ISSN 0032-9460, Problems of Information Transmission, 2014, Vol. 50, No. 4, pp. 320–339. © Pleiades Publishing, Inc., 2014.
Original Russian Text © D. Bartoli, A.A. Davydov, G. Faina, A.A. Kreshchuk, S. Marcugini, F. Pambianco, 2014, published in Problemy Peredachi Informatsii, 2014, Vol. 50, No. 4, pp. 22–42.

Upper Bounds on the Smallest Size of a Complete Arc in $PG(2,q)$ under a Certain Probabilistic Conjecture

D. Bartoli[a,1,2], **A. A. Davydov**[b], **G. Faina**[a,1], **A. A. Kreshchuk**[b], **S. Marcugini**[a,1], **and F. Pambianco**[a,1]

[a] *Department of Mathematics and Computer Sciences, Università degli Studi di Perugia, Italy*
e-mail: daniele.bartoli@dmi.unipg.it, faina@dmi.unipg.it, gino@dmi.unipg.it, fernanda@dmi.unipg.it
[b] *Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow, Russia*
e-mail: adav@iitp.ru, krsch@iitp.ru

Received April 19, 2014; in final form, August 25, 2014

Abstract—In the projective plane $PG(2,q)$, we consider an iterative construction of complete arcs which adds a new point in each step. It is proved that uncovered points are uniformly distributed over the plane. For more than half of steps of the iterative process, we prove an estimate for the number of newly covered points in every step. A natural (and well-founded) conjecture is made that the estimate holds for the other steps too. As a result, we obtain upper bounds on the smallest size $t_2(2,q)$ of a complete arc in $PG(2,q)$, in particular,

$$t_2(2,q) < \sqrt{q}\sqrt{3\ln q + \ln\ln q + \ln 3} + \sqrt{\frac{q}{3\ln q}} + 3,$$
$$t_2(2,q) < 1.87\sqrt{q\ln q}.$$

Nonstandard types of upper bounds on $t_2(2,q)$ are considered, one of them being new. The effectiveness of the new bounds is illustrated by comparing them with the smallest known sizes of complete arcs obtained in recent works of the authors and in the present paper via computer search in a wide region of q. We note a connection of the considered problems with the so-called birthday problem (or birthday paradox).

DOI: 10.1134/S0032946014040036

1. INTRODUCTION

Let $PG(2,q)$ be the projective plane over the Galois field of q elements. An n-arc is a set of n points no three of which are collinear. An n-arc is said to be complete if it is contained in no $(n+1)$-arc in $PG(2,q)$. For an introduction to projective geometries over finite fields, see [1–3].

Relationships between the theory of n-arcs, coding theory, and mathematical statistics are presented in [4, 5] (see also [6]). In particular, a complete arc in $PG(2,q)$, the points of which are treated as 3-dimensional q-ary columns, defines a parity-check matrix of a q-ary linear code with codimension 3, Hamming distance 4, and covering radius 2. Arcs can be interpreted as linear

[1] Supported in part by the Ministry for Education, University and Research of Italy (MIUR), project "Geometrie di Galois e strutture di incidenza," and Italian National Group for Algebraic and Geometric Structures and their Applications (G.N.S.A.G.A.).
[2] Supported by the European Community under a Marie-Curie Intra-European Fellowship, FACE project no. 626511.

maximum distance separable (MDS) codes [7, Section 7; 8]; they are related to optimal coverings arrays [9], superregular matrices [10], and quantum codes [11].

A point set $S \subset PG(2,q)$ is 1-*saturating* if any point of $PG(2,q) \setminus S$ is collinear with two points in S [12–15]. Points of a 1-saturating set in $PG(2,q)$ form a parity-check matrix of a *linear covering code* with codimension 3 and covering radius 2. Finding small 1-saturating sets (respectively, short covering codes) is an open problem. A complete arc in $PG(2,q)$ is, in particular, a 1-saturating set; often, the smallest known complete arc is the smallest known 1-saturating set [12–16]. Let $\ell_1(2,q)$ be the smallest size of a 1-saturating set in $PG(2,q)$. In [17,18], for q large enough, the following upper bound is proved by probabilistic methods (for $3\sqrt{2}$, see [17, p. 24]):

$$\ell_1(2,q) < 3\sqrt{2}\sqrt{q\ln q} < 5\sqrt{q\ln q}. \tag{1}$$

Finding the spectrum of possible sizes of complete arcs is one of the main problems in the study of projective planes, which is also of interest in coding theory. In particular, of interest is the value of the smallest size of a complete arc in $PG(2,q)$, denoted by $t_2(2,q)$. Finding estimates for $t_2(2,q)$ is a hard open problem.

This paper is devoted to *upper bounds* on $t_2(2,q)$.

Surveys of results on sizes of plane complete arcs and methods for their construction can be found in [1–5, 7, 15, 19–31].

Problems connected with small complete arcs in $PG(2,q)$ are considered in [1–5,7,12–16,19–64]; see also references therein.

Exact values of $t_2(2,q)$ are known for $q \le 32$ only; see [1,44,52,56,57] and the paper [12], where the equalities $t_2(2,31) = t_2(2,32) = 14$ are established.

There are the following lower bounds (see [2,33,40,59] and references therein):

$$t_2(2,q) > \begin{cases} \sqrt{2q}+1 & \text{for any } q, \\ \sqrt{3q}+\frac{1}{2} & \text{for } q=p^h,\ p \text{ prime},\ h=1,2,3. \end{cases} \tag{2}$$

Let $t(\mathcal{P}_q)$ be the size of the smallest complete arc in any (not necessarily Desarguesian) projective plane $\mathcal{P}_q$ of order q. In [24], for q *large enough*, the following result is proved by *probabilistic methods* (we give it in the form used in [5, Table 2.6] taking into account the remark [24, p. 320] that all logarithms in [24] are to the natural base):

$$t(\mathcal{P}_q) \le D\sqrt{q}\ln^C q, \quad C \le 300, \tag{3}$$

where C and D are constants independent of q (so-called universal or absolute constants). The authors of [24] conjectured that the constant C can be reduced to $C = 10$. A survey and analysis of random constructions for geometric objects can be found in [17, 18, 46].

In [24,40] it is noted that in a preliminary report of 1989 J.C. Fisher by computer search obtained complete arcs in many planes of small orders and conjectured that the average size of a complete arc is about $\sqrt{3q\log q}$.

Using *algebraic constructions* (see [5, p. 209]), complete arcs in $PG(2,q)$ were obtained with sizes of approximately $\frac{1}{3}q$ [19, 28, 29, 32, 53, 54, 60, 64], $\frac{1}{4}q$ [19, 30, 54], $2q^{0.9}$ for $q > 7^{10}$ [28], and $2.46q^{0.75}\ln q$ for large prime q [53]. It is noted in [46, Section 8] that the smallest size of a complete arc in $PG(2,q)$ obtained via algebraic constructions is

$$cq^{3/4}, \tag{4}$$

where c is a universal constant [7, Theorem 6.8; 30, Section 3].

Denote by $\overline{t}_2(2,q)$ the smallest *known size* of a complete arc in $PG(2,q)$.

From [19,20] (see also references therein) it follows that $\overline{t}_2(2,q) < 4\sqrt{q}$ for $q \le 841$ and $q = 857$. Complete $(4\sqrt{q}-4)$-arcs are obtained for odd $q = p^2$ with $p \le 41$ and $p = 7^2$ [47,51], and for $q = 2^6$, 2^8, 2^{10} [42,43]. Thus,

$$t_2(2,q) < 4\sqrt{q} \quad \text{for} \quad q \le 841,\ q = 857,\ 31^2,\ 2^{10},\ 37^2,\ 41^2,\ 7^4.$$

For $q \le 151$, a number of improvements for $\overline{t}_2(2,q)$ are given in [16].

In [41], $(6\sqrt{q}-6)$-arcs in $PG(2,q)$, $q = 4^{2h+1}$, are constructed; for $h \le 4$ it is proved that they are complete. This gives a complete 3066-arc in $PG(2,2^{18})$.

For $q \le 13\,627$ and a number of sporadic $q \le 45\,893$, values of $\overline{t}_2(2,q)$ (up to January 2013) are collected in [19,20], where the following results are obtained:

$$\begin{aligned}
&t_2(2,q) < 4.5\sqrt{q} && \text{for } q \le 2647,\ q = 2659, 2663, 2683, 2693, 2753, 2801;\\
&t_2(2,q) < 5\sqrt{q} && \text{for } q \le 9497,\ q = 9539, 9587, 9613, 9623, 9649, 9689, 9923, 9973;\\
&t_2(2,q) < \sqrt{q}\ln^{0.72983} q && \text{for } 109 \le q \le 13\,627.
\end{aligned}$$

Let Q_1 be the following set of values of q:

$$\begin{aligned}
Q_1 = &\{2 \le q \le 49\,727,\ q \text{ prime power}\}\\
&\cup \{2 \le q \le 150\,001,\ q \text{ prime}\}\\
&\cup \{40 \text{ sporadic prime } q \text{ in the interval } [150\,503 \ldots 410\,009]\}.
\end{aligned} \tag{5}$$

The values of q in the interval $[150\,503 \ldots 410\,009]$ corresponding to the last row of formula (5) are given in [35, Table 6]. For $q \in Q_1$, the smallest known values of $\overline{t}_2(2,q)$ (up to August 2014) are collected in the recent work [35], where the following bound is obtained:

$$t_2(2,q) < \sqrt{q}\ln^{0.7295} q, \quad 109 \le q, \quad q \in Q_1. \tag{6}$$

In [19,20,35], most of the values $\overline{t}_2(2,q)$ have been obtained by computer search using randomized greedy algorithms described in [19–22,37,65].

In the present paper, the following results are obtained.

• An iterative construction of complete arcs is considered, which adds a new point in each step. It is proved that uncovered points are uniformly distributed over the plane. For more than half of steps of the iterative process, an estimate for the number of newly covered points in each step is proved. A natural and well-founded conjecture is made that the estimate holds for the other steps too (see Conjecture 2). Under this conjecture, new upper bounds on $t_2(2,q)$ are obtained (see (10), (11), and Theorems 2 and 4).

