Iranian Journal of Mathematical Sciences and Informatics
Vol. 17, No. 1 (2022), pp 125-133
DOI: 10.52547/ijmsi.17.1.125

New Large (n, r)-arcs in PG$(2, q)$

Rumen Daskalov

Department of Mathematics and Informatics,
Technical University of Gabrovo, Bulgaria

E-mail: daskalov@tugab.bg

Abstract. An (n, r)-arc is a set of n points of a projective plane such that some r, but no $r+1$ of them, are collinear. The maximum size of an (n, r)-arc in PG$(2, q)$ is denoted by $m_r(2, q)$. In this paper we present a new $(184, 12)$-arc in PG$(2, 17)$, a new $(244, 14)$-arc and a new $(267, 15)$-arc in PG$(2, 19)$.

Keywords: Finite projective plane, (n, r)-arc in a projective plane, (l, t)-blocking set in a projective plane, Maximum size of an (n, r)-arc, Linear codes.

2000 Mathematics subject classification: 51E21, 51E22, 94B05, 94B65.

1. Introduction

Let $GF(q)$ denote the Galois field of q elements and V$(3, q)$ be the vector space of row vectors of length three with entries in GF(q). Let PG$(2, q)$ be the corresponding projective plane. The *points* (x_1, x_2, x_3) of PG$(2, q)$ are the 1-dimensional subspaces of V$(3, q)$. Subspaces of dimension two are called *lines*. The number of points and the number of lines in PG$(2, q)$ is $q^2 + q + 1$. There are $q + 1$ points on every line and $q + 1$ lines through every point.

For both an intrinsic understanding of the plane PG$(2, \mathrm{q})$ and for applications, for example, in coding theory, it is essential to characterize certain subsets of the plane. Some of the essential subsets of the plane are arcs and blocking sets.

Received 11 July 2018; Accepted 27 April 2019

[DOI: 10.52547/ijmsi.17.1.125]

Definition 1.1. An (n, r)-arc is a set of n points of a projective plane such that some r, but no $r+1$ of them, are collinear.

Definition 1.2. An (l, t)-blocking set S in PG$(2, q)$ is a set of l points such that every line of PG$(2, q)$ intersects S in at least t points, and there is a line intersecting S in exactly t points.

An (n, r)-arc is the complement of a $(q^2 + q + 1 - n, q + 1 - r)$-blocking set in a projective plane and conversely.

Definition 1.3. Let M be a set of points in any plane. An i-secant is a line meeting M in exactly i points. Define τ_i as the number of i-secants to a set M.

In terms of τ_i the definitions of an (n, r)-arc and an (l, t)-blocking set become the following: An (n, r)-arc is a set of n points of a projective plane for which $\tau_i \geq 0$ for $i < r$, $\tau_r > 0$ and $\tau_i = 0$ when $i > r$. An (l, t)-blocking set is a set of l points of a projective plane for which $\tau_i = 0$ for $i < t$, $\tau_t > 0$ and $\tau_i \geq 0$ when $i > t$.

For an introduction to projective geometries over finite fields and further information on the geometrical properties of arcs and blocking sets, we refer to [21].

In 1947 Bose [7] proved that

$$m_2(2, q) = q + 1 \text{ for } q \text{ odd}$$
$$m_2(2, q) = q + 2 \text{ for } q \text{ even.}$$

From the results of Barlotti [5] and Ball [3] it follows that for q odd and

$$r = (q + 1)/2,\ r = (q + 3)/2$$
$$m_r(2, q) = (r - 1)q + 1.$$

So, when q is prime, the exact values of $m_r(2, q)$ are known only in three cases. For the rest of the cases the values of $m_r(2, q)$ are bounded by lower and upper bounds. The lower bounds come from different constructions and the upper bounds come from the following two theorems, proved by Ball and Daskalov respectively.

