Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 27–34*

Conjectural upper bounds on the smallest size of a complete cap in $\mathrm{PG}(N,q)$, $N \geq 3$[1]

Daniele Bartoli daniele.bartoli@unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia
Via Vanvitelli 1, Perugia 06123 Italy
Alexander A. Davydov adav@iitp.ru
Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 127994, Russian Federation
Giorgio Faina, Stefano Marcugini, Fernanda Pambianco
{giorgio.faina,stefano.marcugini,fernanda.pambianco}@unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia
Via Vanvitelli 1, Perugia, 06123, Italy

Abstract. In this work we summarize some recent results to be included in a forthcoming paper [2]. In the projective space $\mathrm{PG}(N,q)$ over the Galois field of order q, $N \geq 3$, an iterative step-by-step construction of complete caps by adding a new point on every step is considered. It is proved that uncovered points are evenly placed on the space. A natural conjecture on an estimate of the number of new covered points on every step is done. For a part of the iterative process, this estimate is proved rigorously. Under the conjecture mentioned, new upper bounds on the smallest size $t_2(N,q)$ of a complete cap in $\mathrm{PG}(N,q)$ are obtained, in particular,

$$t_2(N,q) < \frac{1}{q-1}\sqrt{q^{N+1}(N+1)\ln q} + \frac{1}{q-3}\sqrt{q^{N+1}} \sim q^{\frac{N-1}{2}}\sqrt{(N+1)\ln q}.$$

A connection with the Birthday problem is noted. The effectiveness of the bounds is illustrated by comparison with sizes of complete caps obtained by computer.

1 Introduction. The main results

Let $\mathrm{PG}(N,q)$ be the N-dimensional projective space over the Galois field of order q. A cap in $\mathrm{PG}(N,q)$ is a set of points no three of which are collinear. A cap 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. [1, 6].

[1]The research of D. Bartoli, G. Faina, 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). The research of A.A. Davydov was carried out at the IITP RAS at the expense of the Russian Foundation for Sciences (project 14-50-00150).

Caps are connected with Coding Theory. A complete n-cap in a space $\mathrm{PG}(N,q)$, the points of which are treated as $(N+1)$-dimensional q-ary columns, defines a parity check matrix of a non-extandable linear q-ary code with length n, dimension $n-N-1$, minimum distance 4, and covering radius 2 (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 MDS; if $N=3$ it is Almost MDS.

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

A hard open problem in the study of projective spaces is the determination of $t_2(N,q)$. The exact values of $t_2(N,q)$ are known only for very small q.

This work is devoted to *upper bounds* on $t_2(N,q)$.

The trivial lower bound for $t_2(N,q)$ is $\sqrt{2}q^{\frac{N-1}{2}}$. Constructions of complete caps whose size is close to this lower bound are only known for q even [5]. Using a modification of the approach of [6], the probabilistic upper bound

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

where c is a constant independent of q, has been obtained in [3, 4].

Theorem 1. (i) *Under Conjecture* 4(i)*, in* $\mathrm{PG}(N,q)$*,* $N \geq 3$*, it holds that*

$$t_2(N,q) < \frac{\sqrt{D}}{q-1}\sqrt{q^{N+1}(N+1)\ln q} + \frac{\sqrt{q^{N+1}}}{q-3} \sim q^{\frac{N-1}{2}}\sqrt{D(N+1)\ln q}. \quad (1)$$

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

(ii) *Under Conjecture* 4(ii)*, the bound* (1) *with* $D=1$ *holds.*

Conjecture 2. *In* $\mathrm{PG}(N,q)$*,* $N \geq 3$*, the upper bound* (1) *with* $D=1$ *holds for all* q *without any extra conditions and conjectures.*

This work can be treated as a development and generalization of the paper [1].

2 An iterative process. Probabilities of uncovering. The basic and generalized conjectures

In $\mathrm{PG}(N,q)$, $N \geq 3$, let a complete cap be constructed by a step-by-step algorithm (*Algorithm* for short) which adds one new point to the cap in each step; see e.g. a greedy algorithm that in every step adds to the cap a point providing the maximal possible (for the given step) number of new covered points [1]. A *point* of $\mathrm{PG}(N,q)$ is *covered by* a *cap* if the point lies on a bisecant of the cap. The space $\mathrm{PG}(N,q)$ contains $\theta_{N,q} = \frac{q^{N+1}-1}{q-1} = q^N + q^{N-1} + \ldots + q + 1$ points.