• Investigations of nonstandard types of upper bounds on $t_2(2,q)$ connected with decreasing functions are continued (see (7)). One more type of such upper bounds is proposed (see (8)). For these types of bounds, new estimates are obtained (see (12)–(14) and Corollary 2).

• The reasonableness of Conjecture 2 and effectiveness of the new bounds are illustrated by comparing the bounds with the smallest known sizes $\overline{t}_2(2,q)$ of complete arcs in $PG(2,q)$ obtained in the works of the authors [19, 20, 35] and in the present paper via computer search in a wide region of q (see (5), (53), (54), and Figs. 1–3 in Section 6).

Here are some details of the above-mentioned new results.

In the works of the authors [20, 34, 37–39], nonstandard types of upper bounds on $t_2(2,q)$ are proposed. They are based on decreasing functions $c(q)$ and $d(q)$ defined by the following relations:

$$t_2(2,q) = \sqrt{q}\ln^{c(q)} q, \qquad c(q) = \frac{\ln(t_2(2,q)/\sqrt{q})}{\ln\ln q}, \qquad t_2(2,q) = d(q)\sqrt{q}\ln q. \tag{7}$$

In this paper, we propose one more form of an upper bound on $t_2(2,q)$, connected with an upper estimate for a *decreasing function* $m(q)$ given by

$$t_2(2,q) = m(q)\sqrt{q \ln q}. \tag{8}$$

Throughout the paper we denote

$$\widehat{t}_2(2,q) = \sqrt{q}\sqrt{3\ln q + \ln\ln q + \ln 3} + \sqrt{\frac{q}{3\ln q}} + 3. \tag{9}$$

Theorem 1, based on Theorems 2–4 and Corollary 2, summarizes the results of the present paper.

Theorem 1. *Let $c(q)$, $d(q)$, $m(q)$, and $\widehat{t}_2(2,q)$ be given by* (7)–(9). *Let $t_2(2,q)$ be the smallest size of a complete arc in the plane $PG(2,q)$.*

(i) *Under Conjecture* 2, *in $PG(2,q)$ we have the following estimates*:

$$t_2(2,q) < \widehat{t}_2(2,q) = \sqrt{q}\sqrt{3\ln q + \ln\ln q + \ln 3} + \sqrt{\frac{q}{3\ln q}} + 3, \tag{10}$$

$$t_2(2,q) < 1.87\sqrt{q\ln q}, \tag{11}$$

$$c(q) < \frac{\ln(\widehat{t}_2(2,q)/\sqrt{q})}{\ln\ln q}, \tag{12}$$

$$d(q) < \frac{\widehat{t}_2(2,q)}{\sqrt{q}\ln q}, \tag{13}$$

$$m(q) < \sqrt{3 + \frac{\ln\ln q + \ln 3}{\ln q}} + \frac{1}{\sqrt{3}\ln q} + \frac{3}{\sqrt{q\ln q}}; \tag{14}$$

(ii) *Let Conjecture* 2 *hold. Then complete arcs in the plane $PG(2,q)$ satisfying all the upper bounds* (10)–(14) *can be constructed with the help of a step-by-step greedy algorithm which in every step adds a point to the arc providing the maximum possible* (*for the given step*) *number of newly covered points*;

(iii) *Let Q be the set of values of q given by relations* (5), (53), *and* (54). *The sizes $\overline{t}_2(2,q)$ of the smallest known complete arcs in $PG(2,q)$, $q \in Q$, collected in* [35] *and obtained in the present paper satisfy all the upper bounds* (10)–(14).

Our investigations and results allow us to formulate the following conjecture.

Conjecture 1. *In the projective plane $PG(2,q)$, the upper bounds* (10) *and* (11) *hold for all q without any additional conditions.*

The paper is organized as follows. In Section 2 we describe the iterative process and its properties. In Sections 3 and 4 upper bounds on $t_2(2,q)$ are considered. In Section 5 we present nonstandard types of upper bounds based on the results of Sections 3 and 4. In Section 6 we compare the smallest known sizes of complete arcs with the upper bounds of Sections 3–5.

Some results of this work were briefly presented in [34, 36].

2. ANALYSIS OF THE ITERATIVE PROCESS

2.1. Iterative Process

Assume that a complete arc in $PG(2,q)$ is constructed by a step-by-step algorithm (the *Algorithm* for short) which adds one new point to the arc in each step. As an example, we can mention the greedy algorithm that in every step adds to the arc a point providing the maximal possible (for the given step) number of newly covered points; see [19–22, 37, 65] and Section 6.

Recall that a point of $PG(2,q)$ is *covered* by an *arc* if the point lies on a bisecant of the arc, i.e., on a line meeting the arc at two points. Clearly, all points of the arc are covered. The plane $PG(2,q)$ contains q^2+q+1 points.

Consider the $(w+1)$st step of the Algorithm. This step starts with a w-arc chosen as follows. Assume that after the wth step of the Algorithm a w-arc is obtained that does not cover exactly U_w points. Let $\boldsymbol{S}_w(U_w)$ be the set of all w-arcs in $PG(2,q)$ each of which does not cover exactly U_w points. Obviously, the group of collineations $P\Gamma L(3,q)$ preserves $\boldsymbol{S}_w(U_w)$. As a starting arc for the $(w+1)$st step of the Algorithm, we randomly choose a w-arc $\mathcal{K}_w$ of $\boldsymbol{S}_w(U_w)$ so that for each arc of $\boldsymbol{S}_w(U_w)$ the probability to be chosen is $\dfrac{1}{\#\boldsymbol{S}_w(U_w)}$. Thus, the set $\boldsymbol{S}_w(U_w)$ is considered as an *ensemble of random objects* with the uniform probability distribution.

Denote by $\mathcal{U}_w(\mathcal{K}_w)$ the set of points of $PG(2,q)$ that are not covered by the arc $\mathcal{K}_w$. By the definition,

$$\#\mathcal{U}_w(\mathcal{K}_w) = U_w.$$

Let the arc $\mathcal{K}_w$ consist of w points $A_1, A_2, \ldots, A_w$. Let $A_{w+1} \in \mathcal{U}_w(\mathcal{K}_w)$ be the point that will be included to the arc in the $(w+1)$st step. Denote by $\#\mathcal{U}_{w+1}(A_{w+1})$ the number of points that are not covered by the arc $\mathcal{K}_w \cup \{A_{w+1}\}$.

Remark 1. Below we introduce several point subsets depending on A_{w+1}, for which we use the notation of the type $\mathcal{M}_w(A_{w+1})$. In principle, any uncovered point may be added to $\mathcal{K}_w$. Therefore, in general, there exist U_w distinct subsets $\mathcal{M}_w(A_{w+1})$. When a particular point A_{w+1} is not relevant, one may use the short notation $\mathcal{M}_w$. The same concerns the quantities $\Delta_w(A_{w+1})$ and Δ_w introduced below.

A point A_{w+1} defines a bundle $\mathcal{B}(A_{w+1})$ of w tangents (unisecants) to $\mathcal{K}_w$, which is denoted by $\overline{A_1A_{w+1}}, \overline{A_2A_{w+1}}, \ldots, \overline{A_wA_{w+1}}$. In this bundle the ith line connects A_{w+1} with the arc point A_i. Except for $A_1, \ldots, A_w$, each point on the tangents is a *candidate* for being a newly covered point in the $(w+1)$st step. Denote by $\mathcal{C}_w(A_{w+1})$ the set of the candidates. By the definition,

$$\mathcal{C}_w(A_{w+1}) = \mathcal{B}(A_{w+1}) \setminus \mathcal{K}_w,$$
$$\#\mathcal{C}_w = w(q-1)+1.$$

We call A_{w+1} and $\mathcal{B}(A_{w+1}) \setminus \{\mathcal{K}_w \cup \{A_{w+1}\}\}$ the *head* and *basic part* of the bundle $\mathcal{B}(A_{w+1})$, respectively. For a given arc $\mathcal{K}_w$, in total there are $\#\mathcal{U}_w(\mathcal{K}_w)$ distinct bundles.

Let $\Delta_w(A_{w+1})$ be the number of newly covered points in the $(w+1)$st step, i.e.,

$$\Delta_w(A_{w+1}) = \#\mathcal{U}_w(\mathcal{K}_w) - \#\mathcal{U}_{w+1}(A_{w+1}) = \#\{\mathcal{C}_w(A_{w+1}) \cap \mathcal{U}_w(\mathcal{K}_w)\}. \tag{15}$$

In what follows, we consider continuous approximations of the discrete functions $\Delta_w(A_{w+1})$, $\#\mathcal{U}_w(\mathcal{K}_w)$, and $\#\mathcal{U}_{w+1}(A_{w+1})$, keeping the same notation.

