# Doubly transitive parabolic ovals in affine planes of even order $n \leq 64$

Gábor Korchmáros
gabor.korchmaros@unibas.it

Angelo Sonnino
angelo.sonnino@unibas.it

Dipartimento di Matematica e Informatica
Università della Basilicata
Campus Macchia Romana
Viale dell'Ateneo Lucano, 10
85100 Potenza - Italy

**Abstract**

All parabolic ovals in affine planes of even order $q \leq 64$ which are preserved by a collineation group isomorphic to $A\Gamma L(1,q)$ are determined. They are either parabolas or translation ovals.

## 1 Introduction

In an affine plane $\alpha$ of order $n$, a *parabolic oval* is point-set contained in an oval in the projective closure $\overline{\alpha}$ of $\alpha$. In other words, a parabolic oval in $\alpha$ extends to an oval in $\overline{\alpha}$ by adding a point at infinity. As the classical example of an oval is the irreducible conic in the projective Desarguesian plane, so the classical example of a parabolic oval is the parabola in the Desarguesian affine plane.

A parabolic oval $\Omega$ of $\alpha$ is called *doubly transitive* if the collineation group of $\alpha$ which preserves $\Omega$ induces a doubly transitive permutation group on the set of all points of $\Omega$. The known examples of doubly transitive parabolic ovals are the parabolas in Desarguesian planes, the translation ovals in the Desarguesian planes of even order, and the ovals consisting of the absolute points of an orthogonal polarity in commutative twisted field planes of odd order. The problem of finding other examples or prove their non-existence is still open.

In this paper, affine planes of even order $n$ with a doubly transitive parabolic oval $\Omega$ are considered. For this case, Biliotti, Jha and Johnson

**ARS COMBINATORIA 105(2012)**, pp. 419-433

[1] showed that $n$ is a power of 2 and that the collineation group preserving $\Omega$ is a subgroup of $\mathrm{A\Gamma L}(1,n)$. Concerning translation planes of even order, Biliotti, Jha and Johnson used their result to characterise the Desarguesian plane as the unique generalised twisted field plane—as well as the unique André plane—which contains a doubly transitive parabolic oval. They also proved that the Desarguesian plane is the unique affine plane of even order $n \neq 64$ containing two distinct doubly transitive parabolic ovals with two distinct common affine points. The smallest putative non Desarguesian plane of even order with a doubly transitive parabolic oval has order 32. Our main result is the proof of the following theorem.

**Theorem 1.** *Let $\Omega$ be a doubly transitive parabolic oval in an affine plane $\alpha$ of order $q \leq 64$. If the collineation group of $\alpha$ preserving $\Omega$ is $\mathrm{A\Gamma L}(1,q)$ then $\alpha$ is Desarguesian and $\Omega$ is either a parabola or a translation oval.*

# 2 Conics and translation ovals in Desarguesian planes of even order

From results due to Segre [14], Payne [10] and, independently, Hirschfeld [5], in the affine Desarguesian plane of order $q = 2^h$ every parabolic oval preserved by a translation group of order $n$ acting on its points as a sharply transitive permutation group has the following equation in a suitable coordinate system:

$$Y = X^{2^n} \tag{1}$$

with $\gcd(n,h) = 1$. Let $\Omega$ denote such a parabolic oval. When $n = 1$ or $n = h-1$, $\Omega$ is a parabola; otherwise $\Omega$ is called a (proper) translation oval. The collineation group $G$ of $\alpha$ preserving $\Omega$ consists of all collineations

$$\begin{cases} x' = ax^{2^t} + b \\ y' = a^{2^n} y^{2^t} + b^{2^n} \end{cases}$$

with $a, b \in \mathrm{GF}(q)$, $a \neq 0$, and $t \in \{0, 1, \ldots, h-1\}$. Therefore, $G \cong \mathrm{A\Gamma L}(1,q)$ and $G$ acts on the affine points of $\Omega$ as $\mathrm{A\Gamma L}(1,q)$ in its usual doubly transitive permutation representation on the affine line over $\mathrm{GF}(q)$.

# 3 Abstract ovals

Let $\Omega$ be a parabolic oval in an affine plane $\alpha$ of even order $n$. In the projective closure $\overline{\alpha}$ of $\alpha$, let $Y_\infty$ denote the unique point of $\Omega$ at infinity. Since the line at infinity $\ell_\infty$ is tangent to $\Omega$, the nucleus of $\Omega$, say $X_\infty$, is also a point at infinity. Each affine point $P$ of $\alpha$ external to $\Omega$ may be identified by an involutory permutation $\varphi_P$ on the set of affine points of $\Omega$. The fixed points of $\varphi_P$ are the points $A, B$ such that $\{P, X_\infty, A\}$ and $\{P, Y_\infty, B\}$ are collinear triples, while $(C, D)$ is a transposition in $\varphi_P$ if and only if $\{P, C, D\}$ is a collinear triple, see Figure 1.

