Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 67–72*

New type of estimate for the smallest size of complete arcs in $PG(2, q)$

Daniele Bartoli daniele.bartoli@dmi.unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia
Alexander A. Davydov adav@iitp.ru
Institute for Information Transmission Problems, Russian Academy of Sciences
Stefano Marcugini, Fernanda Pambianco
{gino,fernanda}@dmi.unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia

Abstract. We propose a new type of upper bound for the smallest size $t_2(2, q)$ of a complete arc in the projective plane $PG(2, q)$. The upper bound has the form $t_2(2, q) < \sqrt{q} \ln^{c(q)} q$, where $c(q)$ is a decreasing function of q. The case $c(q) < \alpha - \beta q$, where α, β are positive constants independent of q, is considered. It is shown that $t_2(2, q) < \sqrt{q} \ln^{(0.7715-3.2\times10^{-7}q)} q$ if $9311 \leq q \leq 42013, q \in R, q$ prime, where R is a set of 23 values in the region 42013...80021. Moreover, our results allow us to conjecture that this estimate holds for all $q \geq 9311$. An algorithm FOP using any *fixed order* of *points* in $PG(2, q)$ is proposed for constructing complete arcs. The algorithm is based on an intuitive postulate that $PG(2, q)$ contains a sufficient number of relatively small complete arcs. It is shown that the type of order on the points of $PG(2, q)$ is not relevant.

1 Introduction

Let $PG(2, q)$ be the projective plane over the Galois field $\mathbb{F}_q$. A k-arc is a set of k points no three of which are collinear. A k-arc is called complete if it is not contained in a $(k + 1)$-arc of $PG(2, q)$. For an introduction to projective geometries over finite fields, see [4]. In [5], the close relationship among the theory of k-arcs, coding theory and mathematical statistics is presented.

One of the main problems in the study of projective plane, which is also of interest in coding theory, is finding of the smallest size $t_2(2, q)$ of a complete arc in $PG(2, q)$. This is a hard open problem. Surveys and results on the sizes of plane complete arcs, methods of their construction and comprehension of the relating properties can be found, e.g. in [1, 4–7] and references therein. The exact values of $t_2(2, q)$ are known only for $q \leq 32$, see [7].

In this work we *improve the known upper bounds* on $t_2(2, q)$, in particular we propose a *new type of upper bounds* on $t_2(2, q)$.

Let $t(\mathcal{P}_q)$ be the size of the smallest complete arc in any (not necessarily Galois) projective plane $\mathcal{P}_q$ of order q. In [6], for *sufficiently large* q, the following result is proved by *probabilistic methods* (we give it in the form of [5]):

$$t(\mathcal{P}_q) \leq D\sqrt{q} \log^C q, \; C \leq 300, \tag{1}$$

where C and D are constants independent of q (i.e. so-called universal or absolute constants). The authors of [6] conjecture that the constant can be reduced to $C = 10$ but it has not proved.

In [1–3], for large ranges of q, the form of the bound of (1) is applied but the value of the constant C was essentially reduced to $C = 0.75$ [1, 2] and to $C = 0.73$ [3] whereas $D < 1$. In particular, the following results are obtained in [1–3] using randomized greedy algorithms:

$$t_2(2,q) < \sqrt{q}\ln^{0.75} q \quad \text{for } 23 \le q \le 5107 \text{ [1]}. \tag{2}$$

$$t_2(2,q) < \sqrt{q}\ln^{0.75} q \quad \text{for } 23 \le q \le 9109 \text{ [2]}. \tag{3}$$

$$t_2(2,q) < \sqrt{q}\ln^{0.73} q \quad \text{for } 109 \le q \le 10111 \text{ [3]}. \tag{4}$$

In this work we propose and use an algorithm FOP (*fixed order of points*).

Algorithm FOP. In $PG(2,q)$, all *points* are *fixed* in some *order*. A complete arc is built iteratively. On the every i-th step, to the arc $K^{(i-1)}$ obtained on the previous steps one adds the point that is the first by the order among points not lying on the bisecants of $K^{(i-1)}$.