2.2. Probabilities of Uncovering; the Number of Uncovered Points in Subsets of $PG(2,q)$

Let $n_w(D)$ be the number of arcs of $\boldsymbol{S}_w(U_w)$ that do not cover a point D of $PG(2,q)$. Each point $D \in PG(2,q)$ will be considered as a random object that is not covered by a randomly chosen w-arc $\mathcal{K}_w$ with some probability $p_w(D)$ defined as

$$p_w(D) = \frac{n_w(D)}{\#\boldsymbol{S}_w(U_w)}.$$

Lemma 1. *The value $n_w(D)$ is the same for all points $D \in PG(2,q)$.*

Proof. Let $\boldsymbol{K}_w(D) \subseteq \boldsymbol{S}_w(U_w)$ be the subset of w-arcs in $\boldsymbol{S}_w(U_w)$ that do not cover D. By the definition, $n_w(D) = \#\boldsymbol{K}_w(D)$. Let D_i and D_j be two distinct points of $PG(2,q)$. In the group $P\Gamma L(3,q)$, denote by $\Phi(D_i, D_j)$ the subset of collineations taking D_i to D_j. Clearly, $\Phi(D_i, D_j)$ embeds the subset $\boldsymbol{K}_w(D_i)$ in $\boldsymbol{K}_w(D_j)$. Therefore, $\#\boldsymbol{K}_w(D_i) \le \#\boldsymbol{K}_w(D_j)$. Vice versa, $\Phi(D_j, D_i)$ embeds $\boldsymbol{K}_w(D_j)$ in $\boldsymbol{K}_w(D_i)$, and we have $\#\boldsymbol{K}_w(D_j) \le \#\boldsymbol{K}_w(D_i)$. Thus, $\#\boldsymbol{K}_w(D_i) = \#\boldsymbol{K}_w(D_j)$, i.e., $n_w(D_i) = n_w(D_j)$. $\triangle$

Thus, $n_w(D)$ can be considered as n_w. This means that the *probability* $p_w(D)$ is *the same for all points* D; it may be considered as

$$p_w = \frac{n_w}{\#\boldsymbol{S}_w(U_w)}.$$

In turn, since the probability to be uncovered is independent of a point, we conclude that, for a w-arc $\mathcal{K}_w$ randomly chosen from $\boldsymbol{S}_w(U_w)$, the *fraction* $\#\mathcal{U}_w(\mathcal{K}_w)/(q^2+q+1)$ of uncovered points of $PG(2,q)$ *is equal to the probability* p_w that a point of $PG(2,q)$ is not covered. In other words,

$$p_w = \frac{\#\mathcal{U}_w(\mathcal{K}_w)}{q^2+q+1} = \frac{U_w}{q^2+q+1}. \tag{16}$$

Equality (16) can also be explained as follows. By Lemma 1, the multiset consisting of all points that are not covered by all arcs of $\boldsymbol{S}_w(U_w)$ has cardinality $n_w \# PG(2,q)$. This cardinality can also be written as $U_w \#\boldsymbol{S}_w(U_w)$. Thus, $n_w(q^2+q+1) = U_w \#\boldsymbol{S}_w(U_w)$, whence

$$\frac{n_w}{\#\boldsymbol{S}_w(U_w)} = \frac{U_w}{q^2+q+1}.$$

Let $s_w(h)$ be the number of ones in a sequence of h random and independent 1/0 trials each of which yields 1 with probability p_w. For the random variable $s_w(h)$ we have the *binomial* probability distribution [66]; the *expected value* of $s_w(h)$ is

$$\mathbf{E}[s_w(h)] = hp_w = h\frac{U_w}{q^2+q+1}. \tag{17}$$

One can also consider the *hypergeometric* probability distribution [66], which describes the probability of $s'_w(h)$ successes in h random and independent draws without replacement from a finite population of size q^2+q+1 containing exactly U_w successes. In this case, again the *expected value* of $s'_w(h)$ is

$$\mathbf{E}[s'_w(h)] = h\frac{U_w}{q^2+q+1}.$$

We are interested in the values $s_w(h)$ and $s'_w(h)$, since they are the number of uncovered points among h random points of $PG(2,q)$ if events of the type "a point is uncovered" are considered as independent.

Note also that the *average number* $U_w^{\text{aver}}(h)$ of uncovered points among h points of $PG(2,q)$ calculated over all $\binom{q^2+q+1}{h}$ combinations of h points is

$$U_w^{\text{aver}}(h) = \frac{\sum\limits_{i=1}^{h} i\binom{q^2+q+1-U_w}{h-i}\binom{U_w}{i}}{\binom{q^2+q+1}{h}} = \frac{U_w\sum\limits_{i=1}^{h}\binom{q^2+q+1-U_w}{h-i}\binom{U_w-1}{i-1}}{\binom{q^2+q+1}{h}}$$

$$= \frac{U_w\binom{q^2+q+1-1}{h-1}}{\binom{q^2+q+1}{h}} = h\frac{U_w}{q^2+q+1} = \mathbf{E}[s_w(h)].$$

2.3. Tangents to the Arc $\mathcal{K}_w$ and Uncovered Points

In this subsection we take into account that *all points that are not covered* by an arc *lie on tangents* to the arc.

There are $q+2-w$ tangents through every point of $\mathcal{K}_w$. The total number of the tangents is

$$T_w^{\Sigma} = w(q+2-w). \tag{18}$$

Let $\gamma_{w,j}$ be the number of uncovered points on the jth tangent $\mathcal{T}_j$, $j = 1,2,\ldots,T_w^{\Sigma}$. Every uncovered point lies on exactly w tangents; due to this *multiplicity*, on all tangents there are in total Γ_w^{Σ} uncovered points, where

$$\Gamma_w^{\Sigma} = \sum_{j=1}^{T_w^{\Sigma}} \gamma_{w,j} = wU_w. \tag{19}$$

A tangent $\mathcal{T}_j$ belongs to $\gamma_{w,j}$ bundles, since every uncovered point on $\mathcal{T}_j$ may be the head of a bundle. Moreover, $\mathcal{T}_j$ contributes $\gamma_{w,j}(\gamma_{w,j}-1)$ uncovered points to the basic parts of all the bundles; this is also a certain *multiplicity*.

On all the U_w bundles, *taking into account the multiplicity*, there are

$$\sum_{A_{w+1}} \Delta_w(A_{w+1}) = U_w + \sum_{j=1}^{T_w^{\Sigma}} \gamma_{w,j}(\gamma_{w,j}-1)$$

uncovered points, where U_w is the total numbers of all heads.

For an arc $\mathcal{K}_w$, denote by $\Delta_w^{\text{aver}}(\mathcal{K}_w)$ the average value of $\Delta_w(A_{w+1})$ over all $\#\mathcal{U}_w(\mathcal{K}_w)$ uncovered points A_{w+1}, i.e.,

$$\Delta_w^{\text{aver}}(\mathcal{K}_w) = \frac{\sum\limits_{A_{w+1}} \Delta_w(A_{w+1})}{\#\mathcal{U}_w(\mathcal{K}_w)} \geq 1, \tag{20}$$

where the inequality is obvious. By the above,

$$\Delta_w^{\text{aver}}(\mathcal{K}_w) = \frac{\sum\limits_{j=1}^{T_w^{\Sigma}} \gamma_{w,j}^2 - \sum\limits_{j=1}^{T_w^{\Sigma}} \gamma_{w,j}}{\#\mathcal{U}_w(\mathcal{K}_w)} + 1 = \frac{\sum\limits_{j=1}^{T_w^{\Sigma}} \gamma_{w,j}^2}{\#\mathcal{U}_w(\mathcal{K}_w)} - w + 1 \geq 1. \tag{21}$$

We denote a lower estimate for $\Delta_w^{\text{aver}}(\mathcal{K}_w)$ (see Lemma 2) as follows:

$$\begin{aligned} \Delta_w^{\text{low}}(\mathcal{K}_w) &= \max\left\{1, \frac{wU_w}{q+2-w} - w + 1\right\} \\ &= \begin{cases} \dfrac{wU_w}{q+2-w} - w + 1, & U_w > q+2-w, \\ 1, & U_w \leq q+2-w. \end{cases} \end{aligned} \tag{22}$$

Lemma 2. *We have the inequality*

$$\Delta_w^{\text{aver}}(\mathcal{K}_w) \geq \Delta_w^{\text{low}}(\mathcal{K}_w), \tag{23}$$

where the equality

$$\Delta_w^{\text{aver}}(\mathcal{K}_w) = \Delta_w^{\text{low}}(\mathcal{K}_w) = \frac{wU_w}{q+2-w} - w + 1$$

holds if and only if each tangent contains the same number of uncovered points.

Proof. By the Cauchy–Schwarz–Bunyakovsky inequality, we have

$$\left(\sum_{j=1}^{T_w^\Sigma} \gamma_{w,j}\right)^2 \le T_w^\Sigma \sum_{j=1}^{T_w^\Sigma} \gamma_{w,j}^2, \tag{24}$$

where equality holds if and only if all $\gamma_{w,j}$ coincide. Now, from (18) and (19) we have

$$\frac{wU_w}{q+2-w} \le \frac{\sum\limits_{j=1}^{T_w^\Sigma} \gamma_{w,j}^2}{U_w},$$

which together with (19)–(21) gives (23). △

Remark 2. Estimate (23) can be treated as follows. The average number of uncovered points on a tangent is

$$\frac{\Gamma_w^\Sigma}{T_w^\Sigma} = \frac{U_w}{q+2-w}.$$

A bundle contains w tangents having a common point, its head. This explains the term $-(w-1)$.

Throughout the paper we denote

$$b_w^{\text{aver}} = \frac{\Delta_w^{\text{aver}}(\mathcal{K}_w)}{\mathbf{E}[s_w(w(q-1)+1)]}, \qquad b_w^{\text{low}} = \frac{\Delta_w^{\text{low}}(\mathcal{K}_w)}{\mathbf{E}[s_w(w(q-1)+1)]}. \tag{25}$$

Lemma 3. *Let*

$$U_w \ge \frac{(q+2)(q+2-w)}{w-1}. \tag{26}$$

Then

$$\Delta_w^{\text{aver}}(\mathcal{K}_w) \ge \frac{wU_w}{q+2-w} - w + 1 \ge \mathbf{E}[s_w(w(q-1)+1)] = \frac{(w(q-1)+1)U_w}{q^2+q+1}. \tag{27}$$

Proof. By (17), (22), and (23), for $U_w > q+2-w$ we have

$$b_w^{\text{aver}} \ge b_w^{\text{low}} = \frac{w(q^2+q+1)}{(q+2-w)(w(q-1)+1)} - \frac{(w-1)(q^2+q+1)}{(w(q-1)+1)U_w}, \tag{28}$$

whence after simple transformations we obtain

$$b_w^{\text{low}} \ge 1 \quad \text{if} \quad U_w \ge \frac{(q+2)(q+2-w)}{w-1}. \quad \triangle$$

Lemma 4. *We have the inequality*

$$\Delta_w^{\text{aver}}(\mathcal{K}_w) \ge \mathbf{E}[s_w(w(q-1)+1)] \quad \textit{if} \quad U_w \le \frac{q+1}{w}. \tag{29}$$

Proof. By (17), we have $\mathbf{E}[s_w(w(q-1)+1)] < 1$ if $U_w \le \dfrac{q+1}{w}$. Then we use the inequality in (20). △

From Lemmas 2–4 we obtain the following result.

