Contributions to Discrete Mathematics

Volume 3, Number 1, Pages 14–19
ISSN 1715-0868

CONSTRUCTIONS OF SMALL COMPLETE ARCS WITH PRESCRIBED SYMMETRY

PETR LISONĚK, STEFANO MARCUGINI, AND FERNANDA PAMBIANCO

Dedicated to the centenary of the birth of Ferenc Kárteszi (1907–1989).

Abstract. We use arcs found by Storme and van Maldeghem in their classification of primitive arcs in $\mathrm{PG}(2,q)$ as seeds for constructing small complete arcs in these planes. Our complete arcs are obtained by taking the union of such a "seed arc" with some orbits of a subgroup of its stabilizer. Using this approach we construct five different complete 15-arcs fixed by $\mathbf{Z}_3$ in $\mathrm{PG}(2,37)$, a complete 20-arc fixed by $\mathbf{S}_3$ in $\mathrm{PG}(2,61)$, and two different complete 22-arcs fixed by $\mathbf{D}_5$ in $\mathrm{PG}(2,71)$. In all three cases, the size of complete arcs constructed in this paper is strictly smaller than the size of the smallest complete arcs (in the respective plane) known so far.

1. Introduction

Let $\mathrm{PG}(2,q)$ be the projective plane over the field with q elements which we denote by $\mathrm{GF}(q)$. A k-arc in $\mathrm{PG}(2,q)$ is a set of k points, no three of which are collinear. A k-arc in $\mathrm{PG}(2,q)$ is called complete if it is not contained in a $(k+1)$-arc in $\mathrm{PG}(2,q)$. See [4] for an introduction to arcs. Let $t_2(q)$ denote the smallest size (number of points) of a complete arc in $\mathrm{PG}(2,q)$. It is known that for q prime (which is the case throughout this paper), $t_2(q) > (\sqrt{3q}+1)/2$ [1]. The best known asymptotic upper bound on $t_2(q)$ is $O(\sqrt{q}\log^c q)$ [6]. Explicit constructions of complete arcs with about $q/2$ points can be found in [4, Chapter 9].

If we consider the coordinates of the points of a complete arc in $\mathrm{PG}(2,q)$ as column vectors in $\mathrm{GF}(q)^3$, we obtain the parity check matrix of a q-ary linear code with codimension 3, minimum Hamming distance at least 4, and covering radius 2 [5, Section 1.3]. It can be shown that arcs and linear maximum distance separable codes (MDS codes) are equivalent objects, see [5]. Indeed, it is the coding theory which often motivates the study of the spectrum of values of k for which a complete k-arc exists in $\mathrm{PG}(2,q)$ for a fixed value of q.

2000 *Mathematics Subject Classification.* Primary: 51E21. Secondary: 51E22, 94B05.
Key words and phrases. Arc, complete arc, projective plane.
Research of the first author partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

The *index* of a point P with respect to the arc T is the number of bisecants of T through P, see [4, Chapter 9]. The occurrence of points of high index with respect to an arc increases the saturation of that arc (the number of external points that lie on bisecants of the arc) as it decreases the number of points covered by more than one bisecant and thus it is a frequent feature of small complete arcs.

In [8] Storme and van Maldeghem classified all arcs in $\mathrm{PG}(2,q)$ admitting a transitive primitive group of projective transformations. It turns out that, in cases when these arcs are not complete, they still exhibit high saturation when compared to arcs of the same cardinality in the same plane. This suggests the idea of using these arcs as "seeds" for constructing complete arcs which are then obtained as the union of such "seed arc" with some orbits of a suitable subgroup of the stabilizer of the seed arc. This process has been implemented as a computer search using the computer algebra system MAGMA [2].

In the following three sections we give examples of complete arcs constructed in this way. In each of the three planes, the sizes of our arcs are strictly smaller than the sizes of complete arcs obtained by heuristic search [3], and our arcs are the smallest known complete arcs in the respective planes—see [3] and [7] for tables of sizes of the smallest known arcs before this paper.