Effectiveness of Algorithm FOP is based on the following intuitive postulates that we formulated by experience on our previous works, see e.g. [1–3].

• **B1.** In $PG(2,q)$, there are relatively many complete k-arcs with size of order $k \approx \sqrt{q}\ln q$.

• **B2.** In $PG(2,q)$, a complete k-arc, chosen in arbitrary way that is close to the random way, has the size of order $k \approx \sqrt{q}\ln q$ with high probability.

• **B3.** The sizes of complete arcs obtained by Algorithm FOP vary insignificantly with the respect to the order of points.

Using Algorithm FOP we proved Theorem 1 where $R = \{43003, 44017, 45007, 46021, 47017, 48017, 49009, 50021, 51001, 52009, 53003, 54001, 55001, 56003, 57037, 58013, 59009, 60013, 69997, 70001, 79999, 80021\}$.

Theorem 1. *Let $c(q)$ be a decreasing function of q. Let α and β be absolute positive constants independent of q. Then it holds that*

$$t_2(2,q) < \sqrt{q}\log^{c(q)} q, \ \ c(q) < \alpha - \beta q, \ \ \alpha = 0.7715, \ \ \beta = 3.2 \cdot 10^{-7}, \tag{5}$$

where $9311 \le q \le 42013$, $q \in R$, *q prime.*

Complete arcs with sizes satisfying (5) *can be obtained by Algorithm FOP with lexicographical orders of points represented in homogenous coordinates.*

Our results and observations allow us to formulate the following

Conjecture 2. *The upper bound* (5) *holds for all* $q \ge 9311$.

It should be noted that the comparison of results obtained using two orders of points (lexicographical and Singer, see Section 2, Figure 2) shows that no essential differences are present. We conjecture that in general there exists no particular order that can be used to obtain better results than the others in every q. Therefore every randomized order can be used and the results will not essentially be influenced by the choice.

2 Algorithm FOP. Lexicographical and Singer orders

Algorithm FOP. Suppose that the points of $PG(2,q)$ are ordered as $A_1, A_2, \dots, A_{q^2+q+1}$. Consider the empty set as root of the search and let $K^{(j)}$ be the partial solution obtained in the j-th step, as extension of the root. We put

$$K^{(0)} = \emptyset, \quad K^{(1)} = \{A_1\}, \quad K^{(2)} = \{A_1, A_2\}, \quad K^{(j+1)} = K^{(j)} \cup \{A_{m(j)}\},$$
$$m(j) = \min\{i \in [m(j-1), q^2+q+1] \mid \nexists P, Q \in K^{(j)} \ : \ A_i, P, Q \text{ are collinear}\},$$

i.e. $m(j)$ is the minimum index such that the corresponding point is not saturated by $K^{(j)}$. The process ends when a complete arc is obtained.

In our search we use two different orders, lexicographical and Singer.

Singer order. It is well known that $PG(2,q)$ has a cyclic Singer group of order q^2+q+1. The order associated to the Singer group is the following

$$A_1 = (1,0,0), \ A_{i+1} = T(A_i), \ T = \begin{pmatrix} 0 & 0 & c \\ 1 & 0 & b \\ 0 & 1 & a \end{pmatrix}, \ i = 1, 2, \dots, q^2+q,$$

where $x^3 - ax^2 - bx - c$ is the minimal polynomial of a primitive element of $\mathbb{F}_{q^3}$.

In the figures we use the following notations: $\bar{t}_2^L(2,q)$, $\bar{t}_2^S(2,q)$, $\bar{t}_2^G(2,q)$ represent the results obtained with lexicographical order, Singer order and greedy randomized algorithms (see [1–3]), respectively. The function $c_L(q)$ is defined as

$$\bar{t}_2^L(2,q) = \sqrt{q}\log^{c_L(q)} q. \tag{6}$$

The constants are as follows: $\alpha_1 = 0.7715$, $\alpha_2 = 0.755$, and $\beta = 3.2 \times 10^{-7}$.

