Innovations in Incidence Geometry
Volume 6-7 (2007-2008), Pages 203–209
ISSN 1781-6475

ACADEMIA
PRESS

Arcs in cyclic affine planes

Vincenzo Giordano

Abstract

In a cyclic affine plane of order n with $n \equiv 1 \pmod 4$, we construct a new family of k-arcs of size $k = \frac{1}{2}(n+7)$ containing $\frac{1}{2}(n+3)$ points from an oval.

Keywords: difference set, cyclic affine planes, arcs, ovals

MSC 2000: 05B10, 51E21, 51E15

1 Introduction

In a projective plane Π of order n, an *arc* is defined to be a set of points no three of which are collinear. If the arc consists of $k \geq 3$ points, it is called a k-arc. An arc not contained in a larger one is said to be complete. The $(n+1)$-arcs are called *ovals*.

Arcs in the projective plane $\mathsf{PG}(2,q)$ coordinatized by a finite field $\mathsf{GF}(q)$ of order q and their generalizations in higher dimensional projective spaces $\mathsf{PG}(n,q)$ are also relevant in Coding Theory, arcs and maximum distance separable codes being equivalent objects.

By a well known result due to B. Segre, $\frac{1}{2}(n+3)$ is the maximum number of points that an arc in a projective plane Π of odd order n can share with an oval $\mathcal{C}$ of Π. If the maximum is attained by a k-arc $\mathcal{K}$, then $\mathcal{K}$ seems to contain only a few points outside $\mathcal{C}$. In $\mathsf{PG}(2,q)$, this emerged from previous work by B. Segre, L. Lombardo-Radice, G. Pellegrino, G. Korchmáros and A. Sonnino; see [4, 5, 6, 7, 9].

It is also known, that if $k = \frac{1}{2}(n+5)$ and $|\mathcal{K} \cap \mathcal{C}| = \frac{1}{2}(n+3)$, then $\mathcal{K}$ is complete in almost all cases, that is, the probability of finding such a k-arc which is not complete is equal to zero. This suggests that the problem of constructing k-arcs for $k \geq \frac{1}{2}(n+7)$ that share $\frac{1}{2}(n+3)$ points with $\mathcal{C}$ may be difficult. Nevertheless, such k-arcs are know to exist in $\mathsf{PG}(2,q)$.

In this paper, Π is the projective closure of an affine cyclic plane of order $n \equiv 1 \pmod 4$; this includes the case $\Pi = \mathsf{PG}(2,n)$ for a prime power n. Our main goal is the construction of a new k-arc $\mathcal{K}$ with $k = \frac{1}{2}(n+7)$ such that $\mathcal{K}$ contains exactly $\frac{1}{2}(n+3)$ points from an oval $\mathcal{C}$. In [4], the completeness of $\mathcal{K}$ was proven for $\Pi = \mathsf{PG}(2,n)$ with $\frac{1}{2}(n+1)$ prime and $n^2 \equiv 1 \pmod{16}$. However, the problem of proving (or disproving) the completeness of $\mathcal{K}$ for the general case remains open and appears to be rather difficult.

Our method is different from the approaches used in the above cited papers, as it depends on basic algebraic number theory which enters to play through the concept of difference sets.

2 Preliminary results

Let Σ be an affine plane of order n admitting a collineation τ such that the cyclic group G generated by τ leaves one point (say ∞) fixed and acts regularly on the set of all remaining points of Σ. Such an affine plane is called a *cyclic affine plane*; see [2]. The order of the collineation τ is $v = n^2 - 1$. Furthermore, if p_0 denotes any point of Σ other than ∞, then each point p of Σ other than ∞ can be written uniquely as $p = \tau^i(p_0)$, where $\bar{i}$ is an element of the cyclic additive group $\mathbb{Z}_v$. In this way, the points of Σ other than ∞ can be identified with the elements of $\mathbb{Z}_v$. Let R be any line of Σ not incident to the point ∞ and let N be the unique subgroup of $\mathbb{Z}_v$ of order $n-1$. Then the lines of Σ can be identified with the following subsets of $\mathbb{Z}_v$:

(i) the cosets $N + \overline{x}$ together with the point ∞ with $\overline{x} \in \mathbb{Z}_v$;

(ii) the translates $R + \overline{y}$ of R with $\overline{y} \in \mathbb{Z}_v$.

