Journal of Algebraic Combinatorics 3 (1994), 113–128

Cyclic Arcs in $PG(2, q)$

L. STORME
LS@CAGE.RUG.AC.BE
H. VAN MALDEGHEM
HVM@CAGE.RUG.AC.BE
Department of Pure Math and Computer Algebra, University of Gent, Galglaan 2, B-9000 Gent, Belgium

Received April 13, 1993; Revised June 17, 1993

Abstract. B.C. Kestenband [9], J.C. Fisher, J.W.P. Hirschfeld, and J.A. Thas [3], E. Boros, and T. Szönyi [1] constructed complete $(q^2 - q + 1)$-arcs in $PG(2, q^2)$, $q \geq 3$. One of the interesting properties of these arcs is the fact that they are fixed by a cyclic projective group of order $q^2 - q + 1$. We investigate the following problem: What are the complete k-arcs in $PG(2, q)$ which are fixed by a cyclic projective group of order k? This article shows that there are essentially three types of those arcs, one of which is the conic in $PG(2, q)$, q odd. For the other two types, concrete examples are given which shows that these types also occur.

Keywords: k-arc, conic, M.D.S. code, cyclic group

1. Introduction

A k-arc in $PG(2, q)$ is a set of k points, no 3 of which are collinear. A point p of $PG(2, q)$ extends a k-arc K to a $(k + 1)$-arc if and only if $K \cup \{p\}$ is a $(k + 1)$-arc. A k-arc K is complete if it is not contained in a $(k + 1)$-arc. The point set of a conic is a $(q + 1)$-arc of $PG(2, q)$ [4].

In $PG(2, q)$, q odd, every conic is complete as $(q + 1)$-arc. A $(q + 1)$-arc of $PG(2, q)$, q even, is always incomplete. It can be extended in a unique way to a $(q + 2)$-arc by a point r which is called the nucleus of this $(q + 1)$-arc [4].

B. Segre's famous theorem: *Every $(q + 1)$-arc of $PG(2, q)$, q odd, is a conic* [15] was for many geometers a stimulus and motivation to study finite geometry. This theorem is however not valid in $PG(2, q)$, q even. In $PG(2, q)$, q even, $q \geq 16$, different types of $(q + 2)$-arcs are known. The collineation groups which fix these $(q + 2)$-arcs have all been determined. A survey of all known types of $(q + 2)$-arcs in $PG(2, q)$, q even and $q \neq 64$, can be found in [11]; for $q = 64$, see [12].

The following question arises: For which values of k does there exist a complete k-arc in $PG(2, q)$? This problem has been investigated by many geometers. The bibliographies of [4, 5, 6] contain a large number of references to articles in which complete k-arcs of $PG(2, q)$ are constructed. One example of a complete k-arc in $PG(2, q)$ ($k < q + 1$ when q is odd and $k < q + 2$ when q is even) merits special attention. B.C. Kestenband [9], J.C. Fisher, J.W.P. Hirschfeld, and J.A. Thas [3], E. Boros and T. Szönyi [1] constructed in $PG(2, q^2)$, $q \geq 3$, a complete

$(q^2 - q + 1)$-arc which was the intersection of two Hermitian curves. These arcs differ in two ways from the other known complete k-arcs: They are fixed by a cyclic projective group of order $q^2 - q + 1$ and in $PG(2, q^2), q$ even, $q \geq 4$, these complete $(q^2 - q + 1)$-arcs are the largest arcs of $PG(2, q^2)$ which are not contained in a $(q^2 + 2)$-arc.

A lot of complete k-arcs in $PG(2, q)$ were constructed by using the following idea, due to Segre and Lombardo-Radice [10, 16], as a starting point: *The points of the arc are chosen, with some exceptions, among the points of a conic or cubic curve.*

We will look for complete k-arcs in $PG(2, q)$ in a different way. We look for all types of complete k-arcs K which are fixed by a cyclic projective group, i.e., a cyclic subgroup of $PGL(3, q)$, G of order k which acts transitively on the points of K. This will result in new examples of complete k-arcs in $PG(2, q)$ for specific values of q.

2. Known results

Here follow the known complete k-arcs K of $PG(2, q)$ which are fixed by a cyclic projective group of order k, acting transitively on the k points of K.

2.1. *A conic in $PG(2, q)$, q odd*

The conic $C : X_0^2 = X_1X_2$ in $PG(2, q)$, q odd, is a complete $q + 1$-arc. It is fixed by a sharply 3-transitive projective group G which is isomorphic to $PGL(2, q)$ [4, p. 143].

Consider two conjugate elements r_1, r_2 of C in a quadratic extension of $PG(2, q)$. The subgroup H (of G) which fixes r_1 and r_2 is a cyclic subgroup of order $q + 1$ of G. This group H acts transitively on the $q + 1$ points of C. Moreover, all cyclic subgroups of order $q + 1$ of G are conjugate to H. So, C is a complete $(q + 1)$-arc of $PG(2, q)$ which is fixed by a cyclic projective group of order $q + 1$.

2.2. *Complete $(q^2 - q + 1)$-arcs in $PG(2, q^2), q > 2$*

These arcs were first discovered by B.C. Kestenband who found these arcs as one of the possible types of intersection of two Hermitian curves in $PG(2, q^2)$ [9]. They were then studied in detail by Boros and Szönyi [1] and by Fisher, Hirschfeld, and Thas [3]. They also proved that these arcs are fixed by a cyclic projective group H of order $q^2 - q + 1$. Moreover, this group H is a subgroup of a cyclic Singer group of $PG(2, q^2)$.

2.3. Two examples in $PG(2, 11)$ [14]

1. A complete 7-arc K_1 which is fixed by a projective group G_1 of order 21 which is isomorphic to 7:3, i.e., a group of order 21 which is the semidirect product of the cyclic groups Z_7 and Z_3 where Z_7 is a normal subgroup of G_1.
2. A complete 8-arc K_2 which is fixed by a projective group G_2 of order 16 which is isomorphic to the semidihedral group of order 16.