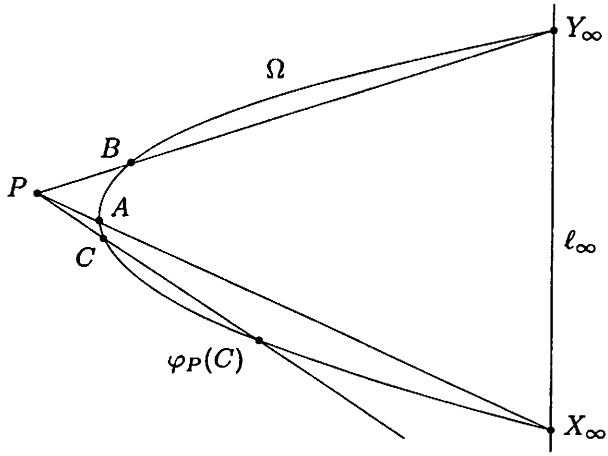


Figure 1: The involution $\varphi_P$ on $\Omega$

For two distinct points $P, Q$ of $\alpha$ both outside $\Omega$ the product $\varphi = \varphi_Q\varphi_P$ may have a few fixed points. In general, $\varphi$ has at most two fixed points, with some exceptions, namely

(I) $\varphi$ has at three fixed points when $PQ$ is a chord of $\Omega$ and either $\{Q, X_\infty, B\}$ or $\{Q, Y_\infty, A\}$ but not both are collinear triples.

(II) $\varphi$ has four fixed points when $PQ$ is a chord of $\Omega$ and both $\{Q, X_\infty, B\}$ and $\{Q, Y_\infty, A\}$ are collinear triples.

Let $g$ be any collineation of $\alpha$ preserving $\Omega$. If $P$ is an affine point external to $\Omega$ and $P' = g(P)$, then $\varphi'_P = g\varphi_P g^{-1}$. In particular, the collineation group $G$ of $\alpha$ preserving $\Omega$ has a natural action on the set

$$\mathcal{P} = \{\varphi_p \mid P \in \alpha; P \notin \Omega\},$$

see Figure 2.

Let $\Phi = \{\phi_P \mid P \in \alpha \setminus \Omega\}$. The pair $(\Omega, \Phi)$ is called a parabolic abstract oval. Two abstract parabolic ovals $(\Omega, \Phi)$ and $(\Omega, \Phi')$ are called isomorphic if there is a permutation $\rho \in \mathrm{Sym}(\Omega)$ such that $\Phi' = \rho\Phi\rho^{-1}$.

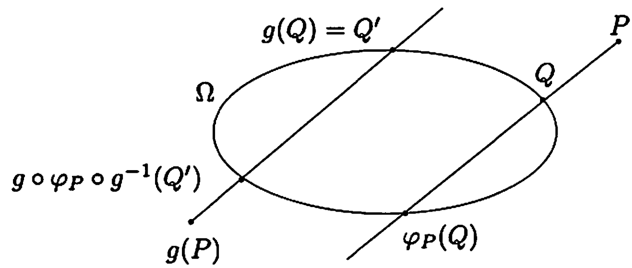


Figure 2: The action of a collineation of $\Omega$ on its involutory permutations

**Lemma 2.** *In the Desarguesian plane* $\mathrm{AG}(2,q)$ *let* $\Omega$ *be a parabola and* $(\Omega,\Phi)$ *the associated abstract parabolic oval. If* $(\Omega,\Phi')$ *is an abstract parabolic oval of an affine plane* $\alpha$ *of order* $q$ *then* $(\Omega,\Phi) \cong (\Omega,\Phi')$ *implies* $\alpha \cong \mathrm{AG}(2,q)$.

*Proof.* This is a corollary to a theorem due to Bruen and Thas [2], and independently to Segre and Korchmáros [15], see also [8]. □

**Lemma 3.** *Let* $\Omega$ *be a parabolic oval in* $\alpha$*. A collineation group* $G$ *of* $\alpha$ *preserving* $\Omega$ *is doubly transitive on the set of points of* $\Omega$ *if and only if it acts transitively on* $\mathcal{P}$*. Further,* $G$ *is sharply doubly transitive on the set of affine points of* $\Omega$ *if and only if it is sharply transitive on* $\mathcal{P}$.

*Proof.* It may be that some collineation in $G$ interchanges $X_\infty$ and $Y_\infty$. If this is the case, let $H$ be the subgroup of $G$ of index two which consists of all collineations fixing both $X_\infty$ and $Y_\infty$.