Figure 1 shows the comparison between the results obtained with lexicographic order and the functions $\sqrt{q}\log^{0.8} q$, $\sqrt{q}\log^{0.75} q$, $\sqrt{q}\log^{0.5} q$, for $q \leq 42013$, q prime. In Figure 2, the comparison between the results obtained with lexicographical and Singer order for prime $q \leq 40009$ is given. Figure 3 shows the comparison between the results obtained with the randomized greedy algorithms presented in [3] and the algorithm with lexicographic order for prime $q \leq 10111$. In Figure 4, the function $c_L(q)$, see (6), for prime $q \leq 42013$ is given.

When q grows the difference in percentage between the results obtained with Algorithm FOP and the randomized greedy algorithms presented in [1–3] decreases, see Figure 3.

In Table 1, some values $t_2(2,q)$ for $q \in [42013, 80021]$ are given.

Figure 1. Results obtained with lexicographical order with $q \leq 42013$, q prime

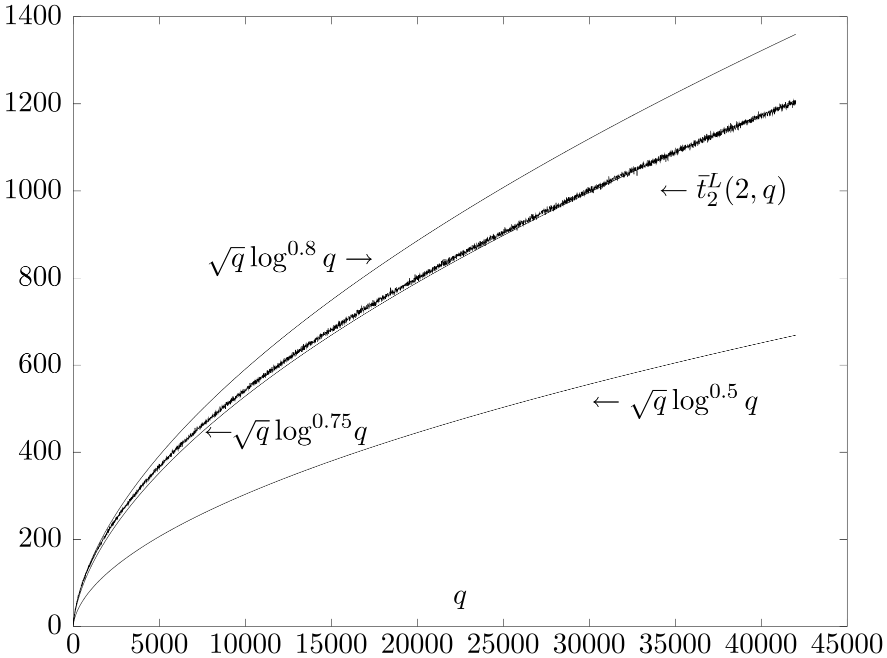

Figure 2. Difference in percentage between results obtained with lexicographical order and Singer order for $q \leq 42013$, q prime