3. k odd

In this section we show that in case k is odd, the cyclic group is necessarily a subgroup of a cyclic Singer group, i.e., a cyclic group acting regularly on the set of points of $PG(2, q)$. As usual, a Singer-cycle is a generator of a cyclic Singer group.

THEOREM 3.1. *Let K be a complete k-arc in $PG(2, q)$ with k odd and suppose $G \leq PGL(3, q)$ is a cyclic group acting regularly on K. Then G is generated by a power of a Singer-cycle (so G is a subgroup of a cyclic Singer group) and hence all orbits of G are complete k-arcs, partitioning $PG(2, q)$ into $(q^2 + q + 1)/k$ such arcs. If moreover $G \leq PGU(3, \sqrt{q})$, then $k = q - \sqrt{q} + 1$ and K is equivalent to the complete $(q - \sqrt{q} + 1)$-arc discovered by B. C. Kestenband (see 2.2).*

Proof. Let us denote by α a generator of the cyclic group G. Suppose G has a point-orbit of length $s < k$ (so $s|k$). Denote this orbit by $\{p_1, \dots, p_s\}$. Then α^s fixes each p_i, $i = 1, 2, \dots, s$. Suppose now $s \geq 3$ and at least 3 points of $\{p_i \| i = 1, 2, \dots, s\}$ lie on a common line M. Clearly, α^s induces the identity on M (since it fixes at least 3 points), so α^s is a perspectivity with axis M and some center c. Note $c \notin K$ since α^s acts semiregularly on K. Since k is odd, there is at least one line L through c tangent to K. But α^s must fix $L \cap K$, contradicting the semiregular action of α^s on K.

Hence if $s \geq 4$, then $\{p_1, \dots, p_4\}$ is a basis fixed point by point by α^s, so α^s is the identity and $s = k$, a contradiction to our assumption. Consequently $s \leq 3$. Now suppose $s = 3$. By the above, p_1, p_2, and p_3 form a nondegenerate triangle. Putting $p_1(1, 0, 0)$, $p_2(0, 1, 0)$, and $p_3(0, 0, 1)$ and assuming $p_i^\alpha = p_{i+1}$, subscripts to be taken modulo 3, then α can be expressed as follows:

$$\alpha : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} 0 & 0 & d \\ 1 & 0 & 0 \\ 0 & c & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

But one computes that in this case α^3 is trivial, so $k = s = 3$, again contradicting our assumptions.

Now $s \neq 2$ since k is odd, so $s = 1$ and α fixes a point p_1. Let L be a line through p_1 tangent to K (L exists since k is odd). Then L^{α^i} is tangent to K for all $i = 1, \ldots, k$ and contains p_1. Since G acts regularly on K, every point of K is on L^{α^i} for some i, $1 \le i \le k$. Hence $K \cup \{p_1\}$ is a $(k+1)$-arc contradicting the completeness of K. So we conclude that every orbit of G on the pointset of $PG(2, q)$ has size k. Consequently $k|(q^2 + q + 1)$.

Now note that neither 2 nor 9 divides $q^2 + q + 1$. So since $k > 3$, there exists a prime $p > 3$ dividing k. Put $k' = k/p$ and consider $\alpha' = \alpha^{k'}$, then α' has order p. Let H be a Sylow p-subgroup of $PGL(3, q)$ containing α'. Since $p|(q^2 + q + 1)$ and therefore $p \not| q^3(q+1)(q-1)^2$ (which is equal to $|PGL(3, q)|/(q^2 + q + 1)$) since $(q^2 + q + 1, q^3(q+1)(q-1)^2) \le 3$, we have $|H|\ |(q^2 + q + 1)$ and so H is a Sylow p-group in a cyclic Singer group S. Since G is an abelian group, G normalizes α', but that implies (since the normalizer of α' is the same normalizer of S in $PGL(3, q)$, which is a group $S : 3$; see e.g. [8, p. 188]) that $G \le S : 3$ and so clearly $G \le S$. It follows easily that every orbit under G is a complete k-arc (since S is transitive) and that K is unique up to equivalence. So the cyclic complete $(q - \sqrt{q} + 1)$-arcs in $PG(2, q)$, q square, (2.2) are unique up to equivalence.

Suppose $G \le PGU(3, \sqrt{q})$, then G fixes a Hermitian curve $\mathcal{H}$ and since all orbits of G in $PG(2, q)$ are equivalent, assume $K \subseteq \mathcal{H}$. Then $k|(\sqrt{q^3} + 1)$. A similar argument as above readily implies $G \le S^*$, where S^* is the subgroup of order $q - \sqrt{q} + 1$ of S (alternatively, $k|(q\sqrt{q} + 1, q^2 + q + 1)$ and this is equal to $q - \sqrt{q} + 1$). Since S^* itself partitions $\mathcal{H}$ into complete $(q - \sqrt{q} + 1)$-arcs (2.2, [1, 3]), G must be equal to S^*, otherwise K is strictly contained in such a complete arc. This completes the proof. □

3.1. Examples

The cyclic 7-arc K_1 in $PG(2, 11)$, discovered by A. R. Sadeh [14] (see also 2.3), is an example of a cyclic complete k-arc in $PG(2, q)$ for which k is odd. Since k must be a divisor of $q^2 + q + 1$ (Theorem 3.1), the order k of cyclic complete k-arcs, with k odd, in $PG(2, q)$ depends on the factorization of $q^2 + q + 1$. The three following examples are cyclic k-arcs in $PG(2, q)$ (k odd) which are fixed by a cyclic projective group of order k which is a subgroup of a cyclic Singer group. Let $r = q^2 + q + 1$ and $t = r/k$. Then α is the Singer-cycle which is considered and $\beta = \alpha^t$ is the generator of the cyclic group G which fixes K. If $K = \{p_0, \ldots, p_{k-1}\}$, then $p_i^\alpha = p_{i+1}$ (indices modulo k). In the second and third example, we also state the total number of points of $PG(2, q)$ which extend K to a larger arc in $PG(2, q)$ and we also give an example of such a point.