Corollary 1. (i) *Let*

$$U_w \ge \frac{(q+2)(q+2-w)}{w-1}.$$

Then for any arc $\mathcal{K}_w$ *of* $\boldsymbol{S}_w(U_w)$ *there exists an uncovered point* A_{w+1} *providing the following inequalities*:

$$\Delta_w(A_{w+1}) \geq \frac{wU_w}{q+2-w} - w + 1 \geq \mathbf{E}[s_w(w(q-1)+1)] = \frac{(w(q-1)+1)U_w}{q^2+q+1}. \tag{30}$$

(ii) *Let*

$$U_w \leq \frac{q+1}{w}.$$

Then for any arc $\mathcal{K}_w$ *of* $\boldsymbol{S}_w(U_w)$ *there exists an uncovered point* A_{w+1} *providing the following inequality*:

$$\Delta_w(A_{w+1}) \geq \mathbf{E}[s_w(w(q-1)+1)] = \frac{(w(q-1)+1)U_w}{q^2+q+1}. \tag{31}$$

Proof. By the definition of the average value (20), there is always an uncovered point A_{w+1} providing the inequality $\Delta_w(A_{w+1}) \geq \Delta_w^{\text{aver}}(\mathcal{K}_w)$. $\triangle$

Remark 3. The lower estimate (23), based on (24), is attained if every tangent contains the same number of uncovered points. But this holds in the first steps of the iterative process only. Then the differences $\gamma_{w,j}^2 - \gamma_{w,i}^2$ become nonzero. However, while the inequality

$$U_w \geq \frac{(q+2)(q+2-w)}{w-1}$$

holds, these differences are relatively small and estimate (23) works "well." As U_w decreases, the differences relatively increase, and the estimate becomes worse in the sense that actually $\Delta_w^{\text{aver}}(\mathcal{K}_w)$ is considerably greater than $\Delta_w^{\text{low}}(\mathcal{K}_w)$. Finally, in a short final interval of the iterative process where $U_w \leq \dfrac{q+1}{w}$ and $\mathbf{E}[s_w(w(q-1)+1)] < 1$, estimate (23) becomes reasonable again. Thus, in the range

$$\frac{(q+2)(q+2-w)}{w-1} > U_w > \frac{q+1}{w}$$

the lower estimate (23) does not reflect the real situation effectively. This leads to the necessity to formulate Conjecture 2 as a (plausible) hypothesis.

An illustration of equation (25), Remark 3, Lemma 3, and Corollary 1 is given in Fig. 4 (see Section 6 below).

Remark 4. To avoid any confusion, here we use the notation $\widetilde{p}_w$ and $\widetilde{\mathbf{E}}[s_w(w(q-1)+1)]$ instead of p_w and $\mathbf{E}[s_w(w(q-1)+1)]$, respectively.

Consider the union of tangents as a multiset $\mathcal{T}_w^{\cup} = \bigcup\limits_{j=1}^{T_w^{\Sigma}} \mathcal{T}_j$. An intersection point of b tangents appears b times in $\mathcal{T}_w^{\cup}$. Clearly,

$$\#\mathcal{T}_w^{\cup} = \sum_{j=1}^{T_w^{\Sigma}} \#\mathcal{T}_j = T_w^{\Sigma}(q+1) = w(q+1)(q+2-w).$$

Similarly to Lemma 1, one can show that for a point D the probability $\widetilde{p}_w(D)$ to be not covered by a randomly chosen arc $\mathcal{K}_w \subset \boldsymbol{S}_w(U_w)$ does not depend on the point D and may be considered as $\widetilde{p}_w$. This implies that the *fraction* $\Gamma_w^{\Sigma}/\#\mathcal{T}_w^{\cup}$ of uncovered points of $\mathcal{T}_w^{\cup}$ *is the probability* $\widetilde{p}_w$ of the event that a point of $\mathcal{T}_w^{\cup}$ is uncovered. In other words,

$$\widetilde{p}_w = \frac{\Gamma_w^{\Sigma}}{\#\mathcal{T}_w^{\cup}} = \frac{U_w}{(q+1)(q+2-w)}.$$

Taking into account (16), we have

$$p_w < \widetilde{p}_w, \tag{32}$$

$$\frac{\widetilde{p}_w}{p_w} = \frac{q^2+q+1}{(q+1)(q+2-w)} \sim \frac{q}{q-w}. \tag{33}$$

Thus, to improve the estimates obtained in this paper, one can use the probability $\widetilde{p}_w$ and the expected value

$$\widetilde{\mathbf{E}}[s_w(w(q-1)+1)] = (w(q-1)+1)\widetilde{p}_w = \frac{(w(q-1)+1)U_w}{(q+1)(q+2-w)} \tag{34}$$

instead of p_w and $\mathbf{E}[s_w(w(q-1)+1)]$, respectively. We do not do this for the sake of simplicity of presentation. However, relations (32) and (33) increase our confidence in Conjecture 2 and make the conjecture more founded. An illustration of the aforesaid is also shown in Fig. 4 (Section 6 below).

Note that $\dfrac{q}{q-w}$ is the order of magnitude of the first term (subtrahend) of b_w^{low} (see (28)).

3. BASIC INEQUALITY

Note that the set of candidates $\mathcal{C}_w(A_{w+1})$ for any point A_{w+1} is not a $(w(q-1)+1)$-set of random points for which events of the type "to be an uncovered point" are independent. Hence, in the general case, the expectation $\mathbf{E}[\Delta_w]$ is not equal to $\mathbf{E}[s_w(w(q-1)+1)] = U_w^{\mathrm{aver}}(w(q-1)+1)$. However, for growing q, the cardinality of the ensemble $\boldsymbol{S}_w(U_w)$ and the number of distinct bundles $\mathcal{B}(A_{w+1})$ are relatively large. Moreover, uncovered points lie on tangents to $\mathcal{K}_w$ only. Using this fact, we have shown in Remark 4 that actually the probability of the event that a point is not covered is greater than $\dfrac{U_w}{q^2+q+1}$. Thus, since the bundles $\mathcal{B}(A_{w+1})$ consist of tangents only, one should expect that

$$\mathbf{E}[\Delta_w] \approx \widetilde{\mathbf{E}}[s_w(w(q-1)+1)] \qquad \text{and} \qquad \mathbf{E}[\Delta_w] > \mathbf{E}[s_w(w(q-1)+1)] \tag{35}$$

(see Remark 8). Finally, the variance of the random variable Δ_w implies the existence of bundles $\mathcal{B}(A_{w+1})$ providing $\Delta_w(A_{w+1}) > \mathbf{E}[\Delta_w]$. Recall also Lemmas 3 and 4 and Corollary 1.

Taking into account all these arguments, the following conjecture seems to be reasonable and well founded.

Conjecture 2. *Let U_w, $\boldsymbol{S}_w(U_w)$, $\mathcal{U}_w(\mathcal{K}_w)$, $\Delta_w(A_{w+1})$, and $\mathbf{E}[s_w(v)]$ be defined as above. Let*

$$\frac{q+1}{w} < U_w < \frac{(q+2)(q+2-w)}{w-1}. \tag{36}$$

Then, for q large enough, in $PG(2,q)$ there exists a w-arc $\mathcal{K}_w \subset \boldsymbol{S}_w(U_w)$ such that one can find an uncovered point A_{w+1} providing the inequality

$$\Delta_w(A_{w+1}) \geq \mathbf{E}[s_w(w(q-1)+1)] = \frac{(w(q-1)+1)U_w}{q^2+q+1}. \tag{37}$$

Note that there are many random factors connected with relative positions and intersections of bisecants and tangents affecting the iterative process, especially for growing q. Therefore, as a rule, there exists a point A_{w+1} providing the inequality $\Delta_w(A_{w+1}) > \mathbf{E}[s_w(w(q-1)+1)]$, in particular, taking into account (35).

Thus, *Conjecture* 2 *is formulated with some "safety margin"* (see Remark 8).

The existence of points A_{w+1} providing $\Delta_w(A_{w+1}) > \mathbf{E}[s_w(w(q-1)+1)]$ is used by greedy algorithms to obtain complete arcs smaller than the bounds that follow from Conjecture 2 (see Section 6).

It should be noted that the range (36) covers less than half of the steps of the iterative process for constructing a complete arc (see Remark 6).

By Corollary 1 and Conjecture 2 (see equations (30), (31), and (37)), taking into account (15), we obtain

$$\begin{aligned}\#\mathcal{U}_{w+1} &= \#\mathcal{U}_w(\mathcal{K}_w) - \Delta_w \\ &\le \#\mathcal{U}_w(\mathcal{K}_w)\left(1 - \frac{w}{q+2+\dfrac{3}{q-1}}\right) \\ &< \#\mathcal{U}_w(\mathcal{K}_w)\Big(1 - \frac{w}{q^*}\Big), \end{aligned} \tag{38}$$

where

$$q^* = q + 3.$$

Clearly, $\#\mathcal{U}_1(\mathcal{K}_1) = q^2 + q$. Using (38) iteratively, we obtain

$$\#\mathcal{U}_{w+1} \le (q^2+q) f_q(w), \tag{39}$$

where

$$f_q(w) = \prod_{i=1}^{w}\left(1 - \frac{i}{q^*}\right). \tag{40}$$

Remark 5. The function $f_q(w)$ and its approximations (including the one by the Taylor series; see (45)) appear in distinct problems of probability theory, e.g., in the so-called *birthday problem* (or birthday paradox; see [66, Section II.3; 67–69] and references therein). Indeed, let a year contain q^* days, and let all birthdays occur with the same probability. Then $P^{\ne}_{q^*}(w+1) = f_q(w)$, where $P^{\ne}_{q^*}(w+1)$ is the probability that no two of $w+1$ randomly chosen people have the same birthday. Moreover, if birthdays occur with different probabilities, we have $P^{\ne}_{q^*}(w+1) < f_q(w)$; see [68].

