Mathematica
Balkanica

New Series Vol. 18, 2004, Fasc. 1-2

New (k, r)-Arcs in $PG(2, 17)$ and the Related Optimal Linear Codes [1]

Rumen Daskalov, Elena Metodieva

A (k, r)-arc is a set of k points of a projective plane such that some r, but no $r+1$ of them, are collinear. The maximum size of a (k, r)-arc in $PG(2, q)$ is denoted by $m_r(2, q)$. In this paper we established that $m_3(2, 17) \geq 27$, $m_4(2, 17) \geq 41$ and $m_{14}(2, 17) \geq 221$.

AMS Subj. Classification : 51E21
Key words: projective plane, arcs in projective plane, optimal codes.

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 of $PG(2, q)$ are the non-zero vectors of $V(3, q)$ with the rule that $X = (x_1, x_2, x_3)$ and $Y = (\lambda x_1, \lambda x_2, \lambda x_3)$ are the same point, where $\lambda \in GF(q) \setminus \{0\}$. Since any non-zero vector has precisely $q-1$ non-zero scalar multiples, the number of points of $PG(2, q)$ is $\frac{q^3-1}{q-1} = q^2 + q + 1$.

If the point $P(X)$ is the equivalence class of the the vector X, then we will say that X is a vector *representing* $P(X)$. A subspace of dimension one is a set of points all of whose representing vectors form a subspace of dimension two of $V(3, q)$. Such subspaces are called *lines.* 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.

Definition 1.1 An $\{l, n\}$-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 n points, and there is a line intersecting S in exactly n points.

[1] This work was partially supported by the Ministry of Education and Science under contract in TU-Gabrovo.

Definition 1.2 A (k,r)-arc is a set of k points of a projective plane such that some r, but no $r+1$ of them, are collinear.

Definition 1.3 The maximum size of a (k,r)-arc in $PG(2,q)$ is denoted by $m_r(2,q)$.

Note that a (k,r)-arc is the complement of a $\{q^2+q+1-k, q+1-r\}$-blocking set in a projective plane and conversely.

Definition 1.4 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.

The τ_i satisfy the next three diophantine equations in any projective plane, which are known as the *standard equations* [9].

Lemma 1.5 *For any set of k points in $PG(2,q)$ the following hold:*

1. $$\sum_{i=0}^{q+1} \tau_i = q^2+q+1$$

2. $$\sum_{i=1}^{q+1} i\tau_i = k(q+1)$$

3. $$\sum_{i=2}^{q+1} i(i-1)\tau_i = k(k-1)$$

In 1947 Bose [4] proved that $m_2(2,q) = q+1$ for q odd, and $m_2(2,q) = q+2$ for q even. Barlotti [3] and also S. Ball [2] proved that $m_r(2,q) = (r-1)q+1$ for q odd prime and $r = (q+1)/2, r = (q+3)/2$.

A $(31,4)$-arc, a $(43,5)$-arc and a $(77,8)$-arc in $PG(2,11)$ were constructed in [1,2]. A $(89,9)$-arc and a $(100,10)$-arc in $PG(2,11)$ were both obtained by Hill and Mason in [7]. A $(131,11)$-arc and a $(144,12)$-arc in $PG(2,13)$ were both constructed also in [7]. A $(23,3)$-arc in $PG(2,13)$ was constructed in [1,2]. A $(35,4)$-arc, a $(48,5)$-arc, a $(63,6)$-arc and a $(117,10)$-arc in $PG(2,13)$ were constructed and the nonexistence of a $(40,4)$-arc was proved in [5].

For the other lower and upper bounds in Table I see [2,8].

Table I: The values of $m_r(2, q)$ (q-prime).

q	3	5	7	11	13
r					
2	4	6	8	12	14
3		11	15	21	23
4		16	22	31..34	35..40
5			29	43..45	48..53
6			36	56	63..66
7				67	79
8				77..78	92
9				89..90	105
10				100..102	117..119
11					131..133
12					144..147

In [1] the next theorem is proved:

Theorem 1.6 *Let K be a (k, 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 $m_r(2, q) \leq (r-1)q + r - (q+1)/2$.

From Theorem 1.6 the next corollary holds:

Corollary 1.7

$$m_3(2, 17) \leq 35, \quad m_4(2, 17) \leq 52, \quad m_{14}(2, 17) \leq 226.$$

In this paper we consider the case $q = 17$ and construct new arcs and blocking sets, using a combinatorial computers search. We will denote the elements of $GF(17)$ with $0, 1, 2, \ldots, 9, a, b, c, d, e, f, g$.

2. The new arcs in $PG(2, 17)$

In 1969 Waterhouse [10] proved that $m_3(2, q) \geq (\sqrt{q} + 1)^2$ using the theory of elliptic cubic curves. It follows from this result that $m_3(2, 17) \geq 26$. We improve this result in the next Theorem 2.1.

Theorem 2.1 *There exist a $(27, 3)$-arc and a $(41, 4)$-arc in $PG(2, 17)$. Therefore,*

$$27 \leq m_3(2, 17) \leq 35 \quad \textit{and} \quad 41 \leq m_4(2, 17) \leq 52.$$

P r o o f.