3.1.1. A complete 21-arc in $PG(2, 37)$.

$$\alpha : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 7 & 2 \\ 2 & 8 & 5 \\ 3 & 6 & 32 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

$$\beta : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 16 & 26 & 2 \\ 36 & 36 & 20 \\ 14 & 27 & 5 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

$K = \{(1, 30, 24), (1, 31, 29), (1, 24, 5), (1, 30, 1), (1, 3, 6), (1, 36, 12), (1, 33, 6),$
$(1, 31, 32), (1, 29, 31), (1, 4, 20), (1, 36, 0), (1, 0, 5), (1, 28, 20),$
$(1, 16, 8), (1, 8, 29), (1, 20, 34), (1, 21, 11), (1, 3, 13),$
$(1, 12, 26), (1, 10, 32), (1, 0, 0)\}.$

3.1.2. An incomplete 21-arc in $PG(2, 67)$.

$$\alpha : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 7 & 2 \\ 2 & 8 & 5 \\ 3 & 6 & 55 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

$$\beta : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 11 & 37 & 23 \\ 6 & 11 & 20 \\ 17 & 31 & 18 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

$K = \{(1, 31, 32), (1, 66, 64), (1, 43, 12), (1, 58, 46), (1, 44, 37), (1, 57, 46),$
$(1, 42, 30), (1, 6, 59), (1, 57, 60), (1, 35, 45), (1, 29, 58), (1, 13, 14),$
$(1, 63, 27), (1, 29, 61), (1, 34, 34), (1, 52, 10), (1, 53, 0), (1, 18, 48),$
$(1, 35, 18), (1, 42, 57), (1, 0, 0)\}$

Exactly 63 points of $PG(2, 67)$ extend K to a 22-arc, f.i., the point (28, 65, 11) extends K to a larger arc.

3.1.3. An incomplete 7-arc in $PG(2, 53)$.

$$\alpha : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 7 & 2 \\ 2 & 8 & 5 \\ 3 & 6 & 8 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

$$\beta : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 25 & 42 & 11 \\ 3 & 40 & 24 \\ 48 & 48 & 5 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

$$K = \{(1, 51, 21), (1, 41, 37), (1, 23, 32), (1, 38, 14), (1, 45, 38), (1, 12, 13), (1, 0, 0)\}.$$

For this arc, there are 1848 points of $PG(2, 53)$ which extend K to a 8-arc, f.i., the point (12, 24, 43) extends K to a larger arc.

4. *k* even

In this section, we shall always assume that $K = \{q_0, \ldots, q_{k-1}\}$ is a complete k-arc, with k even and $k \geq 8$, of $PG(2, q)$, which is fixed by a cyclic projective group G of order k acting transitively on the points of K. This arc K will be called a *cyclic complete k-arc*. Let α be a generator of G. Assume that $\alpha(q_i) = q_{i+1}$ where the indices are calculated modulo k.

THEOREM 4.1. *Let G be a cyclic collineation group of a finite projective plane π. Assume that π^* is the dual plane of π. Then π and π^* have the same cyclic structure under G.*

Proof. See [7, p. 256]. □

LEMMA 4.1. *Let $K = \{q_0, \ldots, q_{k-1}\}$. The $k(k-1)/2$ bisecants of K partition (under G) into $(k-2)/2$ orbits of size k and one orbit of size $k/2$. This last orbit consists of the $k/2$ lines $q_i q_{k/2+i} (i = 0, \ldots, k/2 - 1)$.*

Proof. Assume that there is an orbit of length r ($r < k$). It can be assumed that $q_0 q_r$ is a line of this orbit.

The transformation α^r must fix this line $q_0 q_r$. So $\alpha^r(q_0 q_r) = q_r q_{2r} = q_0 q_r$. Equivalently $2r \equiv 0 \mod k$. This shows that $r = k/2$.

The lines $q_i q_{k/2+i} (i = 0, \ldots, k/2-1)$ constitute an orbit of size $k/2$ since these lines are fixed by $\alpha^{k/2}$. □

Remark 4.1. Lemma 4.1 and Theorem 4.1 imply that there exists an orbit (of points) of size $k/2$.

THEOREM 4.2. *The cyclic group G fixes exactly one point r and exactly one line M of $PG(2, q)$. This point r is the center and the line M is the axis of the involutory perspectivity $\alpha^{k/2}$.*

Proof.

- Part 1: Let r be a point of $PG(2, q)$ which is fixed by G. This point r does not belong to a unisecant of K. For assume that $r q_0$ is a unisecant of K.

Then $\alpha(rq_0) = rq_1$ is also a unisecant of K. Continuing in this way shows that all lines rq_i ($i = 0, \dots, k-1$) are unisecants of K. So r extends K to a $(k+1)$-arc. This contradicts the assumption that K is complete. This means that r belongs to $k/2$ bisecants of K.

The $k(k-1)/2$ bisecants of K partition, under G, into $(k-2)/2$ orbits of size k and one orbit of size $k/2$. This point r cannot belong to a bisecant of K in one of those orbits of size k. Otherwise, r would belong to k bisecants of K. So r belongs to the bisecants of K in that orbit of size $k/2$. This shows that r is the intersection of the lines $q_iq_{k/2+i}(i = 0, \dots, k/2-1)$. So, if a point r of $PG(2, q)$ is fixed by G, then r belongs to the lines $q_iq_{k/2+i}(i = 0, \dots, k/2-1)$. Consequently, G can fix at most one point of $PG(2, q)$.

- Part 2: The bisecants $q_iq_{k/2+i}(i = 0, \dots, k/2-1)$ constitute (under G) an orbit (of lines) of size $k/2$. It now follows from Theorem 4.1 that there exists an orbit O (of points) of size $k/2$.

  The transformation $\alpha^{k/2}$ fixes O point by point. Assume that O contains a 4-arc. The projective transformation $\alpha^{k/2}$ is then the identity. This is false since α is a generator of a cyclic group of order k.