Suppose that $G$ is doubly transitive on $\Omega$. Then

$$|G| = |\Omega|(|\Omega|-1)|G_{A,B}|$$

for any two distinct points $A, B \in \Omega$. We show that $H$ is still doubly transitive on $\Omega$. Since $H$ is a normal subgroup of $G$, $H$ is transitive on $\Omega$. Hence

$$|H| = |\Omega||\Omega'||H_{A,B}|$$

where $\Omega'$ is the orbit of $B$ under the stabiliser $H_A$ of $A$ in $H$. Since $|G| = 2|H|$ and $H_{A,B}$ is a subgroup of $G_{A,B}$, this implies that either $|G_{A,B}| = 2|H_{A,B}|$ and $|\Omega| = |\Omega'|$ or $G_{A,B} = H_{A.B}$ and $|\Omega| - 1 = 2|\Omega'|$. Actually, the latter case cannot occur as $|\Omega|$ is even. Therefore, $|\Omega| - 1 = |\Omega'|$ showing that $H$ is also doubly transitive.

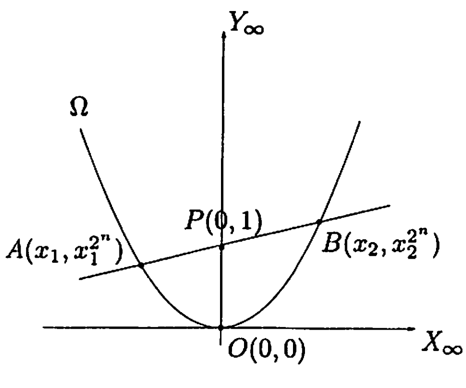


Figure 3: The oval in affine coordinates

Now, let $P, P'$ be two points external to $\Omega$. Let $A, B$ be the fixed points of $\varphi_P$ and arrange the notation such that $A = PX_\infty \cap \Omega$ and $B = PY_\infty \cap \Omega$. Define $A'$ and $B'$ similarly.

Doubly transitivity of $H$ on $\Omega$ implies the existence a collineation $h \in H$ that sends $A$ to $A'$ and $B$ to $B'$. Since $h$ fixes both $X_\infty$ and $Y_\infty$, we see that $h$ sends $P$ to $P'$.

Conversely, if $G$ is transitive on $\mathcal{P}$ then some collineation $g \in G$ sends the unordered pair $\{A, B\}$ to the unordered pair $\{A', B'\}$. Therefore $G$ is doubly-homogeneous on $\Omega$. Since $|\mathcal{P}| = n(n-1)$ is even, this implies the doubly transitivity of $G$ on $\Omega$, by a result due to W.M. Kantor [7], see also [6, Theorem 6.5].

Since $\mathcal{P}$ and a sharply doubly transitive group of degree $n$ have the same size $n(n-1)$, the second part of the claim is a straightforward consequence of the first part. □

**Corollary 4.** *Let $\Omega$ be a parabolic oval in an affine plane $\alpha$ of order $q = 2^h$. Suppose that a collineation group $G$ of $\alpha$ preserving $\Omega$ is isomorphic to* $\mathrm{A\Gamma L}(1,q)$. *If $G$ acts on $\Omega$ as* $\mathrm{A\Gamma L}(1,q)$ *in its doubly transitive permutation representation on the affine line over the Galois field* $\mathrm{GF}(q)$, *then the subgroup of $G$ isomorphic to* $\mathrm{AGL}(1,q)$ *acts on the points of $\alpha$ outside $\Omega$ as a sharply transitive permutation group.*

# 4 Doubly transitive parabolic ovals in affine planes of order $q = 2^h$

With the notation as in the previous section, assume that $\alpha$ has order a power of 2, say $q = 2^h$. Then the affine points of $\Omega$ may be identified with the elements of the Galois field GF$(q)$. Doing so, the involutory permutations in $\mathcal{P}$ are certain mappings on GF$(q)$, and hence each $\varphi_P$ has a polynomial representation over GF$(q)$. In the Desarguesian plane, such polynomials can be computed directly. Choose an appropriate affine frame as in Figure 3 where

$$\Omega = \{ (x, x^{2^n}, 1) \mid x \in \mathrm{GF}(q) \},$$

and consider its involutory permutation $\varphi_P$, with $P = (0,1)$. Projecting $\Omega$ onto itself from $P$, collinearity of the points $A$, $B$ and $P$ with $A, B \in \Omega$ and $A \neq B$ yields

$$(x_1 + x_2)^{2^n - 1} = \frac{x_1^{2^n} + x_2^{2^n}}{x_1 + x_2} = \frac{x_2^{2^n} + 1}{x_2}, \tag{2}$$

from which

$$(x_1 + x_2)^{(2^n - 1)u} = \left(\frac{x_1^{2^n} + 1}{x_1}\right)^u \quad \text{with } u \in \mathbb{Z},.$$

On the other hand

$$(x_1 + x_2)^{(2^n - 1)v} \quad \text{with } v \in \mathbb{Z}.$$

Therefore,

$$(x_1 + x_2)^{(2^n - 1)u + (2^n - 1)v} = \left(\frac{x_1^{2^n} + 1}{x_1}\right)^u. \tag{3}$$

To put (3) in a suitable form, we use the following well known result [13].