1. The set of points

$$\mathcal{K}_1 = \{ \begin{array}{llllll} (0,0,1), & (0,1,0), & (1,1,g), & (1,2,8), & (1,3,b), & (1,4,4), \\ (1,5,a), & (1,6,e), & (1,7,c), & (1,8,2), & (1,9,f), & (1,a,5), \\ (1,b,3), & (1,c,7), & (1,d,d), & (1,e,6), & (1,f,9), & (1,g,1). \end{array} \}$$

is a conic and forms a $(18,2)$-arc in $PG(2,17)$ with secant distribution

$$\tau_0 = 136, \quad \tau_1 = 18, \quad \tau_2 = 153.$$

The technique to construct a large $(k,3)$-arc will be to add to $\mathcal{K}_1$ some points lying on some of its 0-secants. Consider four of the 136 zero-secants to $\mathcal{K}_1$, namely

$$l_1 : x + y + 16z = 0, \qquad l_2 : x + 6y + 11z = 0,$$

$$l_3 : x + 16y + 8z = 0, \qquad l_4 : x + 16y + z = 0.$$

Adding the points $(0,1,1)$, $(1,0,1)$, $(1,a,b)$ lying on l_1, $(1,3,6)$, $(1,6,9)$ on l_2, $(1,0,2)$, $(1,1,0)$, $(1,2,f)$ on l_3 and $(1,d,c)$ on l_4 we obtain new $(27,3)$-arc $\mathcal{K}_2$ in $PG(2,17)$ with secant distribution

$$\tau_0 = 88, \quad \tau_1 = 36, \quad \tau_2 = 99, \quad \tau_3 = 84.$$

2. The new $(41,4)$-arc has been constructed in the following manner. First the point $(1,2,8)$ was deleted from $\mathcal{K}_2$ and after that the obtained arc was extended to a $(41,4)$-arc using the next 15 points $(0,1,8)$, $(1,0,e)$, $(1,1,6)$, $(1,2,g)$, $(1,4,0)$, $(1,4,d)$, $(1,5,g)$, $(1,6,4)$, $(1,7,8)$, $(1,7,d)$, $(1,8,8)$, $(1,8,a)$, $(1,b,9)$, $(1,b,a)$, $(1,g,7)$.

The new $(41,4)$-arc in $PG(2,17)$ has secant distribution

$$\tau_0 = 45, \quad \tau_1 = 44, \quad \tau_2 = 46, \quad \tau_3 = 86, \quad \tau_4 = 86.$$

■

S. Ball [1,2] (see also [8] Table 6.3) proved that for an $\{l,t\}$-blocking set in $PG(2,q)$ with $q = p > 3$ prime and $t < p/2$ it follows that $l \geq (2t+1)(p+1)/2$. For $PG(2,17)$ we have that an $\{l,2\}$-blocking set must have $l \geq 45$ points, an $\{l,3\}$-blocking set must have $l \geq 63$ points and an $\{l,4\}$-blocking set must have $l \geq 81$ points.

Theorem 2.2 *There exist a $\{86,4\}$-blocking set in $PG(2,17)$.*

Therefore,

$$221 \leq m_{14}(2, 17) \leq 226.$$

Proof.

1. The union of three non-concurrent lines is a $\{3q = 51, 2\}$-blocking set (see [7], p. 156, Example 2.2).

Let $l_1 : x = 0$, $l_2 : x + 2z = 0$ and $l_3 : x + y + z = 0$ be the next three lines respectively:

l_1: {(0,0,1), (0,1,0), (0,1,1), (0,1,2), (0,1,3), (0,1,4), (0,1,5), (0,1,6), (0,1,7), (0,1,8), (0,1,9), (0,1,a), (0,1,b), (0,1,c), (0,1,d), (0,1,e), (0,1,f), (0,1,g).}

l_2: {(0,1,0), (1,0,8), (1,1,8), (1,2,8), (1,3,8), (1,4,8), (1,5,8), (1,6,8), (1,7,8), (1,8,8), (1,9,8), (1,a,8), (1,b,8), (1,c,8), (1,d,8), (1,e,8), (1,f,8), (1,g,8). }

l_3: { (0,1,g), (1,0,g), (1,1,f), (1,2,e), (1,3,d), (1,4,c), (1,5,b), (1,6,a), (1,7,9), (1,8,8) (1,9,7), (1,a,6), (1,b,5), (1,c,4), (1,d,3), (1,e,2), (1,f,1), (1,g,0). }

As we can see $l_1 \cap l_2 = \{(0, 1, 0)\}$, $l_1 \cap l_3 = \{(0, 1, g)\}$ and $l_2 \cap l_3 = \{(1, 8, 8)\}$. So the lines are non-concurrent and form a $\{51, 2\}$-blocking set $\mathcal{B}_1$ in $PG(2, 17)$. The secant distribution of $\mathcal{B}_1$ is

$$\tau_2 = 48, \quad \tau_3 = 256, \quad \tau_{18} = 3.$$

The complement of $\mathcal{B}_1$ is a $(256, 16)$-arc in $PG(2, 17)$.