  So O does not contain a 4-arc. There exists a line M which has at least 3 points in common with O. Hence, $\alpha^{k/2}$ fixes M point by point. This signifies that $\alpha^{k/2}$ is a perspectivity with axis M and with a center c. The line M and the point c are the axis and center of the unique involution $\alpha^{k/2}$ in G. Hence, G must fix c and M. It now follows from Part 1 that G fixes exactly one point $r = c$ of $PG(2, q)$. Theorem 4.1 then shows that G fixes exactly one line M of $PG(2, q)$. □

THEOREM 4.3. *In $PG(2, q)$, q even, no cyclic complete k-arcs with k even, exist.*

Proof. It follows from Theorem 4.2 that $\alpha^{k/2}$ is a perspectivity with axis M and with center r where M and r are fixed by α. But $\alpha^{k/2}$ is an involution. So $\alpha^{k/2}$ is an elation since q is even [2, p. 172]. Hence $r \in M$. The elation $\alpha^{k/2}$ only fixes the points on the axis M. So, all the points of $PG(2, q)$ which belong to an orbit to size $k/2$ (under G) must belong to this line M. This line M contains at least one orbit of size $k/2$ (see Remark above).

Now, α induces an element α' (of $PGL(2, q)$) on the line M. The order of α' must be $k/2$ since M contains an orbit of size $k/2$ and since $\alpha^{k/2}$ is the identity on M. Assume that G has an orbit O of size t, $1 < t < k/2$, on M. (G fixes only one point r on M, see Theorem 4.2). Then α^t fixes r and the $t \geq 2$ points of M in that orbit O. Hence α^t fixes M point by point, so α^t is a perspectivity with axis M and center r_1. This center r_1 does not belong to K since the points of K constitute one orbit (under G) of size k. The perspectivity α^t fixes K. So it can only interchange the points of K on a bisecant through r_1 and it must fix the points of K on a tangent through r_1. Then α^{2t} fixes K point by point. Equivalently $\alpha^{2t} = 1$ or $k|2t$. This is false. Therefore, the q points of $M\backslash\{r\}$ partition into orbits of size $k/2$. This implies that $(k/2)|q$. Consider the element

α' of $PGL(2, q)$. Then

$$\alpha' : t \mapsto \frac{at+b}{ct+d} \; (ad + bc \neq 0)$$

$(t \in GF(q)^+; GF(q)^+ = GF(q) \cup \{\infty\}; \infty \notin GF(q))$.
This transformation α' fixes one point of M. Assume that $\alpha'(\infty) = \infty$. Then $c = 0$ and $\alpha' : t \mapsto at + b$ (assume $d = 1$). Assume $a \neq 1$. Then $\alpha'^2 : t \mapsto a^2 t + ab + b$. In general, $\alpha'^i : t \mapsto a^i t + b_i$ for some element b_i of $GF(q)$. But $\alpha'^{k/2} = 1$. Hence $a^{k/2} = 1$. Let u be the order of a. Then $u|(k/2)$, so $u|q$. But $u|(q-1)$. Hence $u = 1$. Therefore $a = 1$ and $\alpha' : t \mapsto t + b$. So $\alpha'^2 : t \mapsto t + 2b = t$. This means that $2 = k/2$. This contradicts $k \geq 8$. We always obtain a contradiction. There are no cyclic complete k-arcs in $PG(2, q)$, q even, for which k is even. □

THEOREM 4.4. *Let K be a cyclic complete k-arc (k even) in $PG(2, q)$, q odd, which is fixed by a cyclic projective group G of order k. Let r and M be the unique point and line which are fixed by G. Then $r \notin M$ and G partitions M into orbits of size $k/2$. So $(k/2)|(q+1)$.*

Proof. The transformation $\alpha^{k/2}$ is an involutory perspectivity with axis M and center r (see Theorem 4.2). Since q is odd, $\alpha^{k/2}$ is a homology. So $r \notin M$ [2, p. 172]. Hence, α does not fix any point of M in $PG(2, q)$. But α induces an element α' of $PGL(2, q)$ on M. So α' fixes 2 conjugate points r_1, r_2 of M in a quadratic extension of $PG(2, q)$.

The subgroup H of $PGL(2, q)$ which fixes the two conjugate points r_1, r_2 of M in $PG(2, q^2) \backslash PG(2, q)$ is a cyclic subgroup H of order $q + 1$, acting transitively on the points of M in $PG(2, q)$. The homology $\alpha^{k/2}$ fixes M point by point. So α' partitions M into orbits of size at most $k/2$. There is at least one orbit O in $PG(2, q)$ of size $k/2$ (4.1). The points of this orbit O are fixed by $\alpha^{k/2}$. So O is contained in M.

Assume that there exists an orbit of length t $(1 < t < k/2)$ on M. Then α'^t fixes the t points of M in this orbit and α'^t also fixes r_1 and r_2. So α'^t fixes M point by point. By using the same reasoning as in the proof of Theorem 4.3, we obtain $t \geq k/2$. This contradicts $t < k/2$. Hence, α' partitions M into orbits of size $k/2$. Therefore $(k/2)|(q+1)$. □

Remark 4.2. Assume again that q is odd. The cyclic group G fixes one point r and one line M with $r \notin M$. It also fixes the conjugate points r_1, r_2 of M in a quadratic extension of $PG(2, q)$. Assume $i^2 = d_1$ with d_1 a nonsquare of $GF(q)$. Choose the reference system in such a way that $r(1, 0, 0), M : X_0 = 0, r_1(0, 1, i)$ and $r_2(0, 1, -i)$. Consider all conics C such that $(1, 0, 0) \notin C$, $(0, 1, i)$, $(0, 1, -i) \in C$ and such that r and M are pole and polar line with respect to C. Then

$$C : X_0^2 - cd_1 X_1^2 + cX_2^2 = 0$$

with c a certain nonzero element of $GF(q)$.