Theorem 1.4. [3] *Let K be an (n, r)-arc in* PG(2, q) *where q is prime.*

1. *If $r \leq (q + 1)/2$ then $m_r(2, q) \leq (r - 1)q + 1$.*

2. *If $r \geq (q + 3)/2$ then $m_r(2, q) \leq (r - 1)q + r - (q + 1)/2$.*

[DOI: 10.52547/ijmsi.17.1.125]

r\q	3	4	5	7	8	9
2	4	6	6	8	10	10
3		9	11	15	15	17
4			16	22	28	28
5				29	33	37
6				36	42	48
7					49	55
8						65

TABLE 1. Exact values of $m_r(2, q)$

Theorem 1.5. [11] *Let K be an (n, r)-arc in* PG(2, q) *with $r > (q+3)/2$ and $q \leq 29$ is prime. Then*

$$m_r(2, q) \leq (r-1)q + r - (q+3)/2.$$

A survey of (n, r)-arcs with the best known results was presented in [22]. After this publication many improvements were obtained in [10], [13] and [8]. Summarizing these improvements, Ball and Hirschfeld [4] presented a new table with bounds on $m_r(2, q)$ for $q \leq 19$. It follows from these tables that the exact values of $m_r(2, q)$ are known only for $q \leq 9$ (see Table 1). A survey of the new improvements in recent years can be found in the online table for $m_r(2, q)$, $q \leq 19$, maintained by S. Ball [1]. New results and tables with lower and upper bounds on $m_r(2, q)$ for $q = 23$, and $q = 25, 27$ are presented in [14] and [15] respectively.

2. About our approach

To obtain good (l, t)-blocking sets we apply local search techniques. The neighborhood structure is simple one. Given an blocking set, then its neighborhood consists of all blocking sets that can be obtained from the given blocking set by adding new points or deleting some points. The choice of a starting solution is based on some heuristic observations. The cost function is chosen to favor as local optima blocking sets with a small number of t-secants. The computation times are in order of several minutes up to a few hours on a PC. Similar techniques are employed for construction of (n, r)-arcs.

Since 2004 many new record-breaking (n, r)-arcs and (l, t)-blocking sets in PG$(2, q)$, $(13 \leq q \leq 31)$ have been constructed, applying this non-exhaustive local computer search (see [10, 12-19]).

In this paper we present a new version of our method for blocking sets that contain some lines. In the new version of our approach the choice of a starting solution is not based on heuristic observations.

[DOI: 10.52547/ijmsi.17.1.125]

	$q=11$	$q=13$	$q=17$	$q=19$
t	l	l	l	l
8				$9q+6$
7			$8q+5$	$8q+4$
6			$7q+5$	$7q+5$
5		$6q$	$6q$	$6q+2$
4	$5q$	$5q$	$5q+1$	$5q$
3	$4q$	$4q-1$	$4q$	$4q$
2	$3q$	$3q-1$	$3q$	$3q-1$

TABLE 2. The best known small (l,t)-blocking sets in PG$(2,q)$

In this article we say that an (n,r)-arc is large, if $r>(q+3)$, and an (l,t)-blocking set is small, if $t<(q-1)/2$. Constructing record-breaking large (n,r)-arcs is a hard problem and computationally it makes more sense to construct their corresponding small (l,t)-blocking sets. We can divide (l,t)-blocking sets into two types those that contain at least one line, and those that do not contain any lines. The following two theorems hold for (l,t)-blocking sets in PG$(2,q)$, q-prime:

Theorem 2.1. [2] *If an (l,t)-blocking set in* PG$(2,q)$*, q-prime, contains a (q+1)-secant, then* $l\geq(t+1)q$

Theorem 2.2. [11] *Let B be an (l,t)-blocking set in* PG$(2,q)$*,* $q<31$*, prime. If* $t<(q-1)/2$*, then* $l\geq(t+1)q+t-(q-3)/2$.