The iterative process ends when $\#\mathcal{U}_{w+1} \le \xi$, where $\xi \ge 1$ is some constant chosen to improve the estimates. Then several (at most ξ) points are added to $\mathcal{K}_w$ to obtain a complete k-arc. The size k of the obtained complete arc is as follows:

$$w + 1 \le k \le w + 1 + \xi \quad \text{provided that} \quad \#\mathcal{U}_{w+1} \le \xi. \tag{41}$$

Theorem 2 (basic inequality). *Let $f_q(w)$ be as in* (40). *Under Conjecture* 2, *for the plane $PG(2,q)$ we have*

$$t_2(2,q) \le w + 1 + \xi, \tag{42}$$

where $\xi \ge 1$ is a constant, and w satisfies the "basic" inequality

$$f_q(w) \le \frac{\xi}{q^2+q}. \tag{43}$$

Proof. According to (39), to provide the inequality $\#\mathcal{U}_{w+1} \le \xi$, it suffices to find w such that $(q^2+q)f_q(w) \le \xi$. Now (42) follows from (41). △

4. SOLVING THE BASIC INEQUALITY

We find an upper bound on the smallest possible solution of inequality (43).

The Taylor series for $e^{-\alpha}$ is $e^{-\alpha} = 1 - \alpha + \dfrac{\alpha^2}{2} - \dfrac{\alpha^3}{6} + \ldots$, whence

$$1 - \alpha < e^{-\alpha} \quad \text{for} \quad \alpha \neq 0. \tag{44}$$

The following inequalities are used in analyzing the birthday problem [66–69]:

$$\prod_{i=1}^{w}\left(1 - \frac{i}{q^*}\right) < \left(1 - \frac{w+1}{2q^*}\right)^w < \prod_{i=1}^{w} e^{-i/q^*} = e^{-(w^2+w)/2q^*} < e^{-w^2/2q^*}. \tag{45}$$

Lemma 5. *The value*

$$w \geq \sqrt{2q^*}\sqrt{\ln\frac{q^2+q}{\xi}} + 1 \tag{46}$$

satisfies the basic inequality (43).

Proof. By (40) and (45), to provide (43) it suffices to find w such that

$$e^{-w^2/2q^*} \leq \frac{\xi}{q^2+q}.$$

Since w must be an integer, 1 is added in (46). △

Theorem 3. *Under Conjnecture* 2, *for the plane* $PG(2,q)$ *we have*

$$t_2(2,q) \leq \sqrt{2(q+3)}\sqrt{\ln\frac{q^2+q}{\xi}} + 2 + \xi, \quad \xi \geq 1, \tag{47}$$

where ξ *is an arbitrarily chosen constant.*

Proof. The assertion follows from (42) and (46). △

Now we choose ξ so as to obtain a relatively small value on the right-hand side of (47). For simplicity, we use the function

$$\varphi(\xi) = \sqrt{2q}\sqrt{\ln\frac{q^2}{\xi}} + \xi.$$

Its derivative is

$$\varphi'(\xi) = 1 - \frac{1}{\xi}\sqrt{\frac{q}{2\ln\dfrac{q^2}{\xi}}}.$$

One can easily check the following facts: $\varphi'(1) < 0$ if $q \geq 9$, $\varphi'(\xi)$ is an increasing function,

$$0 < \varphi'\left(\sqrt{\frac{q}{3\ln q}}\right) = 1 - \sqrt{\frac{3\ln q}{3\ln q + \ln\ln q + \ln 3}} < \varphi'(\sqrt{q}) = 1 - \sqrt{\frac{1}{3\ln q}},$$

and $\varphi'\left(\sqrt{\frac{q}{3\ln q}}\right)$ is close to zero for growing q. Thus, the choice of

$$\xi = \sqrt{\frac{q}{3\ln q}} \tag{48}$$

seems to be appropriate.

Theorem 4. *Under Conjecture* 2, *there are the following upper bounds on the smallest size* $t_2(2,q)$ *of a complete arc in* $PG(2,q)$:

(i) $$t_2(2,q) < \widehat{t}_2(2,q) = \sqrt{q}\sqrt{3\ln q + \ln\ln q + \ln 3} + \sqrt{\frac{q}{3\ln q}} + 3; \tag{49}$$

(ii) $$t_2(2,q) < 1.87\sqrt{q\ln q}. \tag{50}$$

Proof. (i) Note that $\ln(1+a) < a$ if $a > -1$. In (47), we take ξ as in (48). Then

$$t_2(2,q) \le \sqrt{2(q+3)}\sqrt{\ln\frac{(q^2+q)\sqrt{3\ln q}}{\sqrt{q}}} + 2 + \sqrt{\frac{q}{3\ln q}}$$
$$< \sqrt{2q+6}\sqrt{\frac{3}{2}\ln q + \frac{1}{q} + \frac{1}{2}\ln 3 + \frac{1}{2}\ln\ln q} + 2 + \sqrt{\frac{q}{3\ln q}} = \psi(q).$$

One can check that $\psi(q) < \widehat{t}_2(2,q)$ if $q \ge 31$.

(ii) Direct computations show that $\widehat{t}_2(2,q) < 1.87\sqrt{q\ln q}$ if $q \ge 116\,131$. For $q < 116\,131$ we have checked that the smallest known sizes of complete arcs $\overline{t}_2(2,q)$ given in [35] and obtained in the present paper are smaller than $1.87\sqrt{q\ln q}$ (for an illustration, see Fig. 3 in Section 6 below). △

Remark 6. Taking into account (3), (39), (45), and (49), we estimate the order of magnitude of the range

$$U_w \ge \frac{(q+2)(q+2-w)}{w-1} \sim \frac{q^2}{w} - q$$

with respect to the size of a complete arc. We put (see (39) and (45))

$$\frac{q^2}{w} \approx q^2 f_q(w) \approx q^2 e^{-w^2/2q},$$

whence $w \approx \sqrt{2q\ln w}$, $\ln w \approx \frac{1}{2}(\ln 2 + \ln q + \ln\ln w) \gtrsim \frac{1}{2}\ln q$, and $w \approx \sqrt{q\ln q}$. Finally,

$$\frac{w}{\widehat{t}_2(2,q)} \approx \frac{\sqrt{q\ln q}}{\sqrt{3q\ln q}} = \frac{1}{\sqrt{3}} \approx 58\%.$$

Thus, the range where we have a *rigorous proof* without any conjectures covers *more than half of steps of the iterative process* for the construction of a complete arc.

5. NONSTANDARD TYPES OF UPPER BOUNDS

We introduce the notation

$$\widehat{c}(q) = \frac{\ln(\widehat{t}_2(2,q)/\sqrt{q})}{\ln\ln q}, \tag{51}$$

$$\widehat{m}(q) = \sqrt{3 + \frac{\ln\ln q + \ln 3}{\ln q}} + \frac{1}{\sqrt{3}\ln q} + \frac{3}{\sqrt{q\ln q}}. \tag{52}$$

Corollary 2. *Under Conjecture* 2, *for* $PG(2,q)$ *we have the following statements*:

(i) *Let* $t_2(2,q) = \sqrt{q}\ln^{c(q)} q$. *Then* $c(q) < \widehat{c}(q)$;
(ii) *Let* $t_2(2,q) = d(q)\sqrt{q}\ln q$. *Then* $d(q) < \widehat{t}_2(2,q)/\sqrt{q}\ln q$;
(iii) *Let* $t_2(2,q) = m(q)\sqrt{q\ln q}$. *Then* $m(q) < \widehat{m}(q)$.

Proof. The statements follow from Theorem 4 and the definitions of the functions $c(q)$, $d(q)$, and $m(q)$; see (7) and (8). △

6. ILLUSTRATION OF THE EFFECTIVENESS OF THE NEW UPPER BOUNDS

In this section we compare the bounds of Sections 2–5 with the smallest known sizes $\overline{t}_2(2,q)$ of complete arcs in $PG(2,q)$ obtained in [19, 20, 35] and in the present paper via computer search in a wide region of q.

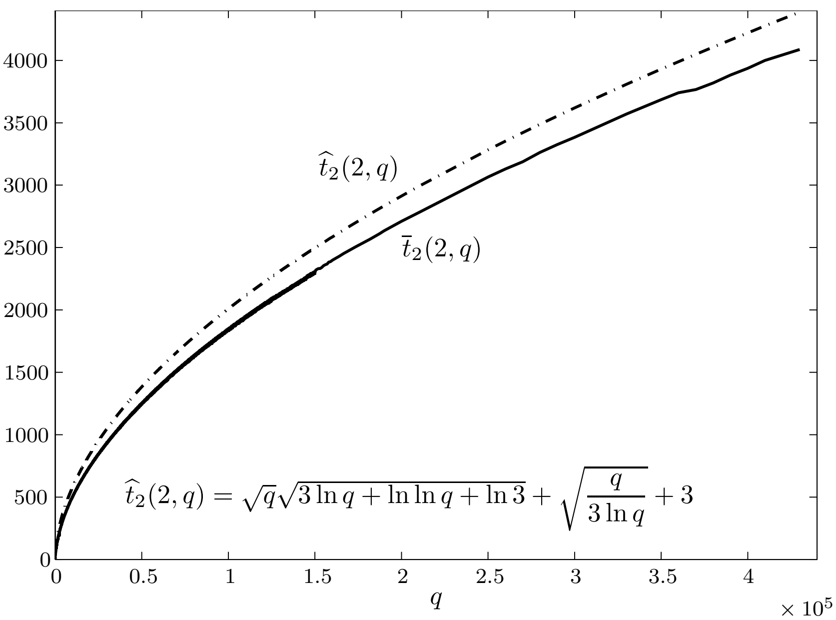

Fig. 1. Upper bound $\widehat{t}_2(2,q)$ on $t_2(2,q)$ (top dash-and-dot curve) and sizes $\overline{t}_2(2,q)$ of complete arcs obtained by greedy algorithms (bottom solid curve), $q \in Q$.