All projective transformations α of $PGL(3, q)$ which fix r, M and which fix the points r_1, r_2 on M are of type

$$\alpha : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & d_1 b & a \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \text{ with } (a, b) \neq (0, 0).$$

Let

$$\alpha^{-1} : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & a' & b' \\ 0 & d_1 b' & a' \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}.$$

Then α maps the conic C onto

$$\alpha(C) : X_0^2 - cd_1(a'^2 - b'^2 d_1)X_1^2 + c(a'^2 - b'^2 d_1)X_2^2 = 0.$$

So α fixes the conic C if and only if $a'^2 - b'^2 d_1 = \det(\alpha^{-1}) = 1$. This means, when $\det(\alpha) = 1$. From now on, we will work with affine coordinates $x = x_1$ and $y = x_2$. Then $(x, y) \equiv (1, x_1, x_2)$, $r(0, 0)$, M is the line at infinity and C : $1 - cd_1 X^2 + cY^2 = 0$, $c \in GF(q)\backslash\{0\}$.
Then

$$\alpha : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ d_1 b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

and α fixes C if and only if $\det(\alpha) = 1$.

The conics C : $1 - cd_1 X^2 + cY^2 = 0$ are concentric ellipses w.r.t. the origin.

THEOREM 4.5. *Let K be a cyclic, complete k-arc in $PG(2, q)$, q odd, with k even ($k > 8$). Then K lies in an affine plane $AG(2, q)$ and (i) K is an ellipse; or (ii) K is the disjoint union of $k/2$ points on an ellipse C_1 and $k/2$ points on an ellipse C_2 where C_1 and C_2 are concentric.*

Proof. Let $G = \langle\alpha\rangle$ be the cyclic projective group of K with involutory homology $\alpha^{k/2}$ (4.4). Choose the reference system as prescribed in 4.2. Then $\alpha^{k/2}$ must be

$$\alpha^{k/2} : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Here is $\det(\alpha^{k/2}) = 1 = (\det(\alpha))^{k/2}$. Hence, the order v of $\det(\alpha)$ divides $k/2$. It follows from Theorem 4.4 that $(k/2)|(q + 1)$. So $v|(q + 1)$. But $v|(q - 1)$ since $\det(\alpha)$ is an element of $GF(q)$. Therefore $v|(q + 1, q - 1)$, which implies that $v|2$. So $\det(\alpha) = 1$ or $\det(\alpha) = -1$. If $\det(\alpha) = 1$, then α fixes the ellipses $C : 1 - cd_1 X^2 + cY^2 = 0$ ($c \neq 0$; see 4.2). So all orbits, not contained in the line at infinity and different from $\{r\}$, are a subset of an ellipse. The orbit K is a complete k-arc, which is contained in an ellipse. So K is an ellipse.

If $\det(\alpha) = -1$, then α maps the ellipse $C_1 : 1 - cd_1X^2 + cY^2 = 0$ onto $C_2 : 1 + cd_1X^2 - cY^2 = 0$, but α^2 fixes C_1 ($c \neq 0$; see Remark 4.2).

Hence, the complete k-arc K consists of $k/2$ points on an ellipse $C_1 : 1 - cd_1X^2 + cY^2 = 0$ and $k/2$ points on $C_2 : 1 + cd_1X^2 - cY^2 = 0$ where c is a certain nonzero element of $GF(q)$. These ellipses C_1 and C_2 are concentric w.r.t. the origin. □

THEOREM 4.6. *Let K be a cyclic, complete k-arc in $PG(2, q)$, q odd, k even, consisting of $k/2$ points on two conics. Then $q \equiv -1 \mod 4$ and $k \equiv 0 \mod 8$.*

Proof. Let G be the cyclic projective group of order k which fixes K. Choose the reference system as indicated in Remark 4.2. Assume furthermore that K consists of $k/2$ points on the ellipse $C_1 : 1 - cd_1X^2 + cY^2 = 0$ and $k/2$ points on $C_2 : 1 + cd_1X^2 - cY^2 = 0$ ($c \neq 0$) (see the proof of Theorem 4.5). The involution $\alpha^{k/2} : (x, y) \mapsto (-x, -y)$ fixes K (see the proof of Theorem 4.5). Here $\det(\alpha^{k/2}) = 1$, so $\alpha^{k/2}$ fixes C_1 and C_2 (Remark 4.2). This involution $\alpha^{k/2}$ fixes C_1 and the 2 conjugate points r_1, r_2 of C_1 on the line at infinity. The conic C_1 is fixed by a sharply 3-transitive projective group G_1. The subgroup H_1 (of G_1) which fixes these conjugate points r_1, r_2 of C_1 on the line at infinity is a cyclic group of order $q+1$, acting in one orbit on the $q+1$ points of C_1. So $\alpha^{k/2}$ is an element of order 2 in H_1 and $\alpha^{k/2}$ partitions C_1 into $(q+1)/2$ orbits of size 2. But $\alpha^{k/2}$ fixes K. Hence, $\alpha^{k/2}$ fixes $K \cap C_1$. So $2|(k/2)$ where $k/2 = |K \cap C_1|$. This shows that $k \equiv 0 \mod 4$. Hence, $\alpha^{k/4}$ exists. Let

$$\alpha^{k/4} : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ d_1b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

with

$$\begin{pmatrix} a & b \\ d_1b & a \end{pmatrix} \begin{pmatrix} a & b \\ d_1b & a \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

So $2ab = 0$ and $a^2 + d_1b^2 = -1$.

Assume $b = 0$. Then $a^2 = -1$. This implies $q \equiv 1 \mod 4$. Let $a = \omega$ with $\omega^2 = -1$. (Note that $\omega \in GF(q)$.) Then $\alpha^{k/4} : (x, y) \mapsto (\omega x, \omega y)$. This means that $\alpha^{k/4}$ is a homology of order 4, with center $r(1, 0, 0)$ and with axis the line at infinity, which fixes K.