Assume that after the w-th step of Algorithm a w-cap is obtained that does not cover exactly U_w points. Let $\mathbf{S}(U_w)$ be the set of all w-caps in $\mathrm{PG}(N,q)$ each of which does not cover exactly U_w points.

Consider the $(w+1)$-st step of Algorithm. This step starts from a w-cap $\mathcal{K}_w$ with $\mathcal{K}_w \in \mathbf{S}(U_w)$. The choice $\mathcal{K}_w$ from $\mathbf{S}(U_w)$ is random such that for every cap of $\mathbf{S}(U_w)$ the probability to be chosen is equal to $\frac{1}{\#\mathbf{S}(U_w)}$. So, the set $\mathbf{S}(U_w)$ is considered as an *ensemble of random objects* with the uniform probability distribution. Every point H of $\mathrm{PG}(N,q)$ is uncovered by $\mathcal{K}_w$ with some probability $p_w(H)$.

Lemma 3. *The probability $p_w(H)$ does not depend of the point H; it may be considered as p_w. Moreover,*

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

Let the cap $\mathcal{K}_w$ consist of w points $A_1, A_2, \ldots, A_w$. Let A_{w+1} be the point that will be included into the cap on the $(w+1)$-th step. The point A_{w+1} defines a bundle of w tangents $\overline{A_1A_{w+1}}, \ldots, \overline{A_wA_{w+1}}$ to $\mathcal{K}_w$. Excluding $A_1, \ldots, A_w$, all the points on the tangents of the bundle are **candidates** to be new covered points in the $(w+1)$-th step. There are $w(q-1)+1$ candidates in the bundle. One can use U_w distinct points A_{w+1}; therefore there are U_w distinct bundles.

Denote by $\mathbf{E}_{w,q}$ the **expected value** of the number of uncovered points among $w(q-1)+1$ randomly taken points in $\mathrm{PG}(N,q)$, if the events to be uncovered are independent. By Lemma 3,

$$\mathbf{E}_{w,q} = (w(q-1)+1)p_w = \frac{(w(q-1)+1)U_w}{\theta_{N,q}}. \tag{2}$$

Let $\Delta_w(A_{w+1})$ be the number of new covered points on the $(w+1)$-th step. Since all new covered points lie on some bundle, they cannot be considered as randomly taken points for which the events to be uncovered are independent.

In the other side, there are many random factors affecting the iterative process, e.g. relative positions and intersections of bisecants and tangents, the number of uncovered points on distinct tangents. Therefore, the conjecture below seems to be reasonable and founded, see also Section 4.

Conjecture 4. (i) ***(the generalized conjecture)*** *In $\mathrm{PG}(N,q)$, for q large enough, for every $(w+1)$-th step of the iterative process, there exists a w-cap $\mathcal{K}_w \in \mathbf{S}(U_w)$ such that there exists an uncovered point A_{w+1} providing inequality*

$$\Delta_w(A_{w+1}) \geq \frac{\mathbf{E}_{w,q}}{D}, \tag{3}$$

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

(ii) ***(the basic conjecture)*** *In (3) we have $D = 1$.*

3 Upper bounds on $t_2(N,q)$ and their effectiveness

Let $D \geq 1$ be a constant independent of q. We denote

$$Q = \frac{\theta_{N,q}}{q-1} = \frac{q^{N+1}-1}{(q-1)^2}, \quad f_q(w;D) = \prod_{i=1}^{w}\left(1 - \frac{i}{DQ}\right).$$

The function $f_{q,D}(w)$ with an integer D is used in the *Birthday problem*.

