Available online at www.sciencedirect.com

SciVerse ScienceDirect

Electronic Notes in Discrete Mathematics 40 (2013) 27–31

Electronic Notes in DISCRETE MATHEMATICS

www.elsevier.com/locate/endm

A new algorithm and a new type of estimate for the smallest size of complete arcs in $PG(2,q)$

Daniele Bartoli [1]
Giorgio Faina, Stefano Marcugini, Fernanda Pambianco [1]

Dipartimento di Matematica e Informatica
Università di Perugia
Perugia, Italy

Alexander A. Davydov [2]

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 [3]. We propose a new type of upper bound for the smallest size $t_2(2,q)$ of a complete arc in the projective plane $PG(2,q)$. We put $t_2(2,q) = d(q)\sqrt{q}\ln q$, where $d(q) < 1$ is a decreasing function of q. The case $d(q) < \alpha/\ln\beta q + \gamma$, where α, β, γ are positive constants independent of q, is considered. It is shown that

$$t_2(2,q) < (2/\ln \tfrac{1}{10}q + 0.32)\sqrt{q}\ln q \ \text{ if } \ q \leq 54881,\ q \text{ prime, or } q \in R,$$

where R is a set of 34 values in the region 55001...110017. Moreover, our results allow us to conjecture that this estimate holds for all q. 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.

Keywords: projective planes, complete arcs, small complete arcs

1571-0653/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.endm.2013.05.006

1 Introduction and main results

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 $PG(2,q)$. In [6], 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 planes, 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 related properties can be found, e.g. in [1,2,5,6,7,8] and references therein. The exact values of $t_2(2,q)$ are known only for $q \leq 32$, see [4,8].

In this work we *improve the known upper bounds* on $t_2(2,q)$, in particular we propose a *new type of upper bound* 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 [7], for *sufficiently large* q, the following result is proven by probabilistic methods (we give it in the form of [6]):

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

where C and D are constants independent of q. The authors of [7] conjecture that the constant can be reduced to $C = 10$ but it has not been proven.

In [1,2], for large ranges of q, the form of the bound of [7] is applied but the value of the constant C is reduced to 0.73 whereas $D < 1$. The following results are obtained in [1,2] using randomized greedy algorithms:

$$t_2(2,q) < \sqrt{q}\ln^{0.75} q \quad \text{for } 23 \leq q \leq 5107 \text{ [1]};$$
$$t_2(2,q) < \sqrt{q}\ln^{0.73} q \quad \text{for } 109 \leq q \leq 12007 \text{ [2]}.$$

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. Suppose that the points of $PG(2,q)$ are ordered as $A_1, A_2, \ldots, A_{q^2+q+1}$. Consider the empty set as a starting 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

$K^{(0)} = \emptyset,\ K^{(1)} = \{A_1\},\ K^{(2)} = \{A_1, A_2\},\ m(1) = 2,\ K^{(j+1)} = K^{(j)} \cup \{A_{m(j)}\},$

[1] Email: daniele.bartoli,faina,gino,fernanda@dmi.unipg.it
[2] Email: adav@iitp.ru

$m(j) = \min\{i \in [m(j-1)+1, q^2+q+1] \mid \nexists P, Q \in K^{(j)} : A_i, P, Q \text{ are collinear}\}$, i.e. $m(j)$ is the minimum subscript i such that the corresponding point A_i is not saturated by $K^{(j)}$. The process ends when a complete arc is obtained.

Effectiveness of Algorithm FOP is based on the following intuitive postulates that we formulated by experience on our previous works, see e.g. [1,2].

• **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 closed 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 respect to the order of points.

Let the points A_i of $PG(2,q)$ be represented in *homogenous coordinates* so that $A_i = (x_0^{(i)}, x_1^{(i)}, x_2^{(i)})$, $x_j^{(i)} \in \mathbb{F}_q$, where the leftmost non-zero element is 1.

Lexicographical order. For *q prime*, let the elements of the field $\mathbb{F}_q = \{0, 1, \ldots, q-1\}$ be treated as integers modulo q. For $A_i = (x_0^{(i)}, x_1^{(i)}, x_2^{(i)})$, we put $i = x_0^{(i)}q^2 + x_1^{(i)}q + x_2^{(i)}$.

Singer order. It is well known that $P\Gamma L(3,q)$ has a cyclic subgroup of order q^2+q+1, the Singer group. An order associated to the Singer group can be defined as follows: $A_1 = (1,0,0)$, $A_{i+1} = T(A_i)$, $T = \begin{pmatrix} 0 & 0 & c \\ 1 & 0 & b \\ 0 & 1 & a \end{pmatrix}$, $i = 1, 2, \ldots, q^2+q$, where $x^3 - ax^2 - bx - c$ is the minimal polynomial of a primitive element of $\mathbb{F}_{q^3}$.

Theorem 1.1 *Let $d(q) < 1$ be a decreasing function of q. Then it holds that*

$$t_2(2,q) = d(q)\sqrt{q}\ln q, \qquad d(q) < \frac{2}{\ln \frac{1}{10}q} + 0.32, \tag{1}$$

where $q \leq 54881$, *q prime, or* $q \in R = \{55001, 56003, 57037, 58013, 59009, 59999, 60013, 69997, 70001, 79999, 80021, 81001, 82003, 83003, 84011, 85009, 86011, 87011, 88001, 89003, 90001, 91009, 92003, 93001, 94007, 95003, 96001, 97001, 98009, 99013, 99989, 99991, 109987, 110017\}$.