So K consists of k points on $k/4$ lines through $r(0, 0)$. This contradicts the definition of a k-arc. Therefore $b \neq 0$. Hence $a = 0$ and $d_1b^2 = -1$. Consequently, -1 is a nonsquare of $GF(q)$. This shows that $q \equiv -1 \mod 4$.

Since d_1 and -1 are nonsquare, select $d_1 = -1$. Then $b \in \{1, -1\}$ and $\alpha^{k/4} : (x, y) \mapsto (y, -x)$ or $\alpha^{k/4} : (x, y) \mapsto (-y, x)$. In both cases, $\det(\alpha^{k/4}) = 1$. So $\alpha^{k/4}$ fixes the conics C_1 and C_2. The transformation $\alpha^{k/4}$ is an element of the cyclic subgroup H_1 (see also in this proof). This implies that $\alpha^{k/4}$ acts on the conic C_1 in orbits of size 4. But $\alpha^{k/4}$ also fixes $K \cap C_1$. So $4|(k/2)$. Hence $k \equiv 0 \mod 8$. □

LEMMA 4.2. *Let K be a cyclic complete k-arc in $PG(2, q)$, k even, $q \equiv -1 \mod 4$, consisting of $k/2$ points on 2 conics. Then it can be assumed that K consists of $k/2$ points on $C_1 : 1 + X^2 + Y^2 = 0$ and $k/2$ points on $C_2 : 1 - X^2 - Y^2 = 0$.*

Proof. This arc K consists of $k/2$ points on $C_1 : 1 - cd_1X^2 + cY^2 = 0$ and $k/2$ points on $C_2 : 1 + cd_1X^2 - cY^2 = 0$ with $c \neq 0$ and d_1 nonsquare in $GF(q)$ (Theorem 4.5). Since $q \equiv -1 \mod 4$, select $d_1 = -1$, so $C_1 : 1 + cX^2 + cY^2 = 0$ and $C_2 : 1 - cX^2 - cY^2 = 0$.

Assume that c is a square (if c is a nonsquare, then $-c$ is a square). The homology $\beta : (x, y) \mapsto (dx, dy)$ with $d^2 = c$ maps C_1 onto $\beta(C_1) : 1 + X^2 + Y^2 = 0$ and C_2 onto $\beta(C_2) : 1 - X^2 - Y^2 = 0$. □

In the following theorem, we again introduce homogeneous coordinates.

THEOREM 4.7. *Let K be a cyclic complete k-arc (k even) consisting of $k/2$ points on the 2 conics $C_1 : X_0^2 + X_1^2 + X_2^2 = 0$ and $C_2 : X_0^2 - X_1^2 - X_2^2 = 0$ in $PG(2, q)$, $q \equiv -1$ mod 4. Assume that K contains $(1, 1, 0)$ and suppose that the cyclic group G (which fixes K) is generated by*

$$\alpha : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & -b \\ 0 & b & a \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}, \ (a^2 + b^2 = -1).$$

Then K is fixed by the involution $\gamma : (x_0, x_1, x_2) \mapsto (x_0, x_2, x_1)$ which interchanges $r_1(0, 1, i)$ and $r_2(0, 1, -i)$ $(i^2 = -1)$.

Proof.

- Part 1: (Note that, with respect to Remark 4.2, the values of b and $-b$ are interchanged in the matrix of α). We can assume that K contains $(1, 1, 0)$ since C_2 is fixed by a sharply 3-transitive projective group [5, p. 233].
  Let $(1, a_j, b_j)$ $(j = 0, \ldots, k-1)$ be the points of K. Choose the indices j such that $(1, 1, 0) = (1, a_0, b_0)$ and such that $(1, a_j, b_j)^\alpha = (1, a_{j+1}, b_{j+1})$ (indices modulo k). Identify $(1, a_j, b_j)$ with (a_j, b_j) and with the element $a_j + ib_j$ of $GF(q^2)$.
  Then $\alpha(1, 1, 0) = (1, a_1, b_1) = (1, a, b) = a_1 + ib_1 = a + ib$.
- Part 2: For all indices j $(0 \le j \le k-1)$ is $(a + ib)^j = a_j + ib_j$. This is proven by induction on j.

$$(a + ib)^0 = 1 = (1, 0) = a_0 + ib_0$$
$$(a + ib)^1 = a + ib = a_1 + ib_1 \quad \text{(see Part 1)}.$$

Suppose that $(a+ib)^j = a_j + ib_j = (a_j, b_j)$. Then $(a+ib)^{j+1} = (a_j+ib_j)(a+ib) = aa_j - bb_j + i(ab_j + ba_j)$ $(i^2 = -1)$. But $a_j + ib_j$ corresponds to $(1, a_j, b_j)$

and $(1, a_j, b_j)^\alpha = (1, aa_j - bb_j, a_jb + b_ja) = (1, a_{j+1}, b_{j+1})$ (Part 1). Hence $(a + ib)^{j+1} = a_{j+1} + ib_{j+1}$.

- Part 3: Part 2 shows that the points of K can be identified with the powers of $a + ib$. A point $(1, a_j, b_j)$ of K either belongs to C_1 or C_2. If $(1, a_j, b_j) \in C_1$ (resp. C_2), then $a_j^2 + b_j^2 = -1$ (resp. $a_j^2 + b_j^2 = 1$). The arc K contains k points. So $(a + ib)^k = 1$ and $(a + ib)^j \neq 1$ for $0 < j < k$. Since $k \equiv 0 \bmod 8$ (Theorem 4.6), the following equalities hold:

$$(a + ib)^{k/2} = -1$$
$$(a + ib)^{k/4}, (a + ib)^{3k/4} \in \{i, -i\}.$$

Assume that $(a + ib)^{k/4} = i$ (The possibility $(a + ib)^{3k/4} = i$ gives analogous results). Then $(a + ib)^{3k/4} = -i$.
Assume that $(1, a_j, b_j) \in C_1$, then $(a_j + ib_j)(b_j + ia_j) = -i$. So $b_j + ia_j = (a + ib)^{3k/4-j}$. Analogously, if $(1, a_j, b_j) \in C_2$, then $(a_j + ib_j)(b_j + ia_j) = i$. So $b_j + ia_j = (a + ib)^{k/4-j}$. In both cases, $b_j + ia_j$ is a power of $a + ib$. So $(1, b_j, a_j)$ is also a point of K. Hence, if $(1, a_j, b_j) \in K$, then $(1, b_j, a_j) \in K$. This proves that K is fixed by γ. □