In Table 2 the parameters of the best known small (l,t)-blocking sets in finite projective planes of prime order at most 19 are presented. From these table we can see that 10 of the best known small (l,t)-blocking sets are $((t+1)q,t)$-blocking sets and they cannot be improved by using lines in PG$(2,q)$. Seven of the remaining ones have worse parameters and only 3 examples with better parameters are known. These are a $(4q-1,3)$-blocking set and a $(3q-1,2)$-blocking set in PG(2,13), and a $(3q-1,2)$-blocking set in PG(2,19)(see [1] and [6] for the secant distributions).

Theorem 2 shows that for $2\leq t<(q-1)/2$ the cardinality of blocking sets satisfying Theorem 1 can be improved by $t-(q+3)/2$, but in practice it has proved difficult to improve their cardinality even by one.

Our approach to construct good blocking sets of the first type is based on the following strategy:

1. We generate a large number (hundreds of thousands) of combinations of $(t+1)$ lines in general position and for each combination we compute the secant distribution of the resulting blocking set.
2. We divide the generated blocking sets into as many groups as distinct secant

[DOI: 10.52547/ijmsi.17.1.125]

distributions.
3. We try to extend the blocking sets in each group to new record-breaking ones by adding and removing points of PG$(2,q)$.
4. The process in 3 gets optimized by choosing at each step the blocking set that has the smallest number of shortest secants.

In the next example we will show how starting from blocking sets consisting of 9 lines in general position, we manage to improve the parameters of the best-known (141,7)-blocking set in PG(2,17), constructed in [8].
1. We generate a large number of combinations of 9 lines. Any combination of 9 lines in general position has 126 points.
2. For each combination we generate the respective $(126,t)$-blocking set.
3. Thus, we obtain 8 different groups of (126,5)-blocking sets, whose secant distributions are:

$$\begin{gathered}
\tau_5=2,\tau_6=76,\tau_7=138,\tau_8=64,\tau_9=18,\tau_{18}=9,\\
\tau_5=2,\tau_6=71,\tau_7=135,\tau_8=67,\tau_9=17,\tau_{18}=9,\\
\tau_5=3,\tau_6=72,\tau_7=144,\tau_8=60,\tau_9=19,\tau_{18}=9,\\
\tau_5=3,\tau_6=73,\tau_7=141,\tau_8=63,\tau_9=18,\tau_{18}=9,\\
\tau_5=4,\tau_6=71,\tau_7=141,\tau_8=65,\tau_9=17,\tau_{18}=9,\\
\tau_5=4,\tau_6=72,\tau_7=138,\tau_8=68,\tau_9=16,\tau_{18}=9,\\
\tau_5=5,\tau_6=69,\tau_7=141,\tau_8=67,\tau_9=16,\tau_{18}=9,\\
\tau_5=7,\tau_6=61,\tau_7=153,\tau_8=59,\tau_9=18,\tau_{18}=9.
\end{gathered}$$

4. We choose a representative blocking set with $\tau_5=2$ and begin a process of extending it by adding points.
5. By adding 14 points to it, we obtain a (143,7)-blocking set B_1.
6. From B_1 we remove 7 points to get a (136, 7)-blocking set B_2 with $\tau_7=18$.
7. We add 6 new points to B_2 to produce a (142, 7)-blocking set B_3.
8. We then remove 5 points from B_3 to obtain a (137,7)-blocking set B_4 with $\tau_7=13$.
9. After a few more rounds of adding and removing points we reach the best-known (141,7)-blocking set.
10. All our attempts to improve this result have so far failed.

It follows from [1] that $m_{12}(2,17)\geq 183$, $m_{14}(2,19)\geq 243$ and $m_{15}(2,19)\geq 265$. In this paper we prove that $m_{12}(2,17)\geq 184$, $m_{14}(2,19)\geq 244$ and $m_{15}(2,19)\geq 267$.

3. A new arcs in PG$(2,17)$ and PG$(2,19)$

Theorem 3.1. *There exists a* $(184,12)$*-arc in* PG(2,17).