**Lemma 5.** *For every prime integer p,*

$$p^{\gcd(n,h)} - 1 = \gcd(p^n - 1, p^h - 1).$$

Lemma 5 applied to $p = 2$ together with the condition $\gcd(n, h) = 1$ imply $\gcd(2^n - 1, 2^h - 1) = 1$. Choose $u, v \in \mathbb{Z}$ such that $(2^n - 1)u + (2^h - 1)v = 1$; from (3),

$$x_2 = \left(\frac{x_1^{2^n} + 1}{x_1}\right)^u + x_1. \tag{4}$$

Finally, using (4) and $x^{2^n - 2} = x^{-1}$ for $x \in \mathrm{GF}(q)$ and $x \neq 0$, a polynomial $F^n$ representing $\varphi_A$ on $\Omega : Y = X^{2^n}$ is

$$F^{(n)}(X) = \left(X^{2^h - 2}(X^{2^n} + 1)\right)^u + X \qquad \text{if } u \geq 0; \tag{5}$$

$$F^{(n)}(X) = \left(X(X^{2^n} + 1)^{2^h - 2}\right)^{-u} + X \qquad \text{if } u < 0. \tag{6}$$

Reducing the powers of $X$ modulo $2^h - 1$, this becomes a polynomial $F^{(n)}(X) \in \mathrm{GF}(2)[X]$ with $\deg F^{(n)}(X) \le 2^n - 1$ and $F^{(n)}(0) = 0$, $F^{(n)}(1) = 1$. Note that $\Omega$ is a parabola if and only if either $n = 1$ and $F^{(1)}(X) = X^{2^h-2}$, or $n = h - 1$ and $F^{(h-1)}(X) = \left(X(X^{2^{h-1}} + 1)^{2^h-2}\right)^2 + X$, with $u = -2$ and $v = 1$.

**Lemma 6.**

$$F^{(h-1)}(X) = \left(\sum_{i=1}^{(2^h-2)/2} X^i\right)^2.$$

*Proof.* We need to show that

$$\left(X(X^{2^{h-1}} + 1)^{2^h-2}\right)^2 + X = X^2 + X^4 + \cdots + X^{2^h-2}.$$

Expanding the left side of the above equality, we obtain

$$\left(X(X^{2^{h-1}} + 1)^{2^h-2}\right)^2 + X = \left(\frac{1}{X}(X^{2^{h-1}} + 1)\right)^{-2} + X =$$

$$\frac{X^2}{(X^{2^{h-1}} + 1)^2} + X = \frac{X^2}{X+1} + X = \frac{X^2}{X+1} + X = \frac{X}{X+1}.$$

Put $X + 1 \mapsto t$. From $\frac{X}{X+1}. = \frac{t+1}{t} = 1 + \frac{1}{t} = 1 + t^{2^h-2}$ we obtain

$$\frac{X}{X+1} = 1 + (X+1)^{2^h-2} = 1 + \sum_{i=0}^{2^h-2} \binom{2^h-2}{i} X^i,$$

and hence the claim. □

If $n = 2$ then $u = -\frac{1}{3}(2^h - 2)$, $v = 1$ and hence by (6)

$$F^{(2)}(X) = \left(X(X^8 + 1)^{2^{h-1}-1}\right)^{\frac{1}{3}(2^h-2)} + X.$$

If $n = h - 2$ then $u = \frac{1}{3}(2^h - 5)$, $v = -\frac{1}{3}(2^{h-2} - 2)$ and hence by (5)

$$F^{(h-2)}(X) = \left(X^{2^h-2}(X^{2^{h-2}} + 1)\right)^{\frac{1}{3}(2^h-5)} + X.$$

# 5 Polynomials

The above discussion suggests an approach to the study of collineation groups of parabolic ovals in any affine plane $\alpha$ of order $q = 2^h$ by means of the polynomials representing the involutory permutations in $\mathcal{P}$. As far as the collineation group is large enough—and the order of the plane is small enough—an exhaustive search of such polynomials may be possible. The aim is to work out this approach for doubly transitive parabolic ovals preserved by $\mathrm{A\Gamma L}(1,q)$. To do this, label such a doubly transitive parabolic oval $\Omega$ with the elements of $\mathrm{GF}(q)$ so that $\mathrm{A\Gamma L}(1,q)$ consists of all semilinear permutations on $\Omega$

$$X \longmapsto \alpha X^{\sigma} + \beta$$

with $\alpha, \beta \in \mathrm{GF}(2^h)$, $\alpha \neq 0$, $\sigma \in \mathrm{Aut}\,\mathrm{GF}(2^h)$.

As in Section 3, let $P$ be the common point of the lines $OY_\infty$ and $EX_\infty$ where $O$ and $E$ are the points of $\Omega$ associated to the elements 0 and 1 of $\mathrm{GF}(q)$. Let $F(X)$ be a permutation polynomial representing the involutory permutation $\varphi_P$. Then

(i) $\deg F(X) < q$

(ii) $F(0) = 0$, $F(1) = 1$;

(iii) $F(F(x)) = x$ for every $x \in \mathrm{GF}(2^h)$;

(iv) $F(x) \neq x$ for every $x \in \mathrm{GF}(2^h) \setminus \{0,1\}$;

Two further properties of $F(X)$ are described in the following result.