COROLLARY 4.1. *Let K be a cyclic complete k-arc in $PG(2, q)$, k even, $q \equiv -1 \bmod 4$, consisting of $k/2$ points on the conics $C_1 : X_0^2 + X_1^2 + X_2^2 = 0$ and $C_2 : X_0^2 - X_1^2 - X_2^2 = 0$. Then K is fixed by a semidihedral projective group of order $2k$.*

Proof. Let K consist of $k/2$ points on $C_1 : X_0^2 + X_1^2 + X_2^2 = 0$ and $k/2$ points on $C_2 : X_0^2 - X_1^2 - X_2^2 = 0$ and assume that $(1, 1, 0) \in K$. Then K is fixed by a cyclic group of order k which fixes the 2 points $(0, 1, i)$ and $(0, 1, -i)$ ($i^2 = -1$) (see Remark 4.2). But K is also fixed by an involution γ which interchanges $(0, 1, i)$ and $(0, 1, -i)$ (Theorem 4.7) and, by using the matrices of α and γ (see Theorem 4.7), $\gamma\alpha\gamma^{-1} = \alpha^{(k/2)-1}$. Hence, K is fixed by a semidihedral projective group of order $2k$ (This is a group of order $2k$ (k even) generated by two elements α and γ where α is an element of order k and where γ is an involution such that $\gamma\alpha\gamma^{-1} = \alpha^{(k/2)-1}$). □

Remark 4.3. Alternative proofs of some of the theorems of this section could be provided by using the results of Pickert, particularly [13, Proposition 3]. Possibility (ii) of Theorem 4.5 does occur. The cyclic complete 8-arc in $PG(2, 11)$ (see 2.3) is of this type.

Here follow some new examples of cyclic k-arcs K in $PG(2, q)$, $k \equiv 0 \bmod 8$, $q \equiv -1 \bmod 4$, which are the disjoint union of $k/2$ points on two conics. Most of them are however incomplete.

The arcs always consist of $k/2$ points on the conics $C_1 : X_0^2 + X_1^2 + X_2^2 = 0$ and $C_2 : X_0^2 - X_1^2 - X_2^2 = 0$. Furthermore, K always contains $(1, 1, 0)$. The arc K is fixed by the cyclic group generated by

$$\alpha : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & -b & a \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

where $(1, a, b)$ is the first point of K and if $K = \{q_0, \ldots, q_{k-1}\}$, then $q_i^\alpha = q_{i+1}$ (indices modulo k). Finally, K is fixed by the involution $\gamma : (x_0, x_1, x_2) \mapsto (x_0, x_2, x_1)$.

(1) An incomplete 8-arc K in $PG(2, 19)$.

$$K = \{(1, 3, 3), (1, 18, 0), (1, 16, 3), (1, 0, 18), (1, 16, 16), (1, 1, 0), (1, 3, 16), (1, 0, 1)\}.$$

There are 56 points of $PG(2, 19)$ which extend K to a 9-arc, 8 of which belong to the line $X_0 = 0$ fixed by the cyclic group. For instance, the point (0, 1, 2) extends K to a larger arc.

(2) A complete 16-arc K in $PG(2, 23)$.

$$K = \{(1, 2, 8), (1, 22, 0), (1, 21, 8), (1, 14, 9), (1, 8, 21), (1, 0, 1), (1, 8, 2), (1, 9, 9), (1, 21, 15), (1, 1, 0), (1, 2, 15), (1, 9, 14), (1, 15, 2), (1, 0, 22), (1, 15, 21), (1, 14, 14)\}.$$

(3) A complete 24-arc K in $PG(2, 59)$.

$$K = \{(1, 10, 28), (1, 58, 0), (1, 49, 28), (1, 35, 29), (1, 41, 18), (1, 29, 35), (1, 31, 10), (1, 0, 58), (1, 31, 49), (1, 30, 35), (1, 41, 41), (1, 24, 29), (1, 49, 31), (1, 1, 0), (1, 10, 31), (1, 24, 30), (1, 18, 41), (1, 30, 24), (1, 28, 49), (1, 0, 1), (1, 28, 10), (1, 29, 24), (1, 18, 18), (1, 35, 30)\}.$$

(4) An incomplete 32-arc K in $PG(2, 239)$.

$$K = \{(1, 50, 75), (1, 238, 0), (1, 189, 75), (1, 18, 91), (1, 77, 93), (1, 70, 70), (1, 146, 162), (1, 91, 18), (1, 164, 50), (1, 0, 238), (1, 164, 189), (1, 148, 18), (1, 146, 77), (1, 169, 70), (1, 77, 146), (1, 221, 91), (1, 189, 164), (1, 1, 0), (1, 50, 164), (1, 221, 148), (1, 162, 146), (1, 169, 169), (1, 93, 77), (1, 148, 221), (1, 75, 189), (1, 0, 1), (1, 75, 50), (1, 91, 221), (1, 93, 162), (1, 70, 169), (1, 162, 93), (1, 18, 148)\}.$$

This arc is extended by 4672 = 146·32 points, 128 of which belong to $X_0 = 0$, of $PG(2, 239)$ to a 33-arc. The point (1, 192, 53) is one of those points which extend K to a larger arc.