Let Q_1 be defined as in (5). Let Q_2 and Q be the following sets of values of q:

$$Q_2 = \{49\,729 \le q \le 151\,303,\ q = p^h,\ h \ge 2,\ p \text{ prime}\} \cup \{430\,007\}, \tag{53}$$

$$\begin{aligned} Q = Q_1 \cup Q_2 = \{&2 \le q \le 150\,001,\ q \text{ prime power}\} \\ &\cup \{41 \text{ sporadic prime } q \text{ in the interval } [150\,503 \ldots 430\,007]\}. \end{aligned} \tag{54}$$

For $q \in Q_1$, the smallest known values of $\overline{t}_2(2,q)$ are collected in [35]. For $q \in Q_2$, the values of $\overline{t}_2(2,q)$ are obtained in the present paper by computer search using randomized greedy algorithms similar to those from [19–22, 35, 37, 65].[3]

Recall that at each step a *randomized greedy algorithm* [19–22, 37] maximizes some objective function f, but some steps are executed in a random manner. Also, if one and the same maximum of f can be obtained in different ways, the choice is made at random. As the value of the objective function f, the number of points lying on bisecants of the obtained arc is considered.

One can begin to construct a complete arc using, for example, a starting arc $\mathcal{K}_1$ consisting of one point. On the $(w+1)$st step one takes all the points that are not covered by $\mathcal{K}_w$ and computes the objective function f temporarily adding each of these points to $\mathcal{K}_w$. The point providing the maximum of f is included in the arc $\mathcal{K}_w$ to obtain the next arc $\mathcal{K}_{w+1}$. For a fixed q, a randomized greedy algorithm is executed several times, which improves the results due to the randomization.

Remark 7. Since $t_2(2,q) \le \overline{t}_2(2,q)$, the values of $\overline{t}_2(2,q)$ are upper bounds themselves. But in this paper we are interested in analytical bounds. The sizes $\overline{t}_2(2,q)$, $q \in Q$, are used for illustration purposes only. An exception is the proof of Theorem 4 (ii) for $q < 116\,131$.

In Figs. 1–3, the upper bounds obtained in Sections 3–5 and the corresponding computer results are presented. For all figures, $q \in Q$. The notation (7), (51), and (52) is used. The quantity $\overline{c}(q)$ in Fig. 2 is defined by $\overline{t}_2(2,q) = \sqrt{q}\ln^{\overline{c}(q)} q$.

[3] The computer search for $q \in Q_2$ was performed using computational resources of the Multipurpose Computing Complex of the National Research Centre "Kurchatov Institute" (`http://computing.kiae.ru/`).

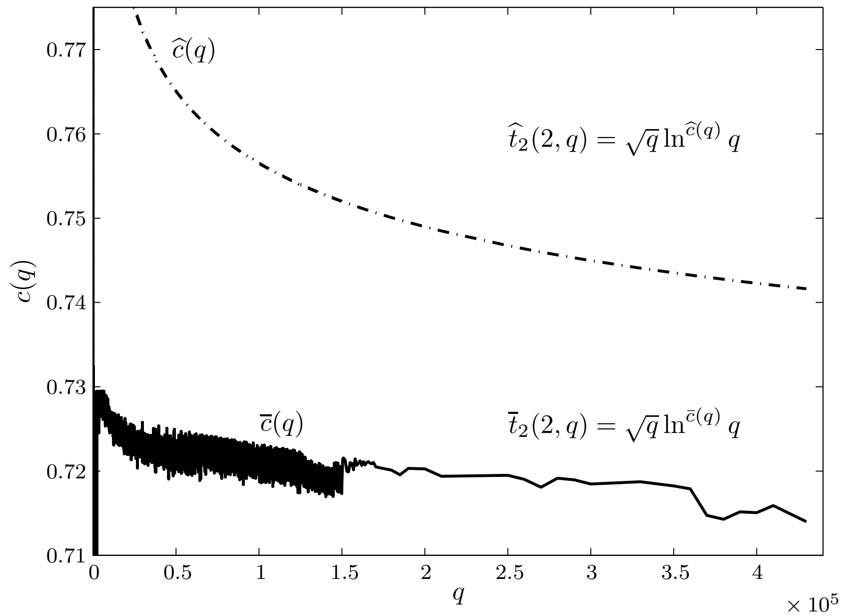

Fig. 2. Upper bound $\widehat{c}(q)$ on the decreasing function $c(q)$ (top dash-and-dot curve) and the value of $\overline{c}(q)$ for complete arcs obtained by greedy algorithms (bottom solid curve), $q \in Q$.

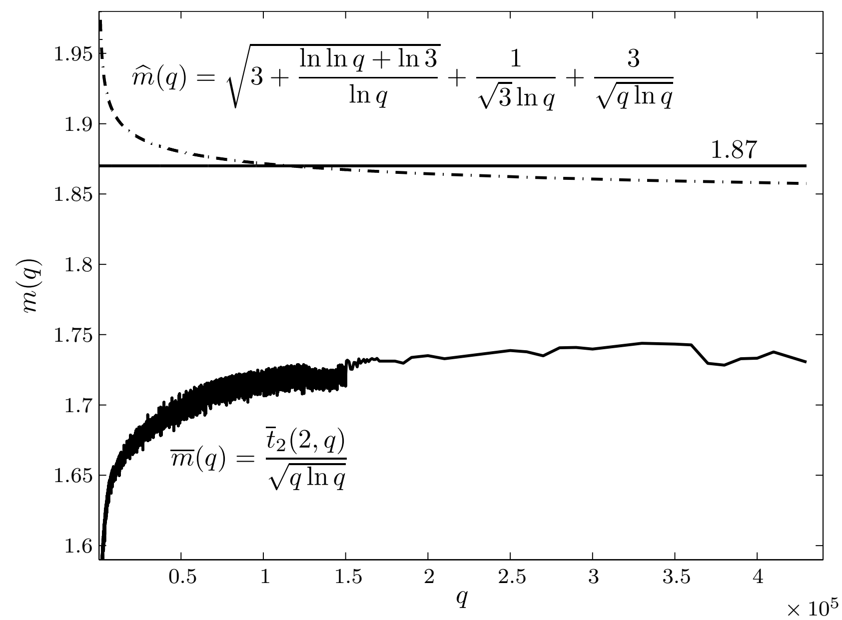

Fig. 3. New type of an upper bound based on the function $m(q)$: the bound $\widehat{m}(q)$ (top dash-and-dot curve), the quantity $\overline{m}(q) = \overline{t}_2(2,q)/\sqrt{q\ln q}$ for complete arcs obtained by greedy algorithms (bottom solid curve), and the bound (11) (the line $y = 1.87$), $q \in Q$.

Figures 1–3 illustrate the reasonableness of Conjecture 2 and effectiveness of the new upper bounds even for small values of q.

Remark 8. The value $\Delta_w^{\mathrm{aver}}(\mathcal{K}_w)$ defined in (20) was computed for many particular arcs $\mathcal{K}_w$. It is important to note that *for all the computations made* (including small q), we have

$$\Delta_w^{\mathrm{aver}}(\mathcal{K}_w) \approx \widetilde{\mathbf{E}}[s_w(w(q-1)+1)] \qquad \text{and} \qquad \Delta_w^{\mathrm{aver}}(\mathcal{K}_w) > \mathbf{E}[s_w(w(q-1)+1)] \tag{55}$$

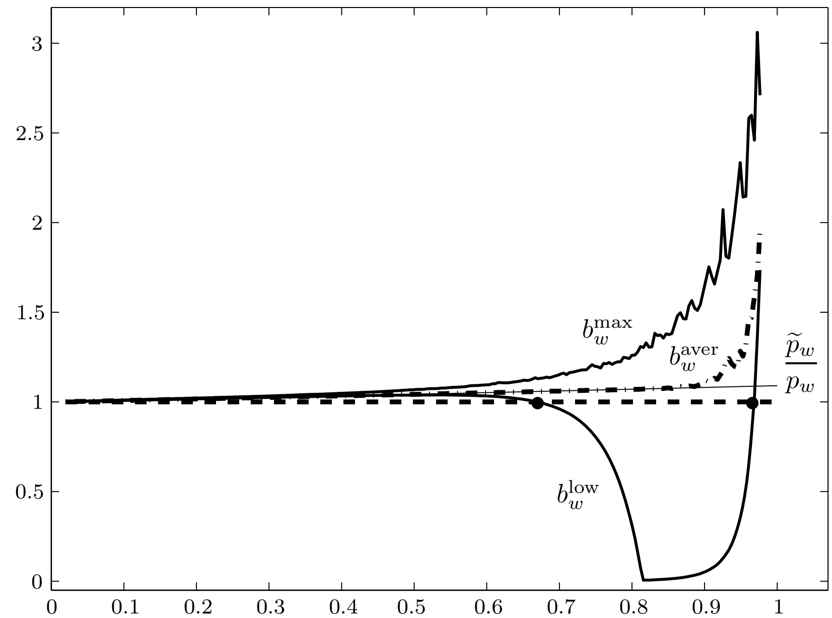

Fig. 4. Values of $b_w^{\bullet}$ for a complete k-arc in $PG(2,q)$, $k=255$, $q=3023$: $b_w^{\max}$ (top solid curve), b_w^{aver} (second dash-and-dot curve), $\dfrac{\widetilde{p}_w}{p_w}$ (solid line close to b_w^{aver}), b_w^{low} (bottom solid curve), dashed line $y=1$; the horizontal axis shows values of $\dfrac{w}{k}$.