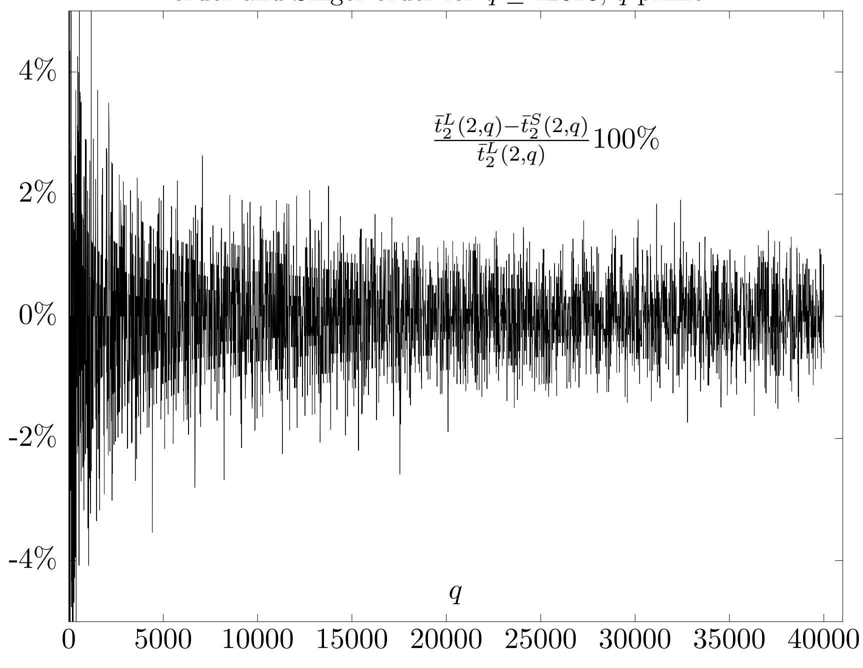

Figure 3. Difference in percentage between results obtained with lexicographical order and greedy algorithms for $q \le 10111$, q prime