[DOI: 10.52547/ijmsi.17.1.125]

Proof: The set of points lying on the next seven lines in common position

$$l_1 : y + 9z = 0, \quad l_2 : x + y + 4z = 0, \quad l_3 : x + 2y + 14z = 0,$$
$$l_4 : x + 7y = 0, \quad l_5 : x + 13y + z = 0, \quad l_6 : x + 15y + 5z = 0,$$
$$l_7 : x + 16 = 0,$$

forms a (105,4)-blocking set with secant distribution:

$$\tau_4 = 3, \tau_5 = 96, \tau_6 = 135, \tau_7 = 66, \tau_{18} = 7.$$

By adding the next 18 additional points (0,1,7), (1,0,7), (1,2,3), (1,3,6), (1,3,9), (1,4,12), (1,4,16), (1,5,6), (1,5,14), (1,6,12), (1,8,8), (1,10,4), (1,10,12), (1,13,15), (1,14,13), (1,15,1), (1,16,9), (1,16,15) we obtain a new (123,6)-blocking set with secant distribution:

$$\tau_6 = 131, \tau_7 = 89, \tau_8 = 56, \tau_9 = 18, \tau_{10} = 4, \tau_{12} = 1, \tau_{17} = 1, \tau_{18} = 7.$$

The complement of this blocking set is a new $(184, 12)$-arc in PG$(2, 17)$.

Theorem 3.2. *There exist a* $(244, 14)$*-arc and a* $(267, 15)$*-arc in* PG(2,19).

1. The set of points lying on the next seven lines in common position

$$l_1 : y + 4z = 0, \quad l_2 : x + 3y + 8z = 0, \quad l_3 : x + 4y + 4z = 0,$$
$$l_4 : x + 6y + 17z = 0, \quad l_5 : x + 7y + 18z = 0, \quad l_6 : x + 13y + 16z = 0,$$
$$l_7 : x + 15y + 14z = 0,$$

forms a (119,4)-blocking set with secant distribution:

$$\tau_4 = 1, \tau_5 = 102, \tau_6 = 171, \tau_7 = 100, \tau_{20} = 7.$$

By adding the next 18 points: (0,1,9), (0,1,11), (1,0,6), (1,3,8), (1,4,17), (1,5,7), (1,6,2), (1,6,16), (1,8,7), (1,11,0), (1,11,4), (1,12,13), (1,13,3), (1,14,12), (1,15,11), (1,16,11), (1,17,1), (1,18,10) we obtain a new (137,6)-blocking set with secant distribution:

$$\tau_6 = 157, \tau_7 = 115, \tau_8 = 82, \tau_9 = 14, \tau_{10} = 3, \tau_{11} = 2, \tau_{19} = 1, \tau_{20} = 7.$$

The complement of this blocking set is a new $(244, 14)$-arc in PG$(2, 19)$.

2. The set of points lying on the six lines in common position

$$l_1 : x + 5z = 0, \quad l_2 : +3y + 8z = 0, \quad l_3 : x + 7y + 2z = 0,$$
$$l_4 : x + 9y + 6z = 0, \quad l_5 : x + 14y + 5z = 0, \quad l_6 : x + 16y + 3z = 0,$$

forms a (105,3)-blocking set with secant distribution:

$$\tau_3 = 3, \tau_4 = 35, \tau_5 = 189, \tau_6 = 147, \tau_{20} = 6.$$

By adding the next 9 points (0,1,10), (1,2,13), (1,4,11), (1,6,1), (1,7,11), (1,8,3), (1,9,14), (1,12,9), (1,18,18) we obtain a new (114,5)-blocking set with secant distribution:

$$\tau_5 = 183, \tau_6 = 119, \tau_7 = 60, \tau_8 = 9, \tau_9 = 3, \tau_{12} = 1, \tau_{20} = 6.$$

[DOI: 10.52547/ijmsi.17.1.125]

	$q=11$	$q=13$	$q=17$	$q=19$
t	l	l	l	l
8				$9q+6$
7			$8q+5$	$8q+4$
6			$7q+4$	$7q+4$
5		$6q$	$6q$	$6q$
4	$5q$	$5q$	$5q+1$	$5q$
3	$4q$	$4q-1$	$4q$	$4q$
2	$3q$	$3q-1$	$3q$	$3q-1$

TABLE 3. The new best known small (l,t)-blocking sets in PG$(2,q)$

The complement of this blocking set is a new $(267,15)$-arc in PG$(2,19)$.

