Collineations of Subiaco and Cherowitzo hyperovals

Christine M. O'Keefe J. A. Thas

Abstract

A Subiaco hyperoval in $\mathrm{PG}(2, 2^h)$, $h \geq 4$, is known to be stabilised by a group of collineations induced by a subgroup of the automorphism group of the associated Subiaco generalised quadrangle. In this paper, we show that this induced group is the full collineation stabiliser in the case $h \not\equiv 2 \pmod 4$; a result that is already known for $h \equiv 2 \pmod 4$. In addition, we consider a set of $2^h + 2$ points in $\mathrm{PG}(2, 2^h)$, where $h \geq 5$ is odd, which is a Cherowitzo hyperoval for $h \leq 15$ and which is conjectured to form a hyperoval for all such h. We show that a collineation fixing this set of points and one of the points $(0, 1, 0)$ or $(0, 0, 1)$ must be an automorphic collineation.

1 Introduction

In the Desarguesian projective plane $\mathrm{PG}(2, q)$ of even order $q = 2^h$, $h \geq 1$, an *oval* is a set of $q + 1$ points, no three collinear, and a *hyperoval* is a set of $q + 2$ points no three of which are collinear. A hyperoval $\mathcal{H}$ can be written, with a suitable choice of homogeneous coordinates for $\mathrm{PG}(2, q)$, as

$$\mathcal{H} = \mathcal{D}(f) = \{(1, t, f(t)) \colon t \in \mathrm{GF}(q)\} \cup \{(0, 1, 0), (0, 0, 1)\}$$

for some function f on $\mathrm{GF}(q)$ satisfying $f(0) = 0$ and $f(1) = 1$, see [6, 8.4.2]. (Note that in [6] an oval is called a $(q + 1)$-arc and a hyperoval is called an oval.)

We are interested in calculating the stabiliser in the automorphism group of $\mathrm{PG}(2, q)$ of some recently discovered hyperovals. The automorphism group of

Received by the editors February 1995.
Communicated by J. Doyen.
1991 *Mathematics Subject Classification* : 51e15,51e21.
Key words and phrases : finite projective planes, hyperovals, collineation groups.

$\mathrm{PG}(2,q)$ is the group $\mathrm{P\Gamma L}(3,q)$ induced by the semilinear transformations of the underlying vector space, which we call *collineations.* The elements of the normal subgroup $\mathrm{PGL}(3,q) \lhd \mathrm{P\Gamma L}(3,q)$ determined by the linear transformations will be called *homographies.* If $\sigma : x \mapsto x^\sigma$ is an automorphism of $\mathrm{GF}(q)$ then σ induces a collineation of $\mathrm{PG}(2,q)$, called an *automorphic collineation,* as follows: $(x,y,z)^\sigma = (x^\sigma, y^\sigma, z^\sigma)$. Let A denote the group of automorphic collineations of $\mathrm{PG}(2,q)$, so that $|A| = h$ and $\mathrm{P\Gamma L}(3,q) = \mathrm{PGL}(3,q) \rtimes A$ (where $\rtimes$ is used to denote the semidirect product).

If $\mathcal{X}$ is a set of points in $\mathrm{PG}(2,q)$, the stabiliser $\mathrm{P\Gamma L}(3,q)_{\mathcal{X}}$ of $\mathcal{X}$ in $\mathrm{P\Gamma L}(3,q)$ is called the *collineation stabiliser* of $\mathcal{X}$ while the stabiliser $\mathrm{PGL}(3,q)_{\mathcal{X}}$ is called the *homography stabiliser* of $\mathcal{X}$. A set of points in $\mathrm{PG}(2,q)$ which is the image under an element of $\mathrm{P\Gamma L}(3,q)$ of a set of points $\mathcal{X}$ is said to be (projectively) *equivalent* to $\mathcal{X}$.