Complete arcs with sizes satisfying (1) *can be obtained by Algorithm FOP with* Lexicographical order *of points represented in homogenous coordinates.*

Conjecture 1.2 *The upper bound* (1) *holds for all q.*

Observation. For prime $q \leq 42013$, the difference between the sizes of complete arcs obtained with Lexicographical order and Singer order is less then 2% and none of the two orders gives the smallest size for all q. It allows us to conjecture that, in general, there exists no particular order that can be used to obtain better results than the other ones for every q. Therefore **arbitrary fixed order** of **points** in $PG(2,q)$ can be used to obtain a bound and the results will not essentially be influenced by the choice.

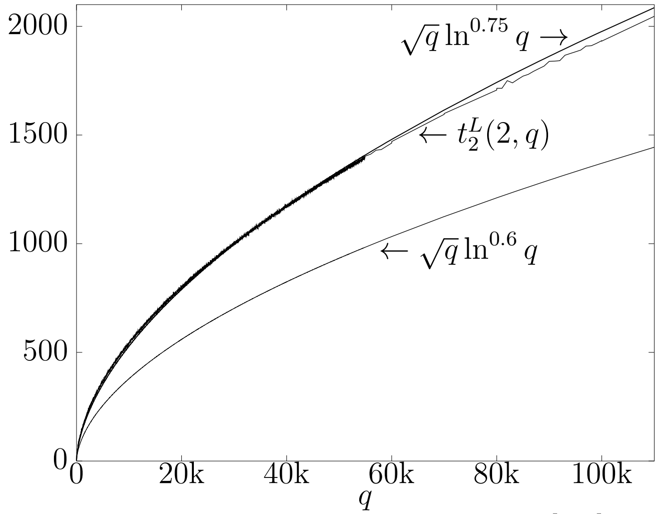
Let $t_2^L(2,q)$ be the size of a complete arc in $PG(2,q)$ obtained by Algorithm FOP with Lexicographical order. The functions $d(q)$ and $d_L(q)$ are defined as

$$d(q) = \frac{t_2(2,q)}{\sqrt{q}\ln q}; \qquad d_L(q) = \frac{t_2^L(2,q)}{\sqrt{q}\ln q}. \tag{2}$$

It is clear that $t_2(2,q) \leq t_2^L(2,q)$ and $d(q) \leq d_L(q)$.

For $q \leq 54881$, $q \in R$, q prime, functions $\sqrt{q}\ln^{0.75} q$ and $\sqrt{q}\ln^{0.6} q$ and sizes of $t_2^L(2,q)$, are showed on Figure 1.

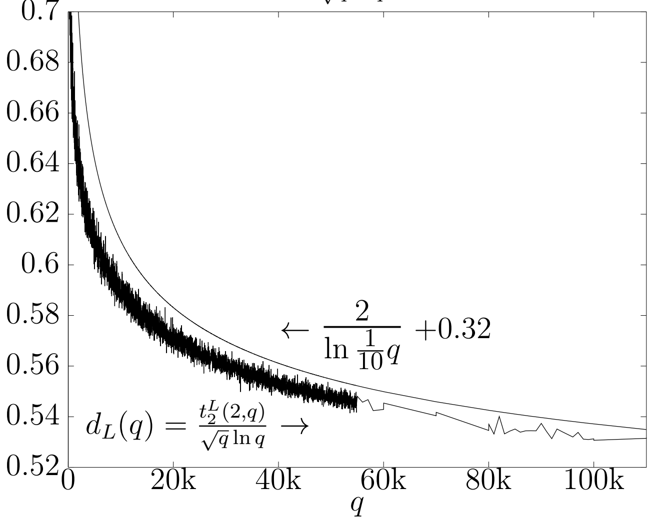
Figure 1. Sizes obtained with Lexicographical order for $q \leq 54881$, q prime, or $q \in R$



The randomized greedy algorithms presented in [1,2] give better results than Algorithm FOP, but when q grows the difference in percentage between the results obtained with Algorithm FOP and greedy algorithms decreases; for $q > 10000$ this difference is smaller than 8%.

In Figure 2, for prime $q \leq 54881$, $q \in R$, the function $d_L(q)$ of (2) is given.

Figure 2. The function $d_L(q) = \frac{t_2^L(2,q)}{\sqrt{q}\ln q}$ for $q \leq 54881$, q prime, or $q \in R$



References

[1] Bartoli, D., 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] Bartoli, D., A. A. Davydov, G. Faina, S. Marcugini and F. Pambianco, *New upper bounds on the smallest size of a complete arc in the plane $PG(2,q)$*, J. Geometry, DOI: 10.1007/s00022-013-0154-6

[3] Bartoli, D., A. A. Davydov, S. Marcugini and F. Pambianco, *New types of estimate for the smallest size of complete arcs in a finite Desarguesian projective plane*, preprint.

[4] D. Bartoli, S. Marcugini, A. Milani and F. Pambianco, *On the minimum size of complete arcs and minimal saturating sets in $PG(2,q)$, q small*, preprint.

[5] 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.

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

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

[8] Marcugini, S., 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.