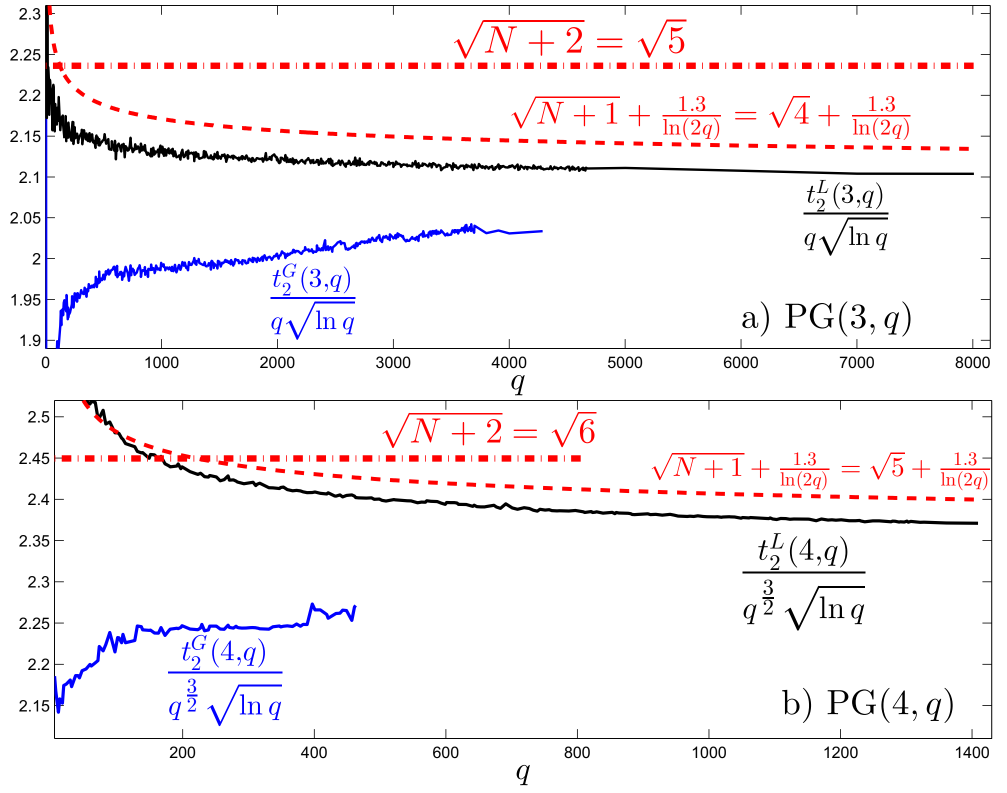

Fig. 2. **Upper bounds** $\frac{t_2(N,q)}{q^{\frac{N-1}{2}}\sqrt{\ln q}}<\sqrt{N+2}$ (*dashed-dotted red line* $y=\sqrt{N+2}$) and $\frac{t_2(N,q)}{q^{\frac{N-1}{2}}\sqrt{\ln q}}<\sqrt{N+1}+\frac{1.3}{\ln(2q)}$ (*top dashed red curve*) **vs values** of $\frac{t_2^L(N,q)}{q^{\frac{N-1}{2}}\sqrt{\ln q}}$, $q\in L_N$ (*the 2-nd solid black curve*) and $\frac{t_2^G(N,q)}{q^{\frac{N-1}{2}}\sqrt{\ln q}}$, $q\in G_N$ (*bottom solid blue curve*). a) $N=3$, PG$(3,q)$; b) $N=4$, PG$(4,q)$

For small q the bounds of Theorem 1.1 are provided by sizes $t_2^G(N,q)$, see Fig. 2. But, in general, values $t_2^G(N,q)$ depend on parameters of an RG algorithm, whereas sizes $t_2^L(N,q)$ depend on N, q only (Remark 2.1). Also, the algorithm FOP takes essentially smaller computer time than RG algorithms.

Let $B_N=\sqrt{N+2}\cdot q^{\frac{N-1}{2}}\sqrt{\ln q}$. By Figure 1, one sees that the difference $B_N-t_2^L(N,q)$ increases when q grows. Moreover, we calculated that the corresponding relative difference $\frac{B_N-t_2^L(N,q)}{B_N}$ increases too. We denote $\beta_N^L(q)=\frac{t_2^L(N,q)}{q^{\frac{N-1}{2}}\sqrt{\ln q}}$. Figure 2 shows that the curves $\beta_N^L(q)$ have decreasing trend. All this raises confidence in correctness of the bound (1) and explains Conjecture 1.2.

Sizes $t_2^L(N,q)$ and $t_2^G(N,q)$ of complete caps obtained in this work and other details are given in [2, 3].

References

[1] Bartoli, D., A. A. Davydov, G. Faina, S. Marcugini and F. Pambianco, *New upper bounds on the smallest size of a complete cap in the space* PG$(3,q)$, in "Proc. VII Int. Workshop on Optimal Codes and Related Topics", OC2013, Albena, Bulgaria, pp. 26–32, 2013.

[2] Bartoli, D., A. A. Davydov, A. A. Kreshchuk, S. Marcugini and F. Pambianco, *Small complete caps in* PG$(3,q)$ *and* PG$(4,q)$, preprint.

[3] Bartoli, D., A. A. Davydov, A. A. Kreshchuk, S. Marcugini and F. Pambianco, *Tables, bounds and graphics of the smallest known sizes of complete caps in the spaces* PG$(3,q)$ *and* PG$(4,q)$, arXiv:1610.09656[math.CO], (2016) https://arxiv.org/abs/1610.09656

[4] Bartoli, D., G. Faina and M. Giulietti, *Small complete caps in three-dimensional Galois spaces*, Finite Fields and Their Applications **24** (2013), 184–191.

[5] Bartoli, D., G. Faina, S. Marcugini and F. Pambianco, *A construction of small complete caps in projective spaces*, J. Geometry, to appear.

[6] Davydov, A. A., G. Faina, S. Marcugini and F. Pambianco, *On sizes of complete caps in projective spaces* PG(n,q) *and arcs in planes* PG$(2,q)$, J. Geometry **94** (2009), 31–58.

[7] Faina, G., F. Pasticci and L. Schmidt,: *Small complete caps in Galois spaces*, Ars Combinatoria **105** (2012), 299–303.

[8] Kim, J. H., and V. Vu, *Small complete arcs in projective planes*, Combinatorica **23** (2003), pp. 311–363.

[9] Platoni, I., *Complete caps in* AG$(3,q)$ *from elliptic curves*, J. Algebra and Its Applications **13** (2014), 1450050 (8 pages).