**Lemma 7.**

(v) $F(X) \in \mathrm{GF}(2)[X]$.

(vi) *For any $\alpha, \beta \in \mathrm{GF}(q)$ with $\alpha \neq \beta$ and $\alpha \neq 0$ the equation $F(\alpha X + \beta) = \alpha F(X) + \beta$ has at most two solutions in* $\mathrm{GF}(2^h)$

*Proof.* The map $\epsilon : x \mapsto x^2$ is in $\mathrm{A\Gamma L}(1,q)$ and it fixes both 0 and 1. Therefore, the corresponding collineation $g \in G$ fixes the points $O$ and $E$. Since $g$ fixes $X_\infty$ and $Y_\infty$, the point $P$ is also fixed by $g$. Hence, the permutations $\varphi_P$ and $\epsilon$ commute, see Figure 2. In terms of $F(X)$, this means that $F(x^2) = F(x)^2$ for every $x \in \mathrm{GF}(q)$. By (i), this implies the polynomial equation $F(X^2) = F(X)^2$ whence (v) follows.

To show (vi), assume on the contrary that $x_1, x_2, x_3 \in \mathrm{GF}(q)$ are pairwise distinct solutions of the equation (vi) for some $\alpha, \beta \in \mathrm{GF}(q)$ with $\alpha \neq 0$. Then, for $i = 1,2,3$,

$$\frac{f(\alpha x_i + \beta) - \beta}{\alpha} = f(x_i). \tag{7}$$

The permutation $\delta : x \mapsto ax + b$ is in AGL$(1,q)$. The corresponding collineation $g$ in $G$ sends $O$ and $E$ to the points $A$ and $B$ associated to $\beta$ and $\alpha + \beta$, respectively. Therefore, if $Q$ is the image of $P$ under $g$, and $G(X)$ the polynomial representing $\varphi_Q$, then

$$G(X) = \frac{F(\alpha X + \beta) - \beta}{\alpha}.$$

From (7),

$$G(x_i) = F(x_i) \quad \text{for} \quad i = 1, 2, 3. \tag{8}$$

Note that as both $a, b$ are supposed to be distinct from $0, 1$, neither (I) nor (II) occurs. Since $\varphi_P$ and $\varphi_Q$ are the projections of $\Omega$ onto itself from $P$ and $Q$, (8) yields $P = Q$. But then Lemma 4 implies that $\delta$ is the identity of AGL$(1,q)$. □

Property (v) of Lemma 7 is required for if an involution $\varphi \in$ A$\Gamma$L$(1,q)$ is to map $\Omega$ onto itself, then the coefficients of the corresponding $F(X)$ must be preserved by any $\sigma \in$ Aut GF$(q)$.

# 6 A$\Gamma$L$(1,q)$-invariant doubly transitive parabolic ovals in affine planes of even order $q \leq 64$

Since $q$ is a power of 2, the possibilities for $q$ are $2, 4, 8, 16, 32$ and $64$. The case $q = 2$ is trivial. If the plane is desarguesian and the parabolic oval is a parabola, then it is doubly transitive with collineation group A$\Gamma$L$(1,q)$. This is the case for every parabolic oval when $q = 4$.

## Case $q = 8$

Up to isomorphism, the unique affine plane of order 8 is AG$(2,8)$, see [3]. In AG$(2,8)$, there exist parabolic ovals which are not parabolas. In the projective closure PG$(2,8)$, each of these consists of seven points of a conic $C$ together with the nucleus $N$ of $C$. Since any collineation of PG$(2,8)$ preserving a subset of seven points of $C$ must preserve the conic, it follows that any collineation preserving a parabolic oval fixes a point of it. Therefore, the unique doubly transitive parabolic ovals in AG$(2,8)$ are the parabolas.

## Case $q = 16$

The classification project of planes of order 16 is still in progress. There are known twenty-two examples, up to isomorphisms, see [9, 11, 12]. Just one of them, the Desarguesian plane, is consistent with our hypotheses. This is confirmed by the following result.