Theorem 5. *Let ξ be a constant independent of w with $\xi \geq 1$. Under Conjecture 4, in $PG(N,q)$ the following holds:*

$$t_2(N,q) \leq w + 1 + \xi$$

where the value w satisfies the inequality

$$\theta_{N,q} f_q(w;D) \leq \xi. \tag{4}$$

Theorem 6. *Let ξ be a constant independent of w with $\xi \geq 1$. Let $D \geq 1$ be a constant independent of q. Under Conjecture 4, it holds that*

$$t_2(N,q) \leq \sqrt{2DQ}\sqrt{\ln\frac{\theta_{N,q}}{\xi}} + 2 + \xi. \tag{5}$$

Taking in (5) $\xi = \frac{1}{q-1}\sqrt{q^{N+1}}$, we obtain Theorem 1.

An illustration of the effectiveness of the new upper bounds is shown on Fig. 1 where $t_2^G(N,q)$ is the size of a complete cap in $\mathrm{PG}(N,q)$ obtained by computer via greedy algorithms[2] in the region G_N where $G_3 = \{q \leq 3701,\ q \text{ prime}\} \cup \{3803, 3907, 4001, 4289\}$, $G_4 = \{q \leq 463,\ q \text{ prime}\} \cup \{503\}$.

4 Reasonableness of conjectures

For a cap $\mathcal{K}_w$, denote by $\Delta_w^{\mathrm{aver}}(\mathcal{K}_w)$ the average value of $\Delta_w(A_{w+1})$ by all U_w uncovered points A_{w+1}, i.e.

$$\Delta_w^{\mathrm{aver}}(\mathcal{K}_w) = \frac{1}{U_w}\sum_{A_{w+1}} \Delta_w(A_{w+1}) \geq 1. \tag{6}$$

Throughout the paper, we consider continuous approximations of the discrete function $\Delta_w(A_{w+1})$, $\Delta_w^{\mathrm{aver}}(\mathcal{K}_w)$ and other ones keeping the same notations.

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

Here and further, for practice calculations connected with the illustration of researches, see Remarks 9 and 10, we used the same cap adding to it one point in the each step of the iterative process; the random choice of the cap $\mathcal{K}_w$ is not applied.