Remark: The new (114,5)-blocking set is a $(6q,5)$-blocking set and according to Theorem 2.1 this is a very good result.

In Table 3 the new best known small (l,t)-blocking sets in PG$(2,q)$ are given.

4. From arcs to codes

Let GF(q) denote the Galois field of q elements, and let V(n,q) denote the vector space of all ordered n-tuples over GF(q). The number of nonzero positions in a vector $\mathbf{x} \in \mathrm{V}(n,q)$ is called the *Hamming weight* wt$(\mathbf{x})$ of $\mathbf{x}$. The *Hamming distance* $d(\mathbf{x},\mathbf{y})$ between two vectors $\mathbf{x},\mathbf{y} \in \mathrm{V}(n,q)$ is defined by $d(\mathbf{x},\mathbf{y}) = \mathrm{wt}(\mathbf{x}-\mathbf{y})$.

A linear code C of length n and dimension k over GF(q) is a k-dimensional subspace of V(n,q).

The *minimum distance* of a linear code C is

$$d(C) = min\ \{d(\mathbf{x},\mathbf{y}) | \mathbf{x},\mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}.$$

Such a code is called an $[n,k,d]_q$ code if its minimum Hamming distance is d. For a linear code, the minimum distance is equal to the smallest of the weights of the nonzero codewords.

A central problem in coding theory is that of optimizing one of the parameters n,k and d for given values of the other two and q-fixed. The basic two versions are:

1. *Find $d_q(n,k)$, the largest value of d for which there exists an $[n,k,d]_q$ code.*

[DOI: 10.52547/ijmsi.17.1.125]

2. Find $n_q(k,d)$, the smallest value of n for which there exists an $[n,k,d]_q$ code.

A code which achieves one of these two values is called *optimal*.

The well-known lower bound for $n_q(k,d)$ is the Griesmer bound [9], [24]

$$n_q(k,d) \geq g_q(k,d) = \sum_{j=0}^{k-1} \lceil \frac{d}{q^j} \rceil$$

($\lceil x \rceil$denotes the smallest integer $\geq x$).

An $[n,k,d]_q$ code is a Griesmer code if $n = g_q(k,d)$. Note that $n_q(k,d) = g_q(k,d)$ for all d when $k = 1$ or 2 [20]. The problem of finding $n_q(k,d)$ for all d has been solved only in the next cases (see [23]): $k \leq 8$ for codes over GF(2), $k \leq 5$ for codes over GF(3), $k \leq 4$ for codes over GF(4), $k = 3$ for codes over GF(q), $5 \leq q \leq 9$. Thus, in the case of three-dimensional codes the problem remains open when $q \geq 11$.

It is well known that there exists a projective $[n,3,d]_q$ code if and only if there exists an $(n, n-d)$-arc in PG$(2,q)$ [20]. So the next corollary holds.

Corollary 4.1. *There exist* $[184,3,172]_{17}$, $[244,3,230]_{19}$, *and* $[267,3,252]_{19}$ *Griesmer codes.*

Acknowledgments

The authors would like to thank the referee for useful and helpful comments and suggestions.

References

1. S. Ball, Three-dimensional Linear Codes, Online table, `http://mat-web.upc.edu/people/simeon.michael.ball/codebounds.html`.
2. S. Ball, *On Sets of Points in Finite Planes*, PhD Thesis, University of Sussex, 1994.
3. S. Ball, Multiple Blocking Sets and Arcs in Finite Planes, *J. London Math. Soc.* **54**, (1996), 427-435.
4. S. Ball, J. W. P. Hirschfeld, Bounds on (n,r)-arcs and Their Applications to Linear Codes, *Finite Fields and Their Applications*, **11**, (2005), 326–336.
5. A. Barlotti, *Some Topics in Finite Geometrical Structures*, Institute of Statistics, University of Carollina, mimeo series, 1965, 439.
6. B. Csajbok, T. Heger, Double Blocking Sets of Size 3q-1 in PG(2,q), arXiv:1805.01267v1.
7. R. C. Bose, Mathematical Theory of the Symmetrical Factorial Design, *Sankyha*, 8, (1947), 107-166.
8. M. Braun, A. Kohnert, A. Wassermann, Construction of (n,r)-arcs in PG(2, q), *Innov. Incid. Geometry*, **1**, (2005), 133–141.