(cf. (35)). From (55) it immediately follows that for the arc $\mathcal{K}_w$ there exists an uncovered point A_{w+1} providing

$$\Delta_w(A_{w+1}) > \mathbf{E}[s_w(w(q-1)+1)].$$

Let

$$b_w^{\max} = \frac{\max\limits_{A_{w+1}} \Delta_w(A_{w+1})}{\mathbf{E}[s_w(w(q-1)+1)]}.$$

An illustration of the aforesaid is shown in Fig. 4, where for a complete k-arc in $PG(2,q)$, $k=255$, $q=3023$, obtained by the greedy algorithm, the values $b_w^{\max}$, b_w^{aver}, b_w^{low}, and $\dfrac{\widetilde{p}_w}{p_w} \sim \dfrac{q}{q-w}$ (see (22), (25), and (33)) are presented. The curves $b_w^{\max}$ and b_w^{aver} are experimental, while b_w^{low} and $\dfrac{\widetilde{p}_w}{p_w}$ are computed by (22) and (33). The horizontal axis shows the values of $\dfrac{w}{k}$. The signs $\bullet$ mark intersections of the line $y=1$ and the curve b_w^{low}. The short final interval of the iterative process where $U_w \le \dfrac{q+1}{w}$ and $\mathbf{E}[s_w(w(q-1)+1)] < 1$ is not shown completely.

It is interesting (and expected) that, for almost all steps of the iterative process, the curve b_w^{aver} and the line $\dfrac{\widetilde{p}_w}{p_w}$ almost coincide. This means that in fact we have $\Delta_w^{\text{aver}}(\mathcal{K}_w) \approx \widetilde{\mathbf{E}}[s_w(w(q-1)+1)]$. This relation is stronger than Conjecture 2. Also, we have $b_w^{\max} > b_w^{\text{aver}}$; i.e., the variance of the random variable Δ_w helps to obtain good results.

Note that the forms of the curves $b_w^{\max}$ and b_w^{aver} are similar for all values of q for which the computation were made. The above-mentioned coincidence of the curve b_w^{aver} and the line $\dfrac{\widetilde{p}_w}{p_w}$ also takes place.

The computations noted in Remark 8, as well as Figs. 1–3, illustrate the reasonableness of Conjectures 2 and 1.

7. CONCLUSION

This paper is devoted to the classical combinatorial problem of upper bounds on the smallest size $t_2(2,q)$ of a complete arc in a projective plane $PG(2,q)$ over a finite field of order q. The problem was posed by the Italian mathematician B. Segre in 1950s; it is hard and still open.

There is a substantial gap between the known upper and lower bounds on $t_2(2,q)$ (see (2)–(4)). The gap is essentially reduced if one considers the lower bound (2) for complete arcs and the theoretical upper bound (1) from [18] for 1-saturating sets in $PG(2,q)$. However, though complete arcs are 1-saturating sets, they are a narrower class of objects. Therefore, for complete arcs, one cannot use the bound (1) directly. Nevertheless, the common nature of complete arcs and 1-saturating sets allows to hope for bounds on $t_2(2,q)$ similar to (1). The hope is confirmed by the experimental upper bound (6) from [35] obtained in a wide range of values of q.

In the present paper, we make an attempt to obtain a theoretical upper bound on $t_2(2,q)$ with the main term of the form $c\sqrt{q\ln q}$ (cf. (1)), where c is a small universal constant. The bound is based on explaining the mechanism of a step-by-step greedy algorithm for constructing complete arcs in $PG(2,q)$ and on quantitative estimations of the algorithm. For more than half of steps of the iterative process, these estimations are proved rigorously. We make a natural (and well-founded) conjecture that they hold for other steps too. We did not obtain a rigorous proof for precisely the part of the process where the variance of the random variable $\Delta(A_{w+1})$ determining the estimates implies the existence of points A_{w+1} which are considerably better than what is necessary for fulfillment of the conjecture (see the curve $b_w^{\max}$ in Fig. 4). This allows us to conclude about usefulness of further investigations in this direction.

The authors are grateful to L.A. Bassalygo and G.A. Kabatiansky for their profound and helpful advice and comments. The authors are grateful to participants of the Coding Theory seminar at the Kharkevich Institute for Information Transmission Problems of the Russian Academy of Sciences for valuable remarks.

REFERENCES

1. Hirschfeld, J.W.P., *Projective Geometries over Finite Fields*, Oxford: Clarendon; New York: Oxford Univ. Press, 1998, 2nd ed.

2. Segre, B., Le geometrie di Galois, *Ann. Mat. Pura Appl.*, 1959, vol. 48, no. 1, pp. 1–96.

3. Segre, B., Introduction to Galois Geometries, *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. I (8)*, 1967, vol. 8, no. 5, pp. 133–236.

4. Hirschfeld, J.W.P. and Storme, L., The Packing Problem in Statistics, Coding Theory and Finite Projective Spaces, *J. Statist. Plann. Inference*, 1998, vol. 72, no. 1–2, pp. 355–380.

5. Hirschfeld, J.W.P. and Storme, L., The Packing Problem in Statistics, Coding Theory, and Finite Projective Spaces: Update 2001, *Finite Geometries (Proc. 4th Isle of Thorns Conf., July 16–21, 2000)*, Blokhuis, A., Hirschfeld, J.W.P., Jungnickel, D., and Thas, J.A., Eds., Dev. Math., vol. 3, Dordrecht: Kluwer, 2001, pp. 201–246.

6. Landjev, I., Linear Codes over Finite Fields and Finite Projective Geometries, *Discrete Math.*, 2000, vol. 213, no. 1–3, pp. 211–244.

7. Szőnyi, T., Arcs, Caps, Codes and 3-independent Subsets, *Giornate di Geometrie Combinatorie (Proc. Int. Sci. Conf., Perugia, Italy, March 11–14, 1992)*, Faina, G. and Tallini, G., Eds., Perugia: Univ. di Perugia, 1993, pp. 57–80.

8. Thas, J.A., M.D.S. Codes and Arcs in Projective Spaces: A Survey, *Matematiche (Catania)*, 1992, vol. 47, no. 2, pp. 315–328.

9. Hartman, A. and Raskin, L., Problems and Algorithms for Covering Arrays, *Discrete Math.*, 2004, vol. 284, no. 1–3, pp. 149–156.

10. Keri, G., Types of Superregular Matrices and the Number of n-Arcs and Complete n-Arcs in $PG(r,q)$, *J. Combin. Des.*, 2006, vol. 14, no. 5, pp. 363–390.

11. Bartoli, D., Marcugini, S., and Pambianco, F., New Quantum Caps in $PG(4,4)$, *J. Combin. Des.*, 2012, vol. 20, no. 10, pp. 448–466.

12. Bartoli, D., Faina, G., Marcugini, S., and Pambianco, F., On the Minimum Size of Complete Arcs and Minimal Saturating Sets in Projective Planes, *J. Geom.*, 2013, vol. 104, no. 3, pp. 409–419.

13. Davydov, A.A., Giulietti, M., Marcugini, S., and Pambianco, F., Linear Nonbinary Covering Codes and Saturating Sets in Projective Spaces, *Adv. Math. Commun.*, 2011, vol. 5, no. 1, pp. 119–147.

14. Davydov, A.A., Marcugini, S., and Pambianco, F., On Saturating Sets in Projective Spaces, *J. Combin. Theory Ser. A*, 2003, vol. 103, no. 1, pp. 1–15.

15. Giulietti, M., The Geometry of Covering Codes: Small Complete Caps and Saturating Sets in Galois Spaces, *Surveys in Combinatorics 2013*, Blackburn, S.R., Holloway, R., and Wildon, M., Eds., London Math. Soc. Lecture Note Ser., vol. 409, Cambridge: Cambridge Univ. Press, 2013, pp. 51–90.

16. Pace, N., On Small Complete Arcs and Transitive A_5-Invariant Arcs in the Projective Plane $PG(2,q)$, *J. Combin. Des.*, 2014, vol. 22, no. 10, pp. 425–434.

17. Boros, E., Szőnyi, T., and Tichler, K., On Defining Sets for Projective Planes, *Discrete Math.*, 2005, vol. 303, no. 1–3, pp. 17–31.

18. Kovács, S.J., Small Saturated Sets in Finite Projective Planes, *Rend. Mat. Appl. (7)*, 1992, vol. 12, no. 1, pp. 157–164.

19. Bartoli, D., Davydov, A.A., Faina, G., Marcugini, S., and Pambianco, F., On Sizes of Complete Arcs in $PG(2,q)$, *Discrete Math.*, 2012, vol. 312, no. 3, pp. 680–698.

20. Bartoli, D., Davydov, A.A., Faina, G., Marcugini, S., and Pambianco, F., New Upper Bounds on the Smallest Size of a Complete Arc in a Finite Desarguesian Projective Plane, *J. Geom.*, 2013, vol. 104, no. 1, pp. 11–43.

21. Davydov, A.A., Faina, G., Marcugini, S., and Pambianco, F., Computer Search in Projective Planes for the Sizes of Complete Arcs, *J. Geom.*, 2005, vol. 82, no. 1–2, pp. 50–62.

22. Davydov, A.A., Faina, G., Marcugini, S., and Pambianco, F., On Sizes of Complete Caps in Projective Spaces $PG(n,q)$ and Arcs in Planes $PG(2,q)$, *J. Geom.*, 2009, vol. 94, no. 1–2, pp. 31–58.

23. Faina, G. and Pambianco, F., On the Spectrum of the Values k for Which a Complete k-Cap in $PG(n,q)$ Exists, *J. Geom.*, 1998, vol. 62, no. 1–2, pp. 84–98.

24. Kim, J.H. and Vu, V.H., Small Complete Arcs in Projective Planes, *Combinatorica*, 2003, vol. 23, no. 2, pp. 311–363.

25. Lombardo-Radice, L., Sul problema dei k-archi completi in $S_{2,q}$. ($q = p^t$, p primo dispari), *Boll. Un. Mat. Ital. (3)*, 1956, vol. 11, pp. 178–181.

26. Pellegrino, G., Un'osservazione sul problema dei k-archi completi in $S_{2,q}$, con $q \equiv 1 \pmod 4$ // Atti Accad. Naz. Lincei. Rend. Cl. Sci. Fis. Mat. Natur. (8), 1977, vol. 63, no. 1–2, pp. 33–44.