Associated with each q-clan, $q = 2^h$, is a generalised quadrangle (GQ) of order (q^2, q) with subquadrangles of order q; associated to any of these subquadrangles is an oval in $\mathrm{PG}(2,q)$ ([8, 11, 12, 19, 20]). Recently, Cherowitzo, Penttila, Pinneri and Royle [5] constructed the class of *Subiaco* ovals in this way. Since an oval is contained in a unique hyperoval, we thus have the Subiaco hyperovals $\mathcal{D}(g)$ and $\mathcal{D}(f_s)$ for $s \in GF(q)$, where

$$\begin{aligned}
a &= \frac{d^2+d^5+d^{1/2}}{d(1+d+d^2)},\\
f(t) &= \frac{d^2t^4+d^2(1+d+d^2)t^3+d^2(1+d+d^2)t^2+d^2t}{(t^2+dt+1)^2}+t^{1/2}\\
g(t) &= \frac{d^4t^4+d^3(1+d^2+d^4)t^3+d^3(1+d^2)t}{(d^2+d^5+d^{1/2})(t^2+dt+1)^2}+\frac{d^{1/2}}{d^2+d^5+d^{1/2}}t^{1/2} \text{ and}\\
f_s(t) &= \frac{f(t)+asg(t)+s^{1/2}t^{1/2}}{1+as+s^{1/2}}
\end{aligned}$$

for $d \in \mathrm{GF}(q)$ satisfying $\mathrm{trace}(1/d) = 1$ and $d^2+d+1 \neq 0$. (For an alternative description of the Subiaco hyperovals, see [16].)

In the case that $q \leq 256$, each Subiaco hyperoval falls into one of the previously known classes of hyperovals [16].

(i) If $q = 2, 4, 8$ then a Subiaco hyperoval is a regular hyperoval see [6, 8.4]. When $q = 8$ the homography stabiliser has order 504 and is isomorphic to $\mathrm{PGL}(2,8)$, when $q = 4$ the homography stabiliser has order 360 and is isomorphic to A_6 and when $q = 2$ the homography stabiliser has order 24 and is isomorphic to S_4 [6, 8.4.2 Corollary 6]. Since A fixes the regular hyperoval $\mathcal{D}(x^2)$, the collineation stabilisers have orders 1512, 720 and 24 (respectively) and are isomorphic to $\mathrm{P\Gamma L}(2,8)$, S_6 and S_4 (respectively).

(ii) If $q = 16$ then a Subiaco hyperoval is a Lunelli-Sce hyperoval [9]. The homography stabiliser has order 36 and is isomorphic to $C_3^2 \rtimes C_4$ while the collineation stabiliser of order 144 is isomorphic to $C_2 \times (C_3^2 \rtimes C_8)$ (where $\times$ denotes the direct product) [15].

(iii) If $q = 32$ then a Subiaco hyperoval is a Payne hyperoval [12]. The homography stabiliser has order 2 (and is isomorphic to C_2) while the collineation stabiliser of

order $2h$ is isomorphic to C_{2h} [21, 10].
(iv) If $q = 64$ then the two projectively distinct Subiaco hyperovals are the two Penttila-Pinneri irregular hyperovals [17]. The homography stabiliser is either C_5 of order 5 or D_{10} of order 10 and the respective collineation stabilisers have order 15 and 60 and are isomorphic to $C_5 \rtimes C_3$ and $C_5 \rtimes C_{12}$.
(v) If $q = 128$ or 256 then the projectively unique Subiaco hyperoval was discovered by Penttila and Royle [18], with homography stabiliser C_2 in each case and collineation stabiliser of order 14 or 16 isomorphic to C_{14} or C_{16}, respectively.

We note that the order of the collineation stabiliser in case (v) was obtained with the assistance of a computer.

In [13, 2, 16], the collineation group of the Subiaco GQ is studied in detail. The action of this group induces an action on each of the subquadrangles of order q and on each associated Subiaco oval. Hence there arises an induced stabiliser of the Subiaco hyperoval, whose order can be easily determined. If $q > 64$ and $h \equiv 2 \pmod 4$ then the induced stabiliser is the full collineation stabiliser of the Subiaco hyperoval. In particular,

Theorem 1 ([16], 6.13, 5.4) (1) Suppose $q > 64$ and $h \equiv 2 \pmod 4$. Up to projective equivalence, there are exactly two Subiaco hyperovals of $\mathrm{PG}(2, q)$, with collineation stabilisers of order $10h$ and $5h/2$, isomorphic to $C_5 \rtimes C_{2h}$ and $C_5 \rtimes C_{h/2}$, respectively.
(2) Suppose that $q > 64$ and $h \not\equiv 2 \pmod 4$. Up to projective equivalence there is only one Subiaco oval, which is fixed by a subgroup of $\mathrm{P\Gamma L}(3, q)$ of order $2h$.

It is immediate from [14], Equations (39) and (43), that the subgroup in Theorem 1 (2) contains only one non-identity homography (of order 2) and is either cyclic of order $2h$ or is the direct product of a cyclic group of order 2 with a cyclic group of order h.