[DOI: 10.52547/ijmsi.17.1.125]

9. J. H. Griesmer, A Bound for Error-correcting Codes, *IBM J. Res. Develop.*, **4**, (1960), 532–542.
10. R. Daskalov, On the Existence and the Nonexistence of Some (k, r)-arcs in PG(2, 17), in Proc. of Ninth International Workshop on Algebraic and Combinatorial Coding Theory, 19-25 June 2004, Kranevo, Bulgaria, 2004, 95–100.
11. R. Daskalov, On the Maximum Size of Some (k, r)-arcs in PG(2, q), *Discrete Mathematics*, **308**(4), (2008), 565-570.
12. R. Daskalov, M. E. J. Contreras, New (k; r)-arcs in the Projective Plane of Order Thirteen, *Journal of Geometry*, **80**(12), (2004), 10-22.
13. R. Daskalov, E. Metodieva, New (k, r)-arcs in $PG(2, 17)$ and the Related Optimal Linear Codes, *Mathematica Balkanica*, New series, **18**, (2004), 121–127.
14. R. Daskalov, E. Metodieva, New (n,r)-arcs in PG(2, 17), PG(2, 19), and PG(2, 23), *Problemi Peredachi Informatsii*, **47**(3), (2011), 3–9. English translation: *Problems of Information Transmission*, **47**(3), (2011), 217–223.
15. R. Daskalov, E.Metodieva, Improved Bounds on $m_r(2, q)$ $q = 19{,}25, 27$, Hindawi Publishing Corporation, *Journal of Discrete Mathematics*, **2013**, Article ID 628952, 7 pages, http://dx.doi.org/10.1155/2013/628952.
16. R. Daskalov, E.Metodieva, New Good (n, r)-arcs in PG(2, 29), *in Proc. of Seventh International Workshop on Optimal Codes and Related Topics*, 6-12 September 2013, Albena, Bulgaria, (2013), 79–84.
17. R. Daskalov, E.Metodieva, Five New (n, r)-arcs in PG(2, 29), *in Proc. of Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory*, 7-13 September 2014, Svetlogorsk (Kaliningrad region), Russia, (2014), 127–132.
18. R. Daskalov, E.Metodieva, Improved Lower Bounds on $m_r(2, 29)$, *Electronic Notes in Discrete Mathematics*, **57**, (2017), 103-108.
19. R. Daskalov, E. Metodieva, Some New (n, r)-arcs in PG(2,31), *Electronic Notes in Discrete Mathematics*, **57**, (2017), 109-114.
20. R. Hill, Optimal Linear Codes, *Cryptography and Coding II*, Oxford University Press, 1992, 41-70.
21. J.W.P. Hirschfeld, *Projective Geometries Over Finite Fields*, Oxford Mathematical Monographs, 2nd Edition, 1998.
22. J. W. P. Hirschfeld, L. Storme, *The Packing Problem in Statistics*, coding theory and finite projective spaces: update 2001, Finite Geometries, Developments in Mathematics, Kluwer, Boston, 2001, 201–246.
23. T. Maruta, Griesmer Bound for Linear Codes Over Finite Fields. http://www.geocities.jp/mars39geo/ griesmer.htm
24. G. Solomon, J.J. Stiffler, Algebraically Punctured Cyclic Codes, *Inform. and Control*, **8**, (1965), 170–179.

[DOI: 10.52547/ijmsi.17.1.125]