(5) An incomplete 40-arc in $PG(2, 179)$.

$$K = \{(1, 35, 57), (1, 178, 0), (1, 144, 57), (1, 55, 52), (1, 56, 117), (1, 37, 8), (1, 140, 140), (1, 171, 142), (1, 117, 56), (1, 127, 124), (1, 57, 144), (1, 0, 1), (1, 57, 35), (1, 52, 124), (1, 117, 123), (1, 8, 142), (1, 140, 39), (1, 142, 8), (1, 56, 62), (1, 124, 52), (1, 144, 122), (1, 1, 0), (1, 35, 122), (1, 124, 127), (1, 123, 62), (1, 142, 171), (1, 39, 39), (1, 8, 37), (1, 62, 123), (1, 52, 55), (1, 122, 35), (1, 0, 178), (1, 122, 144), (1, 127, 55), (1, 62, 56), (1, 171, 37), (1, 39, 140), (1, 37, 171), (1, 123, 117), (1, 55, 127)\}.$$

Only two orbits of the cyclic group on the line $X_0 = 0$ extend K to a 41-arc. Hence exactly 40 points of $PG(2, 179)$ extend K to a 41-arc. The points (0, 1, 128) and (0, 1, 83) are the representatives of these orbits. By selecting two of these 40 points, K extends to a complete 42-arc, so K is extendable in precisely $40 \cdot 39/2 = 780$ ways to a complete 42-arc.

(6) An incomplete 48-arc K in $PG(2, 311)$.

$$K = \{(1, 69, 84), (1, 310, 0), (1, 242, 84), (1, 118, 85), (1, 43, 307), (1, 143, 155), (1, 184, 238), (1, 33, 33), (1, 73, 127), (1, 155, 143), (1, 4, 268), (1, 85, 118), (1, 227, 69), (1, 0, 310), (1, 227, 242), (1, 226, 118), (1, 4, 43), (1, 156, 143), (1, 73, 184), (1, 278, 33), (1, 184, 73), (1, 168, 155), (1, 43, 4), (1, 193, 85), (1, 242, 227), (1, 1, 0), (1, 69, 227), (1, 193, 226), (1, 268, 4), (1, 168, 156), (1, 127, 73), (1, 278, 278), (1, 238, 184), (1, 156, 168), (1, 307, 43), (1, 226, 193), (1, 84, 242), (1, 0, 1), (1, 84, 69), (1, 85, 193), (1, 307, 268), (1, 155, 168), (1, 238, 127), (1, 33, 278), (1, 127, 238), (1, 143, 156), (1, 268, 307), (1, 118, 226)\}.$$

The point (1, 231, 260) extends K to a larger arc. In total, there are 960 points in the plane which extend K to a 49-arc, 96 of which are points on the line $X_0 = 0$.

(7) An incomplete 56-arc K in $PG(2, 307)$.

$$K = \{(1, 19, 49), (1, 306, 0), (1, 288, 49), (1, 198, 20), (1, 137, 195), (1, 185, 62), (1, 106, 95), (1, 222, 295), (1, 253, 253), (1, 12, 85), (1, 95, 106), (1, 245, 122), (1, 195, 137), (1, 287, 109), (1, 49, 288)$$

(1, 0, 1), (1, 49, 19), (1, 20, 109), (1, 195, 170), (1, 62, 122),
(1, 95, 201), (1, 295, 85), (1, 253, 54), (1, 85, 295), (1, 106, 212),
(1, 122, 62), (1, 137, 112), (1, 109, 20), (1, 288, 258), (1, 1, 0),
(1, 19, 258), (1, 109, 287), (1, 170, 112), (1, 122, 245), (1, 201, 212),
(1, 85, 12), (1, 54, 54), (1, 295, 222), (1, 212, 201), (1, 62, 185),
(1, 112, 170), (1, 20, 198), (1, 258, 19), (1, 0, 306), (1, 258, 288),
(1, 287, 198), (1, 112, 137), (1, 245, 185), (1, 212, 106), (1, 12, 222),
(1, 54, 253), (1, 222, 12), (1, 201, 95), (1, 185, 245), (1, 170, 195),
(1, 198, 287)}.

This arc can be extended by 168 points, 56 of which lie on the line $X_0 = 0$, to a 57-arc. For instance, the point (1, 218, 260) extends K to a larger arc.

Acknowledgment

The authors wish to thank the referees for helpful remarks in the preparation of the final version of the paper. The authors are respectively senior research assistant and senior research associate of the National Fund for Scientific Research (Belgium).

References

1. E. Boros and T. Szönyi, "On the sharpness of a theorem of B. Segre," *Combin.* **6** (3) (1986), 261–268.
2. P. Dembowski, *Finite Geometries*, Springer-Verlag, New York, 1968.
3. J.C. Fisher, J.W.P. Hirschfeld, and J.A. Thas, "Complete arcs in planes of square order," *Ann. Discrete Math.* **30** (1986), 243–250.
4. J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, Oxford, England, 1979.
5. J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford University Press, Oxford, England, 1985.
6. J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries*, Oxford University Press, Oxford, England, 1991.
7. D.R. Hughes and F. Piper, *Projective Planes*, Springer-Verlag, Berlin, 1973.
8. B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.
9. B.C. Kestenband, "A family of complete arcs in finite projective planes," *Colloq. Math* LVII (1989), 59–67.
10. L. Lombardo-Radice, "Sul problema dei k-archi completi di $S_{2,q}$," *Boll. Un. Mat. Ital.* **11** (1956), 178–181.
11. C.M. O'Keefe and T. Penttila, "A new hyperoval in $PG(2, 32)$," *J. Geom.* **44** (1992), 117–139.
12. T. Penttila and I. Pinneri, "Irregular hyperovals in $PG(2, 64)$," *J. Geom*, to appear.
13. G. Pickert, "Free mobility in affine planes," *Proc. of the Conference on Algebra and Geometry*, Kuwait, (1981), 153–157.
14. A.R. Sadeh, "Classification of k-arcs in $PG(2, 11)$ and cubic surfaces in $PG(3, 11)$," Ph. D. thesis, University of Sussex, England, 1984.

15. B. Segre, *Lectures on Modern Geometry*. Cremonese, Roma, 1961.
16. B. Segre, "Ovali e curve σ nei piani di Galois di caratteristica due," *Atti dell' Accad. Naz. Lincei Rend.* **32** (8) (1962), 785–790.