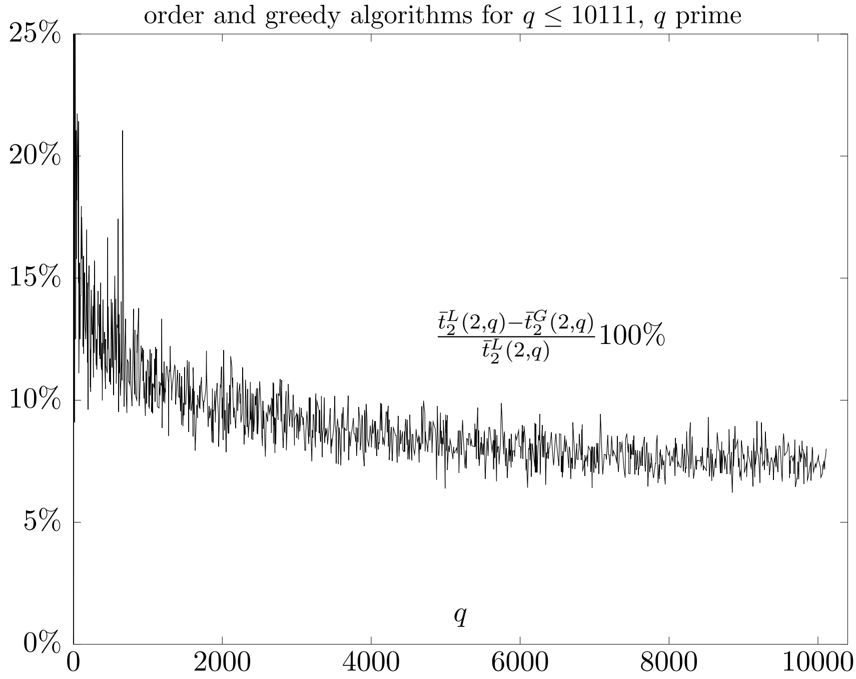

Figure 4. The function $c_L(q)$ for $q \le 42013$, q prime

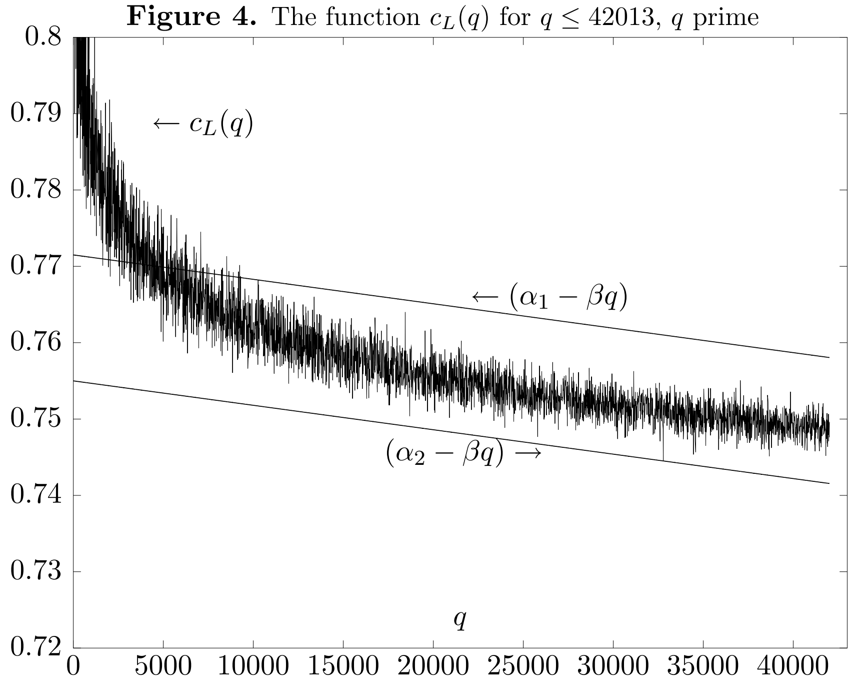

Table 1. Some values of $\bar{t}_2^L = \bar{t}_2^L(2, q)$ for $q \geq 42013$, q prime

q	$\bar{t}_2^L$	$\alpha_1 - \beta q$	$c_L(q)$	$\alpha_2 - \beta q$	q	$\bar{t}_2^L$	$\alpha_1 - \beta q$	$c_L(q)$	$\alpha_2 - \beta q$
42013	1207	0.7580	0.7496	0, 7415	43003	1218	0.7577	0.7478	0.7412
44017	1238	0.7574	0.7491	0.7409	45007	1250	0.7570	0.7478	0.7405
46021	1265	0.7567	0.7475	0.7402	47017	1291	0.7564	0.7509	0.7399
48017	1296	0.7561	0.7475	0.7396	49009	1316	0.7558	0.7490	0.7393
50021	1328	0.7554	0.7480	0.7389	51001	1339	0.7551	0.7468	0.7386
52009	1357	0.7548	0.7477	0.7383	53003	1364	0.7545	0.7454	0.7380
54001	1381	0.7542	0.7461	0.7377	55001	1403	0.7539	0.7484	0.7374
56003	1412	0.7535	0.7467	0.7370	57037	1430	0.7532	0.7477	0.7367
58013	1433	0.7529	0.7445	0.7364	59009	1448	0.7526	0.7449	0.7361
60013	1470	0.7522	0.7471	0.7357	69997	1595	0.7491	0.7448	0.7326
70001	1599	0.7491	0.7458	0.7326	79999	1707	0.7459	0.7416	0.7294
80021	1715	0.7458	0.7434	0.7293					

References

[1] D. Bartoli, A. A. Davydov, G. Faina, S. Marcugini, and F. Pambianco, On sizes of complete arcs in $PG(2, q)$, *Discrete Math.* **312** (2012), 680-698.

[2] D. Bartoli, A. A. Davydov, G. Faina, S. Marcugini, and F. Pambianco, Upper bounds on the smallest size of a complete arc in the plane $PG(2, q)$, http://arxiv.org/abs/1111.3403

[3] D. Bartoli, A. A. Davydov, G. Faina, S. Marcugini, and F. Pambianco, New upper bounds on the smallest size of a complete arc in the plane $PG(2, q)$, in *Proc. XIII Int. Workshop on Algebraic and Combin. Coding Theory, ACCT2012, Pomorie, Bulgaria, 2012*, to appear.

[4] J. W. P. Hirschfeld, *Projective geometries over finite fields,* 2nd ed., Clarendon Press, Oxford, 1998.

[5] J. W. P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces, *J. Statist. Planning Infer.* **72** (1998), 355–380.

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

[7] S. Marcugini, A. Milani, and F. Pambianco, Minimal complete arcs in $PG(2, q)$, $q \leq 32$, in *Proc. XII Int. Workshop on Algebraic and Combin. Coding Theory, ACCT2010, Novosibirsk, Russia, 2010,* 217–222.