2. Complete 15-arcs in $\mathrm{PG}(2,37)$

Suppose that w is a primitive third root of unity in $\mathrm{GF}(q)$ (i.e. $w^3=1$, $w\neq 1$) and let $b\in\mathrm{GF}(q)$. Define the following nine points in $\mathrm{PG}(2,q)$:

$$\begin{array}{lll} p_1=(1,1,1) & p_2=(1,w,w^2) & p_3=(1,w^2,w) \\ p_4=(1,1,b) & p_5=(1,w,w^2b) & p_6=(1,w^2,wb) \\ p_7=(b,1,b) & p_8=(b,w,w^2b) & p_9=(b,w^2,wb). \end{array}$$

Then $K=\{p_1,p_2\dots,p_9\}$ is the set of points from [8], Proposition 1 in which we are taking without loss of generality $d=1$ throughout this paper. Under certain conditions on b (see [8], page 204), the set K is an arc in $\mathrm{PG}(2,q)$, and we will henceforth assume that K is an arc. The arc K is fixed setwise by the group $G=\langle A,B\rangle$ isomorphic to $\mathbf{Z}_3\times\mathbf{Z}_3$ generated by (recall that we take $d=1$ in [8])

$$A=\begin{pmatrix} 1 & 0 & 0 \\ 0 & w & 0 \\ 0 & 0 & w^2 \end{pmatrix}$$

and

$$B=\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & b & 0 \end{pmatrix}.$$

K is a complete arc if and only if $q=13$ [8]. Among interesting properties of K we note that each point in the G-orbit of $r=(1,1,-b-1)$ has index 4 (i.e. the highest possible index) with respect to K, since we have

w	b	arc
26	7	$K \cup G'((1,7,19)) \cup G'((1,28,30))$
26	9	$K \cup G'((1,24,24)) \cup G'((1,28,29))$
26	9	$K \cup G'((1,7,34)) \cup G'((1,24,7))$
10	22	$K \cup G'((1,13,13)) \cup G'((1,29,34))$
10	22	$K \cup G'((1,31,33)) \cup G'((1,31,22))$

FIGURE 1. Complete 15-arcs in $\mathrm{PG}(2,37)$.

the following collinear triples in $\mathrm{PG}(2,q)$: $\{r,p_1,p_4\}$, $\{r,p_2,p_6\}$, $\{r,p_3,p_5\}$ and $\{r,p_8,p_9\}$, where p_i are the points of K as above.

Proposition 2.1. *We have*

$$t_2(37) \leq 15.$$

Proof. Let $G' = \langle AB \rangle$ be the subgroup of G isomorphic to $\mathbf{Z}_3$ generated by the product of matrices A and B:

$$AB = \begin{pmatrix} 0 & 0 & 1 \\ w & 0 & 0 \\ 0 & w^2 b & 0 \end{pmatrix}$$

We construct five pairwise non-isomorphic complete 15-arcs in $\mathrm{PG}(2,37)$ with details recorded in Figure 1. Each row in Figure 1 corresponds to one arc, with the values of b and w fixed at the beginning of the row. In each row, the letter K denotes the set $K = \{p_1,\ldots,p_9\}$ in $\mathrm{PG}(2,37)$ as defined above for the fixed values $b,w \in \mathrm{GF}(37)$, and $G'(s)$ denotes the orbit of G' containing s, again for the same fixed values of b and w.

It can be verified, e.g. using MAGMA [2], that these five sets are non-isomorphic complete 15-arcs in $\mathrm{PG}(2,37)$. $\square$

3. A Complete 20-arc in PG(2, 61)

Let q be a prime power with $q \equiv \pm 1 \pmod{10}$ and let a be an element of $\mathrm{GF}(q)$ satisfying

$$a^2 + a - 1 = 0. \tag{3.1}$$

Consider the following two sets in $\mathrm{PG}(2,q)$:

$$\begin{aligned} M_1 &= \{(1,1,1),(1,a,a),(a,a,1),(a,1,a),(0,1,a), \\ &\quad (1,a,0),(a,0,1),(a,1,0),(1,0,a),(0,a,1)\} \end{aligned} \tag{3.2}$$

and

$$M_2 = \{(1,0,0),(0,1,0),(0,0,1),(a,1,1),(1,a,1),(1,1,a)\}.$$

M_1 and M_2 are projectively equivalent to the sets K_1 and K_2, respectively, which are given in [8], Proposition 12. Indeed, if Π is the projectivity defined by the matrix

$$\begin{pmatrix} 1 & -1 & 0 \\ a & a & -1 \\ 0 & 0 & -a \end{pmatrix}$$

then $\Pi(M_i) = K_i$ for $i = 1, 2$. (The only reason for using a different presentation of K_1 and K_2 in our paper is that we find our presentation easier to work with.) By Proposition 12 of [8], M_1 and M_2 are arcs in $\mathrm{PG}(2, q)$, both fixed by $\mathbf{A}_5$, such that the 10 points of M_1 are precisely the points of $\mathrm{PG}(2, q)$ of index 3 with respect to M_2.