In this paper we will show that if $q = 2^h$, where $q > 64$ and $h \not\equiv 2 \pmod 4$, then the subgroup in Theorem 1 (2) is cyclic and is the full collineation stabiliser of the Subiaco hyperoval.

Cherowitzo [3, 4] has discovered six hyperovals, conjectured to belong to an infinite family. These are $\mathcal{D}(x^\sigma + x^{\sigma+2} + x^{3\sigma+4})$ in $\mathrm{PG}(2, 2^h)$ for $h = 5, 7, 9, 11, 13$ or 15, and where $\sigma \in \mathrm{AutGF}(q)$ is such that $\sigma^2 \equiv 2 \pmod{q-1}$. The collineation stabiliser of the Cherowitzo hyperoval for $h = 5$ is the group A of automorphic collineations of order h [10], and for $h \geq 7$ the order of the collineation stabiliser is divisible by h [3].

We show that, for $\sigma \in \mathrm{AutGF}(q)$ such that $\sigma^2 \equiv 2 \pmod{q-1}$, a collineation which fixes the set of points $\mathcal{D}(x^\sigma + x^{\sigma+2} + x^{3\sigma+4})$ in $\mathrm{PG}(2, 2^h)$ for h odd and fixes either $(0, 1, 0)$ or $(0, 0, 1)$ is an automorphic collineation. Our result is independent of whether such a set is a hyperoval.

2 Preliminaries

In [21], Thas, Payne and Gevaert calculated the collineation stabiliser of the Payne hyperoval by finding an algebraic curve with a large intersection with the hyperoval. They were able to prove that a collineation fixing the hyperoval must fix the curve (over any extension of GF(q)); then they used the projective invariance of some geometric properties of the curve to obtain the result. We will be applying the same basic method here, so we give a review of some properties of algebraic plane curves. More details can be found in [6, 2.6, 10.1].

First, an *algebraic plane curve of degree* n in PG$(2,q)$ is a set of points $\mathcal{C} = V(F) = \{(x,y,z) : F(x,y,z) = 0\}$ where F is a homogeneous polynomial of degree n in the variables x, y, z. If F is irreducible over GF(q) then $\mathcal{C}$ is *irreducible* and if F is irreducible over the algebraic closure of GF(q) then $\mathcal{C}$ is *absolutely irreducible.* In the following, if $P = (p_1, p_2, p_3)$ then $F(P) = F(p_1, p_2, p_3)$. Also, F_x, F_y, F_z denote the partial derivatives of F with respect to x, y, z, respectively.

Further, we recall that an element $g \in \mathrm{P\Gamma L}(3,q)$ is of the form $g : X \mapsto BX^\alpha$, where $X = (x,y,z)$, $B \in \mathrm{GL}(3,q)$ and $\alpha \in A$. The image of an algebraic curve $\mathcal{C} = V(F)$ under g is the curve $g\mathcal{C} = V(F^\alpha \circ A^{-1})$, where if $F(x,y,z) = \sum a_{ijk}x^iy^jz^k$ then $F^\alpha(x,y,z) = \sum a_{ijk}^\alpha x^iy^jz^k$ and $\circ$ denotes composition of functions.

Result 2 ([6], 2.6, 10.1) Let $\mathcal{C} = V(F)$ be an algebraic plane curve of degree n in PG$(2,q)$. Further, suppose that $F(x,y,z) = \sum_{i=0}^{n} F^{(i)}(x,y)z^{n-i}$ where $F^{(i)}$ is a (homogeneous) polynomial of degree i in the variables x, y. Then
(i) a point P of $\mathcal{C}$ is a point of multiplicity greater than one if and only if $F_x(P) = F_y(P) = F_z(P) = 0$, otherwise it is a point of multiplicity one, that is, it is a simple point,
(ii) if $F^{(0)} = F^{(1)} = \ldots = F^{(m-1)} = 0$ but $F^{(m)} \neq 0$ then $\mathcal{C}$ has a point of multiplicity m at $(0,0,1)$,
(iii) with m as in (ii), there exists $k \leq m$ such that the curve $V(F^{(m)})$ consists of m lines in PG$(2,q^k)$ (a line corresponding to a linear factor of $F^{(m)}$ with multiplicity s is counted s times), each of which is a tangent to $\mathcal{C}$ at $(0,0,1)$,
(iv) the multiplicity of a point $P \in \mathcal{C}$ and the number and multiplicity of the tangents to $\mathcal{C}$ at a point are invariant under the action of $\mathrm{P\Gamma L}(3,q)$.