Using the terminology of Design Theory, R is an *affine difference set* of order n; more precisely R is an $(n+1, n-1, n, 1)$-difference set in $\mathbb{Z}_v$ relative to N. This means that every $\overline{g} \in \mathbb{Z}_v \backslash N$ has exactly one representation

$$\overline{g} = \overline{r_1 - r_2}, \quad \text{with} \quad r_1, r_2 \in R, \quad r_1 \neq r_2,$$

but no nonidentity element of N has such a representation. In this paper, by a *translation* of a cyclic affine plane Σ (of order n) we shall always mean a collineation τ_a mapping $\overline{x}$ to $\overline{x+a}$ for all $\overline{x} \in \mathbb{Z}_v$, $\overline{a} \in \mathbb{Z}_v$ and fixing ∞. Let t be an integer such that the mapping $\phi_t : \overline{x} \mapsto \overline{tx}$, $\infty \mapsto \infty$ is a collineation of Σ. Such an integer t is called a *multiplier* of the plane Σ. It is known that every positive divisor of n is a multiplier of Σ; see [8]. If Π denotes the projective closure of Σ, the infinite line L_∞ consists of the points $\rho(\overline{x})$ of $\mathbb{Z}_v/N$, where ρ denotes the canonical epimorphism from $\mathbb{Z}_v$ onto $\mathbb{Z}_v/N$. If n is odd, the numerical multiplier ϕ_n is an involutory $(\rho(\overline{t}), N)$-homology, where $\rho(\overline{t})$ is the unique involution in $\mathbb{Z}_v/N$; if n is even, ϕ_n is an involutorial $(\rho(\overline{0}), N)$-elation; see [8]. It is known that $\mathsf{AG}(2, q)$ is a cyclic affine plane; see [1]. For a non-square element $s \in \mathsf{GF}(q)$, the point (ξ, η) of $\mathsf{AG}(2, q)$ is identified with the element $z = \xi + \sigma\eta$, $\sigma^2 = s$, in the quadratic extension $\mathsf{GF}(q^2)$ of $\mathsf{GF}(q)$ arising from the irreducible polynomial $X^2 - s$. Let α be a primitive element of $\mathsf{GF}(q^2)$. The map $\tau : z \mapsto \alpha z$ induces a linear collineation of $\mathsf{AG}(2, q)$. In fact, if $\alpha = \alpha_1 + \sigma\alpha_2$ and $z = z_1 + \sigma z_2$, then

$$z' = \alpha z = (\alpha_1 + \sigma\alpha_2)(z_1 + \sigma z_2) = \alpha_1 z_1 + s\alpha_2 z_2 + \sigma(\alpha_1 z_2 + \alpha_2 z_1)$$

is equivalent to

$$\begin{pmatrix} z_1' \\ z_2' \end{pmatrix} = \begin{pmatrix} \alpha_1 & s\alpha_2 \\ \alpha_2 & \alpha_1 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}.$$

Then the collineation τ is such that the cyclic group generated by τ fixes the point $(0, 0)$ and acts regularly on the set of all other points of $\mathsf{AG}(2, q)$. If we choose the point $(1, 0)$ as base point, then every point (ξ, η) other than $(0, 0)$ can be written uniquely as $(\xi, \eta) = \tau^i(1, 0)$, where $\overline{i} \in \mathbb{Z}_v$, $v = q^2 - 1$: in this way we obtain a *cyclic model* of $\mathsf{AG}(2, q)$ in which (ξ, η) is identified with $\overline{i} \in \mathbb{Z}_v$ and $(0, 0)$ with ∞.

3 An oval in a cyclic affine plane

First we construct an oval in the projective closure of a cyclic affine plane.