Proposition 3.1. *We have*

$$t_2(61) \leq 20.$$

Proof. Let us fix the root $a = 17$ of the equation $a^2+a-1 = 0$ in $\mathrm{GF}(61)$. Let $\mathbf{S}_3$ denote the subgroup of $\mathrm{PGL}(3, 61)$ consisting of the six 3×3 permutation matrices; this group fixes the arc M_2 setwise. Let $b = 13$ and $c = -b-1 = 47$ be the two solutions of $y^2+y+1 = 0$ in $\mathrm{GF}(61)$; then $T = \{(1, b, c), (1, c, b)\}$ is an orbit of $\mathbf{S}_3$. Let

$$p = (1, 11, 32) \quad \text{and} \quad r = (1, 25, 51).$$

Now let H be the set of 20 points in $\mathrm{PG}(2, 61)$ defined by

$$H = M_2 \cup T \cup \mathbf{S}_3(p) \cup \mathbf{S}_3(r),$$

where $\mathbf{S}_3(s)$ denotes the orbit of $\mathbf{S}_3$ containing the point s. It can be verified e.g. using MAGMA that H is a complete arc in $\mathrm{PG}(2, 61)$. $\square$

3.1. **Remarks.** For the sake of illustration let us list the points with the two highest values (namely 9 and 8) of index with respect to the complete arc H.

The point $j = (1, 1, 1)$ has index 9 with respect to H, because it has index 3 on M_2 and, moreover, $\{j, p, r\}$ (where p and r are defined above) is a collinear triple, hence j has index 6 on $\mathbf{S}_3(p) \cup \mathbf{S}_3(r)$.

Each point in the $\mathbf{S}_3$-orbit of $x = (1, -1, 0)$ has index 9 with respect to H, because x has index 3 on any orbit of $\mathbf{S}_3$ that is a 6-arc, x has index 2 on the arc M_2, and x is collinear with the points $(1, b, c), (1, c, b)$.

Each point in the $\mathbf{S}_3$-orbit of $y = (a, a, 1)$ has index 8 with respect to H. Let us introduce the following notation for the action of H's stabilizer $\mathbf{S}_3$ on the Galois plane under consideration: for a point $z = (z_0, z_1, z_2)$ and $\{k, l, m\} = \{0, 1, 2\}$ let us define $z_{klm} = (z_k, z_l, z_m)$. We note that y has index 3 on the arc M_2, further we have the collinear triples $\{y, q, r_{102}\}$, $\{y, p_{201}, r_{120}\}$ and $\{y, p, (1, b, c)\}$, and two more collinear triples containing y are obtained from the last two triples by the involution $(z_0, z_1, z_2) \longleftrightarrow (z_1, z_0, z_2)$.

4. Complete 22-arcs in PG(2, 71)

Proposition 4.1. *We have*

$$t_2(71) \leq 22.$$

Proof. Let us fix the root $a = 8$ of the equation $a^2 + a - 1 = 0$ in GF(71) and let M_1 denote the 10-arc in PG(2, 71) as defined above in (3.2). Let $\mathbf{D}_5$ denote the subgroup of PGL(3, 71) that fixes M_1 setwise and additionally fixes the point $(1, 0, 0)$. $\mathbf{D}_5$ is isomorphic to the dihedral group of order 10 and it is generated, for example, by the matrices

$$R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 1 & 1 & -a-1 \\ 0 & a+1 & -a-1 \\ 0 & a+1 & -1 \end{pmatrix}.$$