2. A $\{68, 3\}$-blocking set $\mathcal{B}_2$ in $PG(2, 17)$ was constructed by extending the blocking set $\mathcal{B}_1$ with the next 17 points:

$$\begin{array}{llllll} (1,0,0), & (1,0,1), & (1,0,2), & (1,0,3), & (1,0,4), & (1,0,5), \\ (1,0,6), & (1,0,7), & (1,0,8), & (1,0,9), & (1,0,a), & (1,0,b), \\ (1,0,c), & (1,0,d), & (1,0,e), & (1,0,f), & (1,8,0). & \end{array}$$

The obtained blocking set in $PG(2, 17)$ has the following secant distribution

$$\tau_3 = 87, \quad \tau_4 = 190, \quad \tau_5 = 25, \quad \tau_6 = 1, \quad \tau_{18} = 4.$$

The complement of this $\{68, 3\}$-blocking set is a $(239, 15)$-arc in $PG(2, 17)$.

The existence of a $\{4q = 68, 3\}$-blocking set follows also from [7], but our blocking set is different from the blocking set, that can be obtained by the construction (p. 156, Example 2.3) given in [7].

3. A $\{86, 4\}$-blocking set $\mathcal{B}_3$ in $PG(2, 17)$ was constructed by extending the blocking set $\mathcal{B}_2$ with the following 18 points:

$$\begin{array}{llllll} (1,1,4), & (1,2,1), & (1,3,f), & (1,4,g), & (1,5,9), & (1,6,6), \\ (1,6,7), & (1,7,3), & (1,7,c), & (1,8,g), & (1,9,e), & (1,a,b), \\ (1,b,6), & (1,c,5), & (1,c,d), & (1,d,2), & (1,f,d), & (1,g,a). \end{array}$$

The obtained blocking set $\mathcal{B}_3$ in $PG(2,17)$ has the following secant distribution

$$\tau_4 = 116, \quad \tau_5 = 135, \quad \tau_6 = 39, \quad \tau_7 = 11, \quad \tau_8 = 1 \quad \tau_{18} = 5.$$

The complement of this $\{86,4\}$-blocking set is a $(221,14)$-arc in $PG(2,17)$. ■

3. The related linear 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 $\mathbf{x} \in V(n,q)$ is called the *Hamming weight* $\mathrm{wt}(\mathbf{x})$ of $\mathbf{x}$. The *Hamming distance* $d(\mathbf{x},\mathbf{y})$ between two vectors $\mathbf{x},\mathbf{y} \in V(n,q)$ 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 $[n,k,d]_q$ 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. Two versions are:

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

Problem 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 *d-optimal* or *n-optimal* respectively.

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

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

($\lceil x \rceil$ denotes the smallest integer $\geq x$). Codes with parameters $[g_q(k,d),k,d]_q$, are called *Griesmer codes.*

There exist a close relationship between (n,r)-arcs in $PG(2,q)$ and $[n,3,d]_q$ codes, given in the next two Theorems.

Theorem 3.1 *[6] Every $[n,k,d]_q$ Griesmer code with $d \leq q^{k-1}$ is projective.*

Theorem 3.2 *[6] There exist a projective $[n, 3, d]_q$ code if and only if there exist an $(n, n-d)$-arc in $PG(2, q)$.*

From Theorems 2.1–2.2 and Theorems 3.1–3.2 we have the following:

Corollary 3.3 *There exist Griesmer codes with parameters:*

$$[27, 3, 24]_{17}, \quad [41, 3, 37]_{17}, \quad [221, 3, 207]_{17}.$$

References

[1] S. Ball, *On sets of points in finite planes*, Ph.D. Thesis, University of Sussex, 1994.

[2] S. Ball, Multiple blocking sets and arcs in finite planes, *J. London Math. Soc.*, **54** (1996), 427–435.

[3] A. Barlotti, Some topics in finite geometrical structures, Institute of Statistics, University of Carollina, mimeo series, **439** (1965).

[4] R. Bose, Mathematical theory of the symmetrical factorial design, *Sankyha*, **8** (1947), 107–166.

[5] R. Daskalov and M. Jimenez Contreras, New $(k; r)$-arcs in the projective plane of order thirteen, (submitted).

[6] R. Hill, Optimal linear codes, *Cryptography and Coding II*, Oxford University Press, 1992, 41-70.

[7] R. Hill and J.R.M. Mason, On (k, n)-arcs and the falsity of the Lunell-Sce conjecture, in *London Math. Soc. Lecture Note Series*, **49** (1981), CUP, 153–168.

[8] J. W.P. Hirschfeld and 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.

[9] M. Tallini Scafati, Sui (k, n)-archi di un piano grafico finito, *Rend. Naz. Lincei*, **49** (1966), (8), 1–6.

[10] W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. Ecole Norm. Sup.*, **2** (1969), 521-560.

Department of Mathematics,
Technical University of Gabrovo,
5300 Gabrovo, BULGARIA,
e-mail: daskalov@tugab.bg, metodieva@tugab.bg

Received 30.09.2003