Theorem 3.1. *Let Σ be a cyclic affine plane of order n ($v = n^2 - 1$) and Π its projective closure. Then the set*

$$\Omega := \{\overline{0}, \overline{(n-1)}, \ldots, \overline{n(n-1)}\}$$

is an oval of the plane Π.

Proof. For each $i = 0, 1, \ldots, n$ let f_i be the right translation

$$f_i(\overline{x}) := \overline{x + i(n-1)}$$

for all $\overline{x} \in \mathbb{Z}_v$. Let be $\varepsilon_i := f_i\phi_n$, where ϕ_n is the collineation of Π corresponding to the numerical multiplier n. It is easy to check that for each i, the collineation ε_i is an involution. In fact, if $\overline{x} \in \mathbb{Z}_v$, then

$$\varepsilon_i^2(\overline{x}) = \overline{n^2x + in(n-1) + i(n-1)} = \overline{x}\,.$$

We consider the case of odd and even order separately. Let n be odd. In this case, we prove that ε_i is an involutory homology with center $\rho(\overline{t-i})$ and axis $N-\bar{i}$, where $\rho(\bar{t})$ is the unique involution in $\mathbb{Z}_v/N$. For $i=0$, the assertion is true because $\varepsilon_0=\phi_n$ is an involutory $(\rho(\bar{t}),N)$-homology. If $i\in\{1,\dots,n\}$, we prove that ε_i fixes $N-\bar{i}$ pointwise. In fact, if $\overline{h(n+1)-i}\in N-\bar{i}$, then

$$\varepsilon_i(\overline{h(n+1)-i})=\overline{hn(n+1)-in+i(n-1)}=\overline{hn(n+1)-i}=\overline{h(n+1)-i}\,.$$

So ε_i is an involutory perspectivity and then an homology; see [3]. Its center is $\rho(\overline{t-i})$. To show this, observe that the center of ε_i is a point at infinity because the infinite line is fixed by ε_i; see [3]. Now it is enough to prove that ε_i fixes the line $N+\overline{t-i}$ through the point $\rho(\overline{t-i})$. Note that ϕ_n fixes the line $N+\bar{t}$:

$$\phi_n(N+\bar{t})=N+\bar{t}\,. \tag{1}$$

Let $\overline{h(n+1)+t-i}\in N+\overline{t-i}$. By (1), there exists an integer s such that

$$\overline{hn(n+1)+nt}=\overline{s(n+1)+t}\,. \tag{2}$$

Therefore

$$\varepsilon_i(\overline{h(n+1)+t-i})=\overline{hn(n+1)+nt-in+i(n-1)}=\overline{hn(n+1)+nt-i}\,.$$

By (2) it follows that

$$\varepsilon_i(\overline{h(n+1)+t-i})=\overline{s(n+1)+t-i}\in N+\overline{t-i}\,.$$

Let n be even. In this case $\varepsilon_0=\phi_n$ is an involutorial $(\rho(\bar{0}),N)$-elation. We prove that, for each $i=0,1,\dots,n$, ε_i is an involutorial elation with center $\rho(\overline{-i})$ and axis $N-\bar{i}$. If $\overline{h(n+1)-i}\in N-\bar{i}$, then

$$\varepsilon_i(\overline{h(n+1)-i})=\overline{hn(n+1)-i}=\overline{h(n+1)-i}\,.$$

Hence ε_i fixes $N-\bar{i}$ pointwise and so it is an involutory perspectivity. As a consequence, ε_i is an elation and its center (which is necessarily a point at infinity) is $\rho(\overline{-i})$.

It turns out that $\varepsilon_0,\varepsilon_1,\dots,\varepsilon_n$ are $n+1$ involutory perspectivities with *distinct* centers and axes.