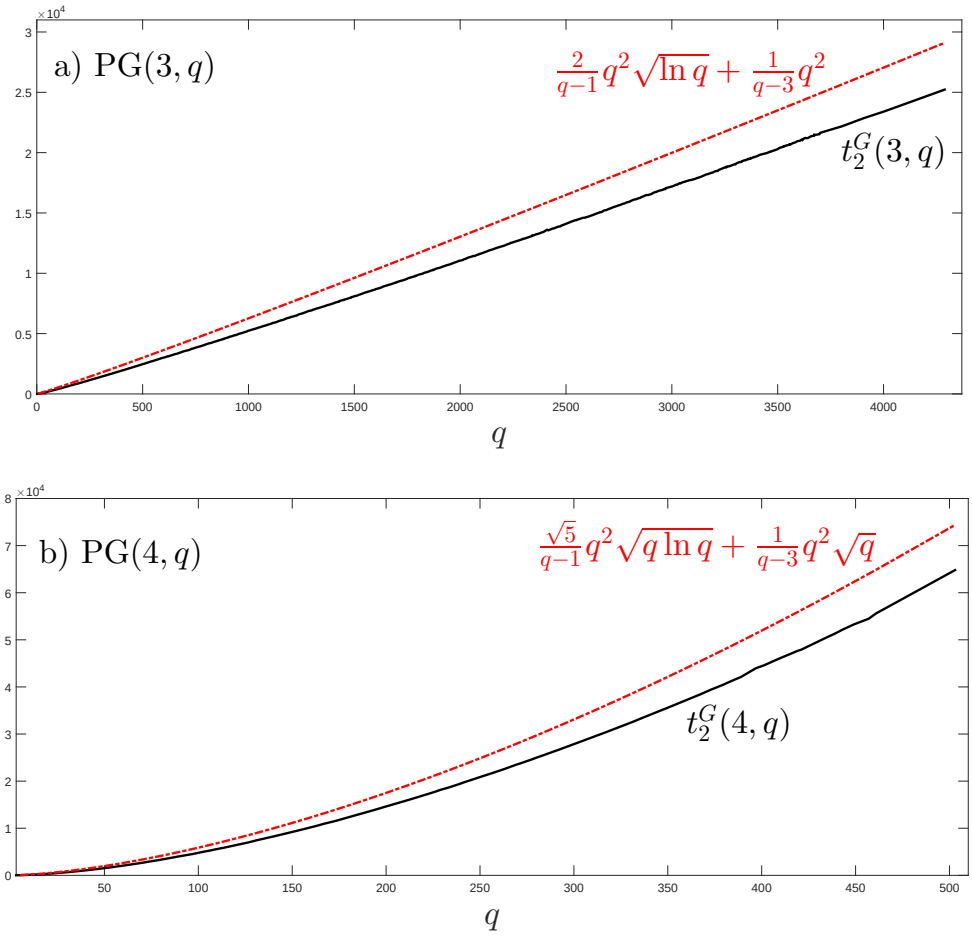

Figure 1: **Upper bounds** on $t_2(N,q)$ of (1) with $D=1$ (*top dushed-dotted curve*) **vs sizes** $t_2^G(N,q)$ of complete caps obtained by greedy algorithms (*bottom solid curve*), $q\in G_N$, $N=3,4$. a) PG$(3,q)$; b) PG$(4,q)$

Lemma 7. *For any w-cap $\mathcal{K}_w \in \mathbf{S}(U_w)$, there hold the following inequalities*

$$\max_{A_{w+1}} \Delta_w(A_{w+1}) \geq \Delta_w^{\rm aver}(\mathcal{K}_w) \geq \max\{1, \frac{wU_w}{\theta_{N-1,q}+1-w} - w + 1\}. \qquad (7)$$

The equalities $\max\limits_{A_{w+1}} \Delta_w(A_{w+1}) = \Delta_w^{\rm aver}(\mathcal{K}_w) = \frac{wU_w}{\theta_{N-1,q}+1-w} - w + 1$ *hold if and only if each tangent contains the same number of uncovered points. The equalities* $\max\limits_{A_{w+1}} \Delta_w(A_{w+1}) = \Delta_w^{\rm aver}(\mathcal{K}_w) = 1$ *hold if and only if each tangent contains at most one uncovered point.*

Let $D \geq 1$ be a constant independent of q. We denote

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

For a **part** of the **iterative process**, we **rigorously prove** Conjecture 4.

Theorem 8. *Let $D \geq 1$ be a constant independent of q. Let one of the following conditions hold: $U_w \geq \Phi_{w,q}(D)$, $\Upsilon_{w,q}(D) \geq U_w$. Then for any cap $\mathcal{K}_w$ of $\mathbf{S}(U_w)$, there exists an uncovered point A_{w+1} providing the inequality* (3).

Remark 9. To illustrate Conjecture 4, the values $\Delta_w(A_{w+1})$ were calculated for numerous concrete iterative processes. *For all the calculations done* it holds that $\max\limits_{A_{w+1}} \Delta_w(A_{w+1}) > \mathbf{E}_{w,q}$. The ratio $\max\limits_{A_{w+1}} \Delta_w(A_{w+1})/\mathbf{E}_{w,q}$ has an increasing trend when w grows. In Fig. 2 for a complete k-cap in $\mathrm{PG}(3,101)$, $k = 415$, the following values are shown (see (2)–(7)): $\delta_w^{\max} = \frac{1}{\mathbf{E}_{w,q}} \cdot \max\limits_{A_{w+1}} \Delta_w(A_{w+1})$ (*top solid curve*), $\delta_w^{\rm aver} = \frac{1}{\mathbf{E}_{w,q}} \cdot \Delta_w^{\rm aver}(\mathcal{K}_w)$ (*the 2-nd dashed-dotted curve*), $\delta_w^{\min} = \frac{1}{\mathbf{E}_{w,q}} \cdot \min\limits_{A_{w+1}} \Delta_w(A_{w+1})$ (*the 3-rd solid curve*), $\delta_w^{\rm rigor} = \frac{1}{\mathbf{E}_{w,q}} \cdot \max\{1, \frac{wU_w}{\theta_{N-1,q}+1-w} - w + 1\}$ (*bottom dotted curve*). The horizontal axis shows the values of $\frac{w}{k}$. The dashed lines $y = 1$ and $y = \frac{1}{5}$ correspond to Conjecture 4(ii) where $D = 1$ and to Conjecture 4(i) with $D = 5$. The signs $\bullet$ correspond to values $\Phi_{w,q}(D)$ and $\Upsilon_{w,q}(D)$ with $D = 1$ and $D = 5$.