Let $m_P(\mathcal{C})$ denote the multiplicity of the point P on the curve $\mathcal{C}$. The next result follows from Bézout's theorem.

Result 3 ([6], 10.1 IV and VII) Let $\mathcal{C}_1 = V(F_1)$ and $\mathcal{C}_2 = V(F_2)$ be algebraic plane curves of degree n_1 and n_2 in PG$(2,q)$, respectively. Let γ denote the algebraic closure of GF(q), so that $\widehat{\mathcal{C}}_1 = V(F_1)$ and $\widehat{\mathcal{C}}_2 = V(F_2)$ are algebraic plane curves of degree n_1 and n_2 in PG$(2,\gamma)$. If $\widehat{\mathcal{C}}_1$ and $\widehat{\mathcal{C}}_2$ have no common component, then

$$\sum_{P \in \widehat{\mathcal{C}}_1 \cap \widehat{\mathcal{C}}_2} m_P(\widehat{\mathcal{C}}_1) m_P(\widehat{\mathcal{C}}_2) \leq n_1 n_2.$$

Lemma 4 Let $\mathcal{C}$ and $\mathcal{C}'$ be algebraic curves, each containing the point $(0,0,1)$ as a simple point, each with tangent $x = 0$ at $(0,0,1)$ and such that the intersection multiplicity of $x = 0$ with $\mathcal{C}$ is s and the intersection multiplicity of $x = 0$ with $\mathcal{C}'$ is t, where $s \leq t$. Then the multiplicity of the intersection of $\mathcal{C}$ with $\mathcal{C}'$ at $(0,0,1)$ is at least s.

Proof: For the proof, we use non-homogeneous coordinates (X, Y). The hypotheses on the curves imply that the equations have the form:

$$\begin{aligned} \mathcal{C} &: \quad XF(X,Y) + Y^sG(Y) = 0, \\ \mathcal{C}' &: \quad XF'(X,Y) + Y^tG'(Y) = 0, \end{aligned}$$

for some polynomials F, G, F', G'. Now a point (X, Y) lies in $\mathcal{C} \cap \mathcal{C}'$ if and only if the following equations are satisfied:

$$\begin{aligned} XF(X,Y) + Y^s G(Y) &= 0, \\ Y^s[Y^{t-s}G'(Y)F(X,Y) - G(Y)F'(X,Y)] &= 0, \end{aligned}$$

implying that the multiplicity of intersection of $\mathcal{C}$ and $\mathcal{C}'$ at $(0,0)$ is at least s. ∎

3 Collineations of Subiaco hyperovals

Suppose for this section that $q > 64$ and that $h \not\equiv 2 \pmod 4$. Recall that there is a projectively unique Subiaco hyperoval in $\mathrm{PG}(2, q)$, which can be written as

$$\mathcal{H} = \{(1, t, f(t)) \colon t \in \mathrm{GF}(q)\} \cup \{(0,1,0), (0,0,1)\}$$

where

$$f(t) = \frac{d^2t^4 + d^2(1+d+d^2)t^3 + d^2(1+d+d^2)t^2 + d^2t}{(t^2+dt+1)^2} + t^{1/2}$$

and $d \in \mathrm{GF}(q)$ satisfies $\mathrm{trace}(1/d) = 1$ and $d^2 + d + 1 \neq 0$.

3.1 Subiaco hyperovals and algebraic curves

In this section we find an algebraic plane curve which coincides with $\mathcal{H}$ as a set of points in $\mathrm{PG}(2, q)$, and investigate some of its properties.

In non-homogeneous coordinates Y, Z, a point $(t, f(t))$ of the Subiaco hyperoval $\mathcal{H}$ satisfies the equation

$$\begin{aligned} & Z = \frac{d^2Y^4 + d^2(1+d+d^2)(Y^3+Y^2) + d^2Y}{(Y^2+dY+1)^2} + Y^{1/2} \\ \Leftrightarrow\ & Z^2 = \frac{d^4Y^8 + d^4(1+d^2+d^4)(Y^6+Y^4) + d^4Y^2}{(Y^2+dY+1)^4} + Y; \end{aligned}$$

so in homogeneous coordinates x, y, z the point $(1, t, f(t))$ of $\mathcal{H}$ satisfies

$$(z^2+xy)(x^2+dxy+y^2)^4 + d^4(x^2y^8+x^8y^2) + d^4(1+d^2+d^4)(x^4y^6+x^6y^4) = 0.$$