**Theorem 8.** *Let $\alpha$ be an affine plane of order* 16 *containing a doubly transitive parabolic oval $\Omega$. If a collineation group $G \cong$ AGL(1,16) of $\alpha$ preserving $\Omega$ acts on the affine points of $\Omega$ as* AGL(1,16) *in its doubly transitive permutation group, then $\alpha$ is the Desarguesian plane and $\Omega$ is a parabola.*

*Proof.* An exhaustive search performed by GAP [4] showed that here are 13 polynomials $F_j(X)$ for which Properties (i)–(v) hold:

$$F_1(X) = X^4 + X^9 + X^{10} + X^{12} + X^{14};$$
$$F_2(X) = X^2 + X^{11} + X^{14};$$
$$F_3(X) = X^4 + X^5 + X^7 + X^{10} + X^{11} + X^{13} + X^{14};$$
$$F_4(X) = X + X^2 + X^5 + X^7 + X^8 + X^{10} + X^{11} + X^{13} + X^{14};$$
$$F_5(X) = X + X^2 + X^3 + X^4 + X^6 + X^9 + X^{11} + X^{12} + X^{14};$$
$$F_6(X) = X^2 + X^3 + X^4 + X^5 + X^6 + X^7 + X^8 + X^9 + X^{10} + X^{11} + X^{12} + X^{13} + X^{14};$$
$$F_7(X) = X + X^3 + X^4 + X^5 + X^8 + X^{12} + X^{14};$$
$$F_8(X) = X + X^3 + X^5 + X^6 + X^8 + X^{10} + X^{14};$$
$$F_9(X) = X^5 + X^8 + X^{14};$$
$$F_{10}(X) = X + X^4 + X^6 + X^9 + X^{14};$$
$$F_{11}(X) = X^2 + X^4 + X^6 + X^8 + X^{10} + X^{12} + X^{14} = \left(\sum_{i=1}^{7} X^i\right)^2;$$
$$F_{12}(X) = X + X^2 + X^5 + X^6 + X^{10} + X^{12} + X^{14};$$
$$F_{13}(X) = X^{14};$$

but only $F_{11}(X)$ and $F_{13}(X)$ satisfy also Property (vi). Since $F_{11}(X) = F^{(3)}(X)$ by Lemma 6, the claim follows □

## Case $q = 32$

Using the approach described in Case $q = 16$, an exhaustive search performed by GAP returned only four polynomials satisfying all the properties (i)–(vi), namely:

$$F_1(X) = X^{30};$$
$$F_2(X) = X^{22} + X^{24} + X^{30};$$
$$F_3(X) = X^{10} + X^{12} + X^{14} + X^{16} + X^{26} + X^{28} + X^{30};$$
$$F_4(X) = \left(\sum_{i=1}^{15} X^i\right)^2.$$

They represent all the possible doubly transitive parabolic ovals of order 32 admitting the prescribed collineation group. Comparing the polynomials $F_1$, $F_2$, $F_3$ and $F_4$ with those obtained by Equality (5) and using Lemma 6, we find the following correspondence:

| Polynomial | Oval | Type |
|---|---|---|
| $F_1(X)$ | $Y = X^2$ | parabola |
| $F_2(X)$ | $Y = X^8$ | translation oval |
| $F_3(X)$ | $Y = X^4$ | translation oval |
| $F_4(X)$ | $Y^2 = X$ | parabola |

This proves the following result.

**Theorem 9.** *Let $\alpha$ be an affine plane of order 32 containing a doubly transitive parabolic oval $\Omega$. If a collineation group $G \cong \mathrm{AGL}(1,32)$ of $\alpha$ preserving $\Omega$ acts on the affine points of $\Omega$ as $\mathrm{AGL}(1,32)$ in its doubly transitive permutation group, then $\alpha$ is the Desarguesian plane and $\Omega$ is either a parabola or a translation oval.*

## Case $q = 64$

An exhaustive search using the above approach is also possible, although some more effort is needed to exploit thoroughly the properties in Lemma 7. The essential idea is to use (v) in its equivalent form

(vii) If $g$ is the permutation on $\Omega$ induced by $\sigma : X \mapsto X^2$ then $g$ and $\varphi_P$ commute.

After identifying $\Omega$ with the set $\{1, 2, \ldots, 64\}$, the group $\mathrm{A\Gamma L}(1,64)$ may be assumed to be the collineation group of $\pi$ acting on $\Omega$ as the permutation group generated by

$$g_1 = (1,64,48,19,54,13,49,6,11,2,17,36,27,63,26,34,9,58,42,31,50)$$
$$(3,60,62,40,43,20,10,39,35,23,51,24,4,47,41,14,12,22,15,37,33)$$
$$(5,25,28,59,61,56,8,30,52,46,55,53,7,21,38,44,16,45,32,29,18);$$
$$g_2 = (1,34,16,29,6,28,48,20,52,38,73,36,22,54,27,47,55,46,58,41,2,$$
$$13,57,33,25,43,60,4,53,7,56,9,8,44,3,26,62,15,23,39,17,50,24,$$
$$11,35,51,59,12,49,63,30,40,32,19,5,21,45,14,31,10,42,18,61);$$
$$g_3 = (1,27,24,26,13,45)(2,5,10,48,60,29)(3,41,32,21,18,37)(4,28,25,$$
$$61,22,23)(6,57,31)(7,38,8,47,35,39)(9,54,17)(11,15,43,34,55,59)$$
$$(12,51,50,44,46,49)(14,16,58,30,40,19)(20,53)(33,42,52,56,36,62)$$

Doing so, the subgroup AGL$(1,64)$ of A$\Gamma$L$(1,64)$ is the collineation group acting on $\Omega$ as the permutation group generated by $g_1$ and $g_2$. Since the fixed points of $g_3$ are 63 and 64, we may assume that $A = 64$, $B = 63$. Therefore, the fixed points of $\varphi_P$ are 64 and 65. Also, $g_3^2$ is a planar collineation of order 4 fixing the points $20, 53, 64, 63$. Since $g^2$ and $\varphi_P$ commute, this implies that $\varphi_P(20) = 53$, $\varphi_P(53) = 20$.