In Fig. 2, the region where we rigorously prove Conjecture 4 lies left of $\Phi_{w,q}(D)$ and right of $\Upsilon_{w,q}(D)$. This region takes $\sim 35\%$ of the whole iterative process for $D = 1$ and $\sim 75\%$ for $D = 5$.

Remark 10. Let $\gamma_{w,j}$ be the number of uncovered points on the j-th tangent after the w-th step of Algorithm. The lower estimate in (7) is attained in two cases: either *every tangent contains the same number of uncovered points* (i.e.

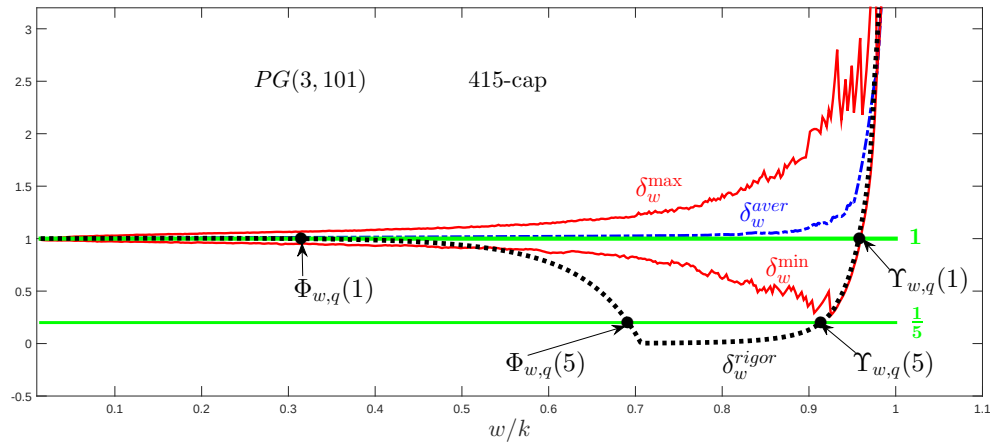

Figure 2: **Illustration of reasonableness of Conjectures 4(i) and 4(ii)**

$\gamma_{w,j} = \gamma_{w,i}$ for all pairs i, j) or *each tangent contains at most one uncovered point*. The 1-st situation holds in the first steps of the iterative process only. Then while the inequality $U_w(D) \geq \Phi_{w,q}(D)$ holds, the differences $\gamma_{w,j} - \gamma_{w,i}$ are relatively small and estimate (7) works "well". As U_w decreases, the differences relatively increase, and the estimate becomes worse in the sense that actually $\Delta_w^{\rm aver}(\mathcal{K}_w)$ is considerably greater than $\max\{1, \frac{wU_w}{\theta_{N-1,q}+1-w} - w + 1\}$.

The 2-nd situation is possible, in principle, when $U_w \leq \theta_{N-1,q}+1-w$ and the average number $\gamma_w^{\rm aver}$ of uncovered points on a tangent is smaller than 1. But on this stage of the iterative process variations in the values $\gamma_{w,j}$ are relatively big; and again $\Delta_w^{\rm aver}(\mathcal{K}_w)$ is considerably greater than $\max\{1, \frac{wU_w}{\theta_{N-1,q}+1-w} - w + 1\}$.

In the final region of the iterative process, where $U_w \leq \Upsilon_{w,q}(D)$ and $\frac{\mathbf{E}_{w,q}}{D} \leq 1$, estimate (7) becomes reasonable once more. Thus, in the region $\Phi_{w,q}(D) > U_w > \Upsilon_{w,q}(D)$ the estimate (7) does not reflect the real situation effectively.