Now we are in a position to prove that the above defined set Ω is an oval. The lines of the plane Π, other than the infinite line L_∞, are the traslates of R and the cosets of N. It follows that, if λ, μ and ν are three distinct integers of the set $\{0,1,\dots,n\}$, with $\lambda<\mu<\nu$, then

$$\overline{\lambda(n-1)},\quad \overline{\mu(n-1)}\quad\text{and}\quad \overline{\nu(n-1)}\quad\text{are collinear}$$

if and only if

$$\overline{0}, \quad \overline{(\mu-\lambda)(n-1)} \quad \text{and} \quad \overline{(\nu-\lambda)(n-1)} \quad \text{are collinear}\,.$$

First of all note that, if n is odd, then the line N contains only two points of Ω, namely $\overline{0}$ and $\frac{1}{2}(n+1)(n-1)$. If n is even, the line N contains only one point of Ω, namely $\overline{0}$. Let h and k be two distinct integers of the set $\{1,\dots,n\}$. Assume on the contrary that the three points

$$\overline{0}, \qquad \overline{h(n-1)}, \qquad \overline{k(n-1)}$$

are collinear. Let L be the line on which these three points lie. From the last remark, L must be necessarily a translate $R-\overline{r_i}$ for some $\overline{r_i} \in R$. Clearly

$$\overline{h(n-1)} = \varepsilon_h(\overline{0})$$

and

$$\overline{k(n-1)} = \varepsilon_k(\overline{0}).$$

Therefore

$$\varepsilon_h(L) = \varepsilon_h([\overline{0},\varepsilon_h(\overline{0})]) = [\varepsilon_h(\overline{0}),\varepsilon_h^2(\overline{0})] = [\varepsilon_h(\overline{0}),\overline{0}] = L\,.$$

In the same way we see that

$$\varepsilon_k(L) = L.$$

Finally L is a line fixed by both ε_h and ε_k and different from the axes of ε_h and ε_k. Then the centers of ε_h and ε_k must lie on L. But this is a contradiction since ε_h and ε_k have distinct centers (points at infinity). □

Corollary 3.2. *Let Σ be a cylic affine plane of order n. Then the oval*

$$\Omega := \{\overline{0}, \overline{(n-1)}, \dots, \overline{n(n-1)}\}$$

defined in the Theorem 3.1, is preserved by all multipliers of Σ.

4 An $(n+7)/2$-arc arising from an oval

In this section we investigate arcs in the projective closure Π of a cyclic affine plane Σ of order n, with $n \equiv 1 \pmod 4$. Let Ω be the oval defined in Theorem 3.1. Our aim is to determine a point-set $\mathcal{U}$ of size $\frac{1}{2}\,(n+3)$ lying on Ω with the following property: $\mathcal{U}$ can be extended to an $\frac{1}{2}\,(n+7)$-arc by adding two points at infinity.

Theorem 4.1. *Let $n \equiv 1 \pmod 4$. In Π, the point-set*

$$\mathcal{K} := \left\{ \overline{0}, \overline{2(n-1)}, \dots, \overline{\frac{(n-5)(n-1)}{2}}, \overline{\frac{(n-1)(n-1)}{2}}, \overline{\frac{(n+1)(n-1)}{2}}, \overline{\frac{(n+5)(n-1)}{2}}, \dots, \overline{(n-2)(n-1)}, \overline{n(n-1)}, \rho\left(\overline{\frac{n+1}{2}}\right), \rho\left(\overline{\frac{n+5}{2}}\right) \right\}$$

is an arc of size $\frac{1}{2}(n+7)$ containing $\frac{1}{2}(n+3)$ points of the oval Ω.

Proof. For each $j = 1, \dots, \frac{n-1}{2}$ let S_j be the line of Π through the points $\overline{j(n-1)}$ and $\overline{(n-j+1)(n-1)}$. From the congruence

$$jn(n-1) \equiv (n-j+1)(n-1) \pmod v$$

the collineation ϕ_n fixes the line S_j. Since ϕ_n is an involutory $(\rho(\overline{\frac{n+1}{2}}), N)$-homology, see Theorem 3.1, the lines fixed by ϕ_n are the axis N and all the lines through the center $\rho(\overline{\frac{n+1}{2}})$. Therefore, the $\frac{n-1}{2}$ lines through $\rho(\overline{\frac{n+1}{2}})$ and the chords of Ω are just the above defined lines S_j.