Furthermore, $g = g_3^3$ is a Baer involution fixing the points 6, 9, 17, 31, 54, 57, 63 and 64. Let $\overline{\pi}$ be the (affine) Baer subplane of $g$. Then $\overline{\pi}$ is a subplane of $\pi$ isomorphic to AG$(2,8)$ such that $\overline{\Omega} = \{6,9,17,31,54,57,63,64\}$ is a parabolic oval in $\overline{\pi}$. The centralizer $C$ of $g$ in A$\Gamma$L$(1,64)$ has order 336 and the factor group $\overline{G} = C/\langle g\rangle$ is a collineation group of $\overline{\pi}$ preserving the parabolic oval $\overline{\Omega}$. Therefore, the result for Case 8 applies. More precisely, $\overline{G} \cong$ A$\Gamma$L$(1,8)$ and $\overline{G}$ acts on $\overline{\Omega}$ as A$\Gamma$L$(1,8)$ in its natural doubly transitive permutation. A system of generators of $\overline{G}$ consists of the following three permutations on $\overline{\Omega}$:

$$h_1 = (6,57)(9,17)(31,64)(54,63);$$
$$h_2 = (9,64,54)(17,31,63);$$
$$h_3 = (6,9,17)(31,64,63).$$

Therefore, the action of $\varphi_P$ on $\overline{\Omega}$ is $(6,9)(17,31)(54,57)(63,64)$.

It remains to compute the action of $\varphi_P$ on the set $\Omega_0$ consisting of the other 54 points in $\Omega$. From (vii), $\varphi_P$ is an involutory permutation belonging to the centralizer $C(g)$ of $g$ in the symmetric group on $\Omega_0$. The order of $C(g)$ is equal to 3656994324480; more precisely

$$C(g) = \underbrace{(C_6 \times \cdots \times C_6)}_{9 \text{ times}} \rtimes S_9.$$

A Sylow 2-subgroup $S_2$ of $C(g)$ has order $2^{16}$, and it contains 4127 involutions. Some computations performed by GAP show however that $S_2$ and hence $C(g)$ has only five pairwise non-conjugate involutions under $C(g)$, namely $g^3$ and

$$\begin{aligned}
k_1 = &(1,26)(2,18)(3,10)(4,40)(5,37)(7,46)(8,12)(11,36)(13,27)(14,25)\\
&(15,62)(16,61)(19,28)(21,29)(22,58)(23,30)(24,45)(32,60)(33,43)\\
&(34,42)(35,50)(38,49)(39,44)(41,48)(47,51)(52,55)(56,59);\\
k_2 = &(1,26)(2,7)(3,16)(4,43)(5,38)(8,10)(11,22)(12,44)(13,27)(14,37)\\
&(15,23)(18,19)(21,40)(24,45)(25,55)(28,34)(29,39)(30,32)(33,56)\\
&(35,60)(36,42)(41,58)(46,51)(47,48)(49,50)(52,62)(59,61);\\
k_3 = &(1,26)(2,7)(3,21)(4,43)(5,38)(8,10)(11,22)(12,44)(13,27)(14,30)\\
&(15,23)(16,40)(18,41)(19,58)(24,45)(25,55)(28,34)(29,39)(32,37)\\
&(33,56)(35,60)(36,42)(46,51)(47,48)(49,50)(52,62)(59,61);\\
k_4 = &(1,26)(2,22)(3,21)(4,10)(5,23)(7,47)(8,39)(11,34)(12,44)(13,27)\\
&(14,30)(15,55)(16,40)(18,41)(19,58)(24,45)(25,60)(28,48)(29,61)\\
&(32,37)(33,56)(35,38)(36,42)(43,59)(46,51)(49,50)(52,62);\\
k_5 = &(1,26)(2,48)(3,21)(4,61)(5,60)(7,47)(8,39)(10,29)(11,34)(12,44)\\
&(13,27)(14,30)(15,55)(16,40)(18,41)(19,58)(22,28)(23,25)(24,45)\\
&(32,37)(33,56)(35,38)(36,42)(43,59)(46,51)(49,50)(52,62).
\end{aligned}$$

The classes $K_i$containing $k_i$, $i \in \{1,2,3,4,5\}$, have the following sizes: $|K_1| = 1224720$, $|K_2| = 272160$, $|K_3| = 13608$, $|K_4| = 216$, $|K_5| = 1$.