27. Pellegrino, G., Archi completi, contenenti $(q+1)/2$ punti di una conica, nei piani di Galois di ordine dispari, *Rend. Circ. Mat. Palermo (2)*, 1993, vol. 42, no. 2, pp. 273–308.

28. Szőnyi, T., Small Complete Arcs in Galois Planes, *Geom. Dedicata*, 1985, vol. 18, no. 2, pp. 161–172.

29. Szőnyi, T., Note on the Order of Magnitude of k for Complete k-Arcs in $PG(2,q)$, *Discrete Math.*, 1987, vol. 66, no. 3, pp. 279–282.

30. Szőnyi, T., Complete Arcs in Galois Planes: A Survey, *Quaderni del Sem. Geom. Comb.*, no. 94, Roma: Univ. Roma, 1989.

31. Szőnyi, T., Some Applications of Algebraic Curves in Finite Geometry and Combinatorics, *Surveys in Combinatorics 1997*, Bailey, R.A., Ed., London Math. Soc. Lecture Note Ser., vol. 241, Cambridge: Cambridge Univ. Press, 1997, pp. 198–236.

32. Abatangelo, V., A Class of Complete $[(q+8)/3]$-Arcs of $PG(2,q)$, with $q=2^h$ and $h\ (\geq 6)$ Even, *Ars Combin.*, 1983, vol. 16, pp. 103–111.

33. Ball, S., On Small Complete Arcs in a Finite Plane, *Discrete Math.*, 1997, vol. 174, no. 1–3, pp. 29–34.

34. Bartoli, D., Davydov, A., Faina, G., Kreshchuk, A., Marcugini, S., and Pambianco, F., Two Types of Upper Bounds on the Smallest Size of a Complete Arc in the Plane $PG(2,q)$, in *Proc. 7th Int. Workshop on Optimal Codes and Related Topics (OC'2013), Albena, Bulgaria, Sept. 6–12, 2013*, pp. 19–25.

35. Bartoli, D., Davydov, A.A., Faina, G., Kreshchuk, A.A., Marcugini, S., and Pambianco, F., Tables of Sizes of Small Complete Arcs in the Plane $PG(2,q)$, $q \leq 410009$, `arXiv:1312.2155v2 [math.CO]`, 2014.

36. Bartoli, D., Davydov, A.A., Faina, G., Kreshchuk, A.A., Marcugini, S., and Pambianco, F., Conjectural Upper Bounds on the Smallest Size of a Complete Arc in $PG(2,q)$ Based on an Analysis of Step-by-Step Greedy Algorithms, in *Proc. 14th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2014), Svetlogorsk, Russia, Sept. 7–13, 2014*, pp. 24–31.

37. Bartoli, D., Davydov, A.A., Faina, G., Marcugini, S., and Pambianco, F., New Types of Estimates for the Smallest Size of Complete Arcs in a Finite Desarguesian Projective Plane, *J. Geom.*, to appear. Available at `http://link.springer.com/article/10.1007/s00022-014-0224-4`.

38. Bartoli, D., Davydov, A.A., Marcugini, S., and Pambianco, F., New Type of Estimations for the Smallest Size of Complete Arcs in $PG(2,q)$, in *Proc. 13th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2012), Pomorie, Bulgaria, June 15–21, 2012*, pp. 67–72.

39. Bartoli, D., Faina, G., Marcugini, S., Pambianco, F., and Davydov, A.A., A New Algorithm and a New Type of Estimate for the Smallest Size of Complete Arcs in $PG(2,q)$, *Electron. Notes Discrete Math.*, 2013, vol. 40, pp. 27–31.

40. Blokhuis, A., Blocking Sets in Desarguesian Planes, *Combinatorics, Paul Erdős is Eighty*, vol. 2, Miklós, D., Sós, V.T., and Szónyi, T., Eds., Bolyai Soc. Math. Stud., vol. 2, Budapest: János Bolyai Math. Soc., 1996, pp. 133–155.

41. Davydov, A.A., Giulietti, M., Marcugini, S., and Pambianco, F., On Sharply Transitive Sets in $PG(2,q)$, *Innov. Incidence Geom.*, 2007/08, vol. 6/7, pp. 139–151.

42. Davydov, A.A., Giulietti, M., Marcugini, S., and Pambianco, F., New Inductive Constructions of Complete Caps in $PG(N,q)$, q Even, *J. Combin. Des.*, 2010, vol. 18, no. 3, pp. 176–201.

43. Faina, G. and Giulietti, M., On Small Dense Arcs in Galois Planes of Square Order, *Discrete Math.*, 2003, vol. 267, no. 1–3, pp. 113–125.

44. Faina, G., Marcugini, S., Milani, A., and Pambianco, F., The Spectrum of the Values k for Which There Exists a Complete k-Arc in $PG(2,q)$ for $q \leq 23$, *Ars Combin.*, 1997, vol. 47, pp. 3–11.

45. Faina, G. and Pambianco, F., On Some 10-Arcs for Deriving the Minimum Order for Complete Arcs in Small Projective Planes, *Discrete Math.*, 1999, vol. 208/209, pp. 261–271.

46. Gács, A. and Szőnyi, T., Random Constructions and Density Results, *Des. Codes Cryptogr.*, 2008, vol. 47, no. 1–3, pp. 267–287.

47. Giulietti, M., Small Complete Caps in $PG(2,q)$ for q an Odd Square, *J. Geom.*, 2000, vol. 69, no. 1–2, pp. 110–116.

48. Giulietti, M., Small Complete Caps in Galois Affine Spaces, *J. Algebraic Combin.*, 2007, vol. 25, no. 2, pp. 149–168.

49. Giulietti, M., Small Complete Caps in $PG(N,q)$, q Even, *J. Combin. Des.*, 2007, vol. 15, no. 5, pp. 420–436.

50. Giulietti, M., Korchmáros, G., Marcugini, S., and Pambianco, F., Transitive A_6-Invariant k-Arcs in $PG(2,q)$, *Des. Codes Cryptogr.*, 2013, vol. 68, no. 1–3, pp. 73–79.

51. Giulietti, M., and Ughi, E., A Small Complete Arc in $PG(2,q)$, $q=p^2$, $p \equiv 3 \pmod 4$, *Discrete Math.*, 1999, vol. 208/209, pp. 311–318.

52. Gordon, C.E., Orbits of Arcs in $PG(N,K)$ under Projectivities, *Geom. Dedicata*, 1992, vol. 42, no. 2, pp. 187–203.

53. Hadnagy, É., Small Complete Arcs in $PG(2,p)$, *Finite Fields Appl.*, 1999, vol. 5, no. 1, pp. 1–12.

54. Korchmáros, G., New Examples of Complete k-Arcs in $PG(2,q)$, *European J. Combin.*, 1983, vol. 4, no. 4, pp. 329–334.

55. Lisoněk, P., Marcugini, S., and Pambianco, F., Constructions of Small Complete Arcs with Prescribed Symmetry, *Contrib. Discrete Math.*, 2008, vol. 3, no. 1, pp. 14–19.

56. Marcugini, S., Milani, A., and Pambianco, F., Minimal Complete Arcs in $PG(2,q)$, $q \le 29$, *J. Combin. Math. Combin. Comput.*, 2003, vol. 47, pp. 19–29.

57. Marcugini, S., Milani, A., and Pambianco, F., Complete Arcs in $PG(2,25)$: The Spectrum of the Sizes and the Classification of the Smallest Complete Arcs, *Discrete Math.*, 2007, vol. 307, no. 6, pp. 739–747.

58. Östergård, P.R.J., Computer Search for Small Complete Caps, *J. Geom.*, 2000, vol. 69, no. 1–2, pp. 172–179.

59. Polverino, O., Small Minimal Blocking Sets and Complete k-Arcs in $PG(2,p^3)$, *Discrete Math.*, 1999, vol. 208/209, pp. 469–476.

60. Szőnyi, T., Arcs in Cubic Curves and 3-Independent Subsets of Abelian Groups, *Combinatorics (Proc. 7th Hungarian Colloq., Eger, Hungary, July 5–10, 1987)*, Hajnal, A., Lovász, L., and Sós, V.T., Eds., Colloq. Math. Soc. János Bolyai, vol. 52, Amsterdam: North-Holland, 1988, pp. 499–508.

61. Ughi, E., The Values $\sqrt{2q}$ and $\log_2 q$: Their Relationship with k-Arcs, *Ars Combin.*, 2000, vol. 57, pp. 201–207.

62. Ughi, E., Small Almost Complete Arcs, *Discrete Math.*, 2002, vol. 255, no. 1–3, pp. 367–379.

63. Voloch, J.F., On the Completeness of Certain Plane Arcs, *European J. Combin.*, 1987, vol. 8, no. 4, pp. 453–456.

64. Voloch, J.F., On the Completeness of Certain Plane Arcs. II, *European J. Combin.*, 1990, vol. 11, no. 5, pp. 491–496.

65. Davydov, A.A., Marcugini, S., and Pambianco, F., Complete Caps in Projective Spaces $PG(n,q)$, *J. Geom.*, 2004, vol. 80, no. 1–2, pp. 23–30.

66. Feller, W., *An Introduction to Probability Theory and Its Applications*, New York: Wiley, 1970, vol. 1, 3rd ed. Translated under the title *Vvedenie v teoriyu veroyatnostei i ee prilozheniya*, Moscow: Mir, 1984, vol. 1, 2nd ed.

67. Brink, D., A (Probably) Exact Solution to the Birthday Problem, *Ramanujan J.*, 2012, vol. 28, no. 2, pp. 223–238.

68. Clevenson, M.L. and Watkins, W., Majorization and the Birthday Inequality, *Math. Mag.*, 1991, vol. 64, no. 3, pp. 183–188.

69. Sayrafiezadeh, M., The Birthday Problem Revisited, *Math. Mag.*, 1994, vol. 67, no. 3, pp. 220–223.