Using polynomial resultants it can be easily checked that, if $T = \{(1, b, c), (1, c, b)\}$ is a two-element orbit of $\mathbf{D}_5$, then b and c are distinct roots of $y^2 - (2a+1)y - a + 2 = 0$ in GF(71). For our fixed value $a = 8$ let $b = 39$ and $c = 49$. Let

$$u = (1, 67, 16) \quad \text{and} \quad v = (1, 25, 5)$$

and let $\mathbf{D}_5(s)$ be the orbit of $\mathbf{D}_5$ containing the point s. Define the two arcs

$$J_1 = M_1 \cup T \cup \mathbf{D}_5(u) \quad \text{and} \quad J_2 = M_1 \cup T \cup \mathbf{D}_5(v).$$

It can be verified e.g. using MAGMA that J_1 and J_2 are two non-isomorphic complete 22-arcs in PG(2, 71). □

4.1. **Remarks.** Again for illustration we list the points with the two highest values (namely 10 and 9) of index with respect to the arcs J_1 and J_2. These points are the same for both arcs. Let $\Pi_M(x) := Mx^T$ denote the projectivity defined by the matrix M.

Each of the five points in the $\mathbf{D}_5$-orbit of $s = (0, 1, -1)$ has index 10 on J_1 and J_2 because of the collinear triples of the form $\{s, p, \Pi_R(p)\}$ where R is one of the generators of $\mathbf{D}_5$ given above. Notice that the only fixed points of Π_R in J_1 or J_2 are $(1, 1, 1)$ and $(1, a, a)$.

Each of the five points in the $\mathbf{D}_5$-orbit of $t = (-a+2, a, a)$ has index 9 on J_1 and J_2. Next we give the coordinates of points in collinear triples through the point t. We use expressions containing a in cases where the collinearity follows already using the general algebraic condition (3.1) on a, and we use numerical values (where $a = 8$) in the remaining cases. We have the collinear triples $\{t, (1, a, 0), (a, 0, 1)\}$, $\{t, (8, 1, 8), (1, b, c)\}$ and $\{t, (1, 1, 1), (1, a, a)\}$. Another two triples are obtained by applying Π_R to the first two triples. Let $T = RS$ be the product of the two generators of $\mathbf{D}_5$ given above. For each of J_1 and J_2, two more collinear triples are of the form $\{t, w, \Pi_T(w)\}$ and $\{t, (0, 1, 8), \Pi_U(w)\}$ for suitably chosen point w and $U \in \mathbf{D}_5$, and the last two triples are again obtained by applying Π_R. Taking $w = u$ and $U = S^{-2}$ yields the arc J_1, whereas taking $w = v$ and $U = S^{-1}$ yields J_2.

References

1. A. Blokhuis, *On the size of a blocking set in* $\mathrm{PG}(2,p)$, Combinatorica **14** (1994), no. 1, 111–114.
2. W. Bosma and J. J. Cannon, *Handbook of Magma functions*, School of Mathematics and Statistics, University of Sydney, Sydney, 2000.
3. A. A. Davydov, G. Faina, S. Marcugini, and F. Pambianco, *Computer search in projective planes for the sizes of complete arcs*, J. Geom. **82** (2005), no. 1-2, 50–62.
4. J. W. P. Hirschfeld, *Projective geometries over finite fields*, second ed., Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1998.
5. J. W. P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces: update 2001*, Finite geometries, Dev. Math., vol. 3, Kluwer Acad. Publ., Dordrecht, 2001, pp. 201–246.
6. J. H. Kim and V. H. Vu, *Small complete arcs in projective planes*, Combinatorica **23** (2003), no. 2, 311–363.
7. F. Pambianco and L. Storme, *Small complete caps in spaces of even characteristic*, J. Combin. Theory Ser. A **75** (1996), no. 1, 70–84.
8. L. Storme and H. Van Maldeghem, *Primitive arcs in* $\mathrm{PG}(2,q)$, J. Combin. Theory Ser. A **69** (1995), no. 2, 200–216.

Department of Mathematics, Simon Fraser University,
Burnaby, BC, V5A 1S6, Canada
E-mail address: lisonek@math.sfu.ca

Dipartimento di Matematica e Informatica,
Università degli Studi di Perugia,
Via Vanvitelli 1, 06123 Perugia, Italy
E-mail address: gino@dipmat.unipg.it
E-mail address: fernanda@dipmat.unipg.it