It turns out that the restriction of $\varphi_P$ on $\Omega_0$ is one of the above involutions, up to conjugacy in $C(g)$. This allows to perform the exhaustive search of $\varphi_P$ by means of a test based on (vi). It is convenient to perform such a test in terms of abstract hyperoval oval. For this purpose, add $65 = X_\infty$ and $66 = Y_\infty$ to $\Omega$ in such a way that $\Omega' = \Omega \cup \{65, 66\}$ be a hyperoval in the projective closure of $\pi$.

Now, from an involutory permutation $j$ on $\Omega_0$, define an involutory permutation $j'$ on $\Omega' = \Omega \cup \{65, 66\}$ by the following rule:

$$j' = j * (6,9)(17,31)(54,57)(63,66)(64,65).$$

Also, extend the action of $\mathrm{A\Gamma L}(1,64)$ on $\Omega'$ assuming both extra-points to be fixed points. Then the test consists in selecting the involutory permutations $j'$ with $j$ ranging over the above four classes such that for every non-trivial permutation $\psi \in \mathrm{AGL}(1,64)$ the number of fixed points of $\psi j' \psi^{-1} j'$ be at most two. The exhaustive search performed by GAP returned only one permutation for $\varphi_P$:

$$(1,26)(2,47)(3,34)(4,52)(5,35)(6,9)(7,48)(8,29)(10,39)(11,21)$$
$$(12,40)(13,27)(14,50)(15,18)(16,44)(17,31)(19,51)(20,53)(22,33)$$
$$(23,42)(24,45)(25,36)(28,56)(30,49)(32,59)(37,43)(38,60)(41,55)$$
$$(46,58)(54,57)(61,62)(63,66)(64,65).$$

Therefore, there exist only two polynomials having all properties (i)–(vi), namely:

$$F^{(1)}(X) = X^{62};$$
$$F^{(5)}(X) = \left(\sum_{i=1}^{31} X^i\right)^2 .$$

They represent all the possible doubly transitive parabolic ovals of order 64 admitting the prescribed collineation group. Hence, the following result is proven.

**Theorem 10.** *Let $\alpha$ be an affine plane of order* 64 *containing a doubly transitive parabolic oval $\Omega$. If a collineation group $G \cong$* AGL(1, 64) *of $\alpha$ preserving $\Omega$ acts on the affine points of $\Omega$ as* AGL(1, 64) *in its doubly transitive permutation group, then $\alpha$ is the Desarguesian plane and $\Omega$ is a parabola.*


# Acknowledgement

The authors wish to thank Tim Penttila for helpful discussions.


# References


[1] M. Biliotti, V. Jha, and N. L. Johnson, *Two-transitive parabolic ovals*, J. Geom. **70** (2001), no. 1-2, 17–27.

[2] A. A. Bruen and J. A. Thas, *Flocks, chains and configurations in finite geometries*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **59** (1976), 744–748.

[3] P. Dembowski, *Finite geometries*, Classics in Mathematics, Springer-Verlag, Berlin, 1997, Reprint of the 1968 original.

[4] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2006, (`http://www.gap-system.org`).

[5] J. W. P. Hirschfeld, *Ovals in desarguesian planes of even order*, Ann. Mat. Pura Appl. (4) **102** (1975), 79–89.

[6] R. Huppert and N. Blackburn, *Finite groups iii*, first ed., Grundlehren der matematischen Wissenshaften, vol. 243, Springer Verlag, Springer, 1982.

[7] W. M. Kantor, *k-homogeneous groups*, Math. Z **124** (1972), 261–265.

[8] G. Korchmáros, *Segre-type theorems in finite geometry*, Rend. Mat. Appl. (7) **26** (2006), no. 1, 95–120.

[9] G. E. Moorhouse, *On projective planes of order less than 32*, Finite geometries, groups, and computation, Walter de Gruyter GmbH & Co. KG, Berlin, 2006, pp. 149–162.

[10] S. E. Payne, *A complete determination of translation ovoids in finite Desarguian planes*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **51** (1971), 328–331 (1972).

[11] T. Penttila, G. F. Royle, and M. K. Simpson, *Hyperovals in the known projective planes of order* 16, J. Combin. Des. **4** (1996), no. 1, 59–65.

[12] G. Royle, *Projective planes of order* 16, , (`http://people.csse.uwa.edu.au/gordon/remote/planes16`).

[13] B. Segre, *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane*, Ann. Mat. Pura Appl. (4) **64** (1964), 1–76.

[14] B. Segre and U. Bartocci, *Ovali ed altre curve nei piani di Galois di caratteristica due*, Acta Arith. **18** (1971), 423–449.

[15] B. Segre and G. Korchmáros, *Una proprietà degli insiemi di punti di un piano di Galois caratterizzante quelli formati dai punti delle singole rette esterne ad una conica*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **62** (1977), no. 5, 613–619.