For each $k = 0, \dots, \frac{n-3}{2}$, let R_k be the line of Π through $\overline{k(n-1)}$ and $\overline{(n-k-1)(n-1)}$. From the congruence

$$kn(n-1) + (n-1)(n-1) \equiv (n-k-1)(n-1) \pmod v$$

the collineation ε_{n-1} fixes the line R_k. Since ε_{n-1} is an involutory $(\rho(\overline{\frac{n+5}{2}}), N - \overline{n-1})$-homology, see Theorem 3.1, the $\frac{n-1}{2}$ lines through $\rho(\overline{\frac{n+5}{2}})$ which are 2-secant of Ω are just the above defined lines R_k. Finally, the lines through $\rho(\overline{\frac{n+1}{2}})$ and $\rho(\overline{\frac{n+5}{2}})$ which are 2-secant of Ω meet Ω in two points a and b such that

- a and b are both even or odd multiples of $\overline{n-1}$,
- $a \in \mathcal{K} \cap \Omega$ and $b \in \overline{\mathcal{K}} \cap \Omega$.

This completes the proof. □

We remark that the translation $f_{(n+1)/2}$ mapping $\overline{x}$ to $\overline{x + v/2}$, is an involutory (L_∞, ∞)-homology preserving the oval Ω and leaving $\mathcal{K}$ invariant.

Remark 4.2. It has been conjectured that every cyclic affine plane is desarguesian, and this has been proven for affine cyclic planes of order $n \leq 1000$. If π is the projective closure $\mathsf{PG}(2, n)$ of the affine plane $\mathsf{AG}(2, n)$ with $n \equiv 1 \pmod 4$, by the famous Segre's theorem, the oval Ω defined in Theorem 3.1 is a conic.

Then, the point-set $\mathcal{K}$ defined in Theorem 4.1 is a k-arc of size $k = \frac{1}{2}(n+7)$ containing $\frac{1}{2}(n+3)$ points from a conic. For $n \leq 337$ (with the only exception of $n = 17$), an exhaustive computer aided computation shows that $\mathcal{K}$ is complete. If $n = 17$, $\mathcal{K}$ can be extended to a 14-arc by adding two other points outside Ω; so we obtain a complete arc sharing ten points with the conic Ω and containing four points outside the conic.

References

[1] **R.C. Bose**, An affine analogue of Singer's theorem, *J. Indian Math. Soc.* **6** (1942), 1–15.

[2] **A.J. Hoffman**, Cyclic affine planes, *Can. J. Math.* **4** (1952), 295–301.

[3] **D.R. Hughes** and **F. Piper**, *Projective Planes*, Springer Verlag, GTM **6**, 1973.

[4] **G. Korchmáros** and **A. Sonnino**, Complete arcs arising from conics, *Discrete Math.* **267** (2003), 181–187.

[5] **L. Lombardo-Radice**, Sul problema dei k-archi completi in $S_{2,q}$ ($q = p^t$, p primo dispari), *Boll. Un. Mat. Ital.* (3) **11** (1956), 178–181.

[6] **G. Pellegrino**, Un'osservazione sul problema dei k-archi completi in $S_{2,q}$, con $q \equiv 1 \pmod 4$, *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* (8) **63** (1977), no. 1-2, 33–44.

[7] ______, On complete arcs in the plane PG$(2,q)$, with q odd, containing $(q+3)/2$ points of a conic, *Rend. Mat. Appl.* (7) **12** (1992), no. 3, 649–674.

[8] **A. Pott**, *Finite Geometry and Character Theory*, Lecture Notes **1601**, Springer, Berlin/Heidelberg/New York, 1995.

[9] **B. Segre**, Curve razionali normali e k-archi negli spazi finiti, *Ann. Mat. Pura Appl.* (4) **39** (1955), 357–379.

Vincenzo Giordano

Dipartimento di Matematica, Università degli Studi di Bari, Via Orabona 4, I-70125 Bari, Italy

e-mail: vin.giordano@libero.it