Denote by $\gamma_w^{\rm aver}$ the average number of uncovered point on a tangent. It holds that $\gamma_w^{\rm aver} = U_w/(\theta_{N-1,q} + 1 - w)$. Let $\gamma_w^{\max}$ and $\gamma_w^{\min}$ be the maximum and minimum of the number $\gamma_{w,j}$ of uncovered points on a tangent, respectively. An illustration of the fact that the numbers $\gamma_{w,j}$ of uncovered points on tangents lie in a relatively wide region is shown on Fig. 3, where for complete k-caps in PG$(3, 101)$, $k = 415$ obtained by the greedy algorithm, the values $\gamma_w^{\max}/\gamma_w^{aver}$ (*top solid curve*) and $\gamma_w^{\min}/\gamma_w^{aver}$ (*bottom solid curve*) are presented. The value $\gamma_w^{\max}/\gamma_w^{aver}$ increases when the ratio w/k grows; in the region $0.8 < \frac{w}{k} < 0.95$ (it is not shown in Fig. 3), the value $\gamma_w^{\max}/\gamma_w^{aver}$ increases from 28 to 590.

Other estimates and bounds on $t_2(N, q)$ are given in [2].

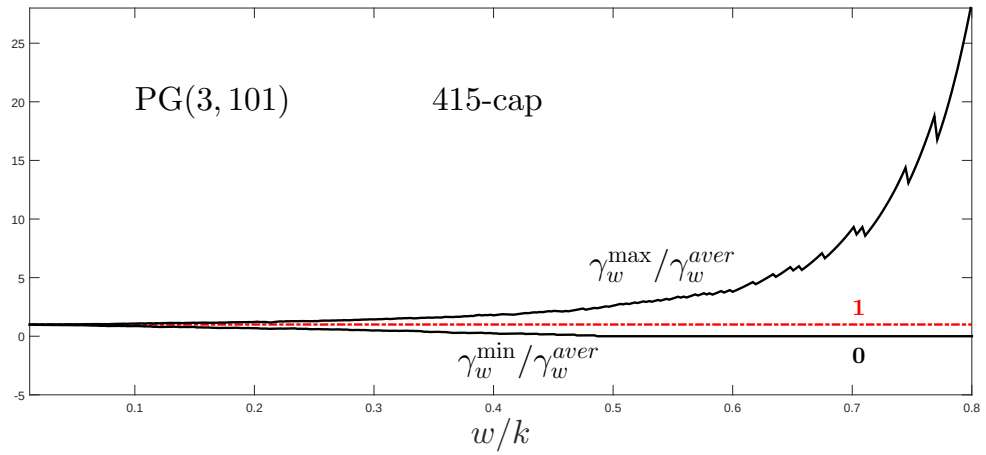

Figure 3: **Dispersion of the number of uncovered points on tangents**

References

[1] D. Bartoli, A.A. Davydov, G. Faina, G., A.A. Kreshchuk, S. Marcugini, F. Pambianco, Upper bounds on the smallest size of a complete arc in PG$(2, q)$ under a certain probabilistic conjecture. *Problems Inform. Transmission* **50**, 2014, 320–339.

[2] D. Bartoli, A.A. Davydov, G. Faina, G., S. Marcugini, F. Pambianco, Upper bounds on the smallest size of a complete cap in PG(N, q) under a certain probabilistic conjecture, preprint.

[3] D. Bartoli, S. Marcugini, F. Pambianco, A probabilistic construction of low density quasi-perfect linear codes, In *Proc. XIV Int. Workshop on Algebraic and Combinatorial Coding Theory, ACCT2014, Svetlogorsk, Russia,* pp. 51–56, 2014. http://www.moi.math.bas.bg/acct2014/a8.pdf

[4] D. Bartoli, S. Marcugini, F. Pambianco, A construction of small complete caps in projective spaces, submitted.

[5] A.A. Davydov, M. Giulietti, S. Marcugini, F. Pambianco, New inductive constructions of complete caps in PG(n, q), q even. *J. Combin. Des.* **18**, 2010, 177–201.

[6] J.H. Kim, V. Vu, Small complete arcs in projective planes. *Combinatorica* **23**, 2003, 311–363.