We denote this last equation by $F(x,y,z) = 0$, noting that F is a homogeneous polynomial of degree 10 in the variables x, y, z, and define an algebraic curve $\mathcal{C}$ in $\mathrm{PG}(2, q)$ by

$$\mathcal{C} = V(F) = \{(x,y,z) \colon F(x,y,z) = 0\}.$$

Lemma 5 The curve $\mathcal{C}$ and the hyperoval $\mathcal{H}$ coincide as sets of points in $\mathrm{PG}(2, q)$.

Proof: It is clear that $\mathcal{H}$ and $\mathcal{C}$ coincide on the set of points (x,y,z), $x \neq 0$, so we only need to check that $\mathcal{C}$ and $\mathcal{H}$ coincide on the set of points $(0,y,z)$. Now $F(0,y,z) = z^2y^8 = 0$ if and only if either $y = 0$ or $z = 0$, hence $\mathcal{H}$ and $\mathcal{C}$ only contain the points $(0,1,0), (0,0,1)$ among the points $(0,y,z)$. ∎

In the following, let γ be the algebraic closure of GF(q) and let $\widehat{\mathcal{C}} = V(F)$ denote the algebraic curve of degree 10 in PG$(2,\gamma)$.

Lemma 6 The curve $\widehat{\mathcal{C}}$ has a unique multiple point $(0,0,1)$ of multiplicity 8 and the two linear factors of $x^2+dxy+y^2=0$ (conjugate in a quadratic extension of GF(q)) are the equations of the tangents to $\widehat{\mathcal{C}}$ at $(0,0,1)$ (each with multiplicity 4).

Proof: The multiple points of $\widehat{\mathcal{C}}$ are determined by the solutions of the following system of equations:

$$\begin{aligned} F(x,y,z) &= 0, \\ F_x(x,y,z) &= y(x^8+d^4x^4y^4+y^8)=0, \\ F_y(x,y,z) &= x(x^8+d^4x^4y^4+y^8)=0, \\ F_z(x,y,z) &= 0. \end{aligned}$$

Now $x=0 \Leftrightarrow y=0$ and we have found the multiple point $(0,0,1)$, of multiplicity 8. The factors of $(x^2+dxy+y^2)^4=0$ determine the (eight) tangents to $\widehat{\mathcal{C}}$ at $(0,0,1)$.

If $x \neq 0$ and $y \neq 0$ then $x^2+dxy+y^2=0$. Further,

$$\begin{aligned} F(x,y,z)=0 &\Leftrightarrow d^4(x^2y^8+x^8y^2)+d^4(1+d^2+d^4)(x^4y^6+x^6y^4)=0 \\ &\Leftrightarrow d^2(xy^4+x^4y)+d^2(1+d+d^2)(x^2y^3+x^3y^2)=0 \\ &\Leftrightarrow d^2xy\left(y^3+x^3+(1+d+d^2)(xy^2+x^2y)\right)=0 \\ &\Leftrightarrow d^2xy\left(y(y^2+dxy+x^2)+x(y^2+dxy+x^2)+d^2xy(x+y)\right)=0 \\ &\Leftrightarrow d^4x^2y^2(x+y)=0 \\ &\Leftrightarrow x=y. \end{aligned}$$

Substituting $x=y$ into the equation $x^2+dxy+y^2=0$ implies that $dxy=0$, which is impossible. ∎

Lemma 7 The curve $\mathcal{C}$ is absolutely irreducible.

Proof: If one of the two tangents to $\mathcal{C}$ at $(0,0,1)$ is a component of $\widehat{\mathcal{C}}$, then so is the other tangent, and in this case $x^2+dxy+y^2$ must be a factor of $F(x,y,z)$. Hence $x^2+dxy+y^2$ divides $d^4(x^2y^8+x^8y^2)+d^4(1+d^2+d^4)(x^4y^6+x^6y^4)$, so divides $y^6+x^6+(1+d^2+d^4)(x^2y^4+x^4y^2) = x^2(x^4+d^2x^2y^2+y^4)+y^2(y^4+d^2x^2y^2+x^4)+d^4(x^2y^4+x^4y^2)$, so divides $d^4x^2y^2(x^2+y^2)$, so divides x^2+y^2, so divides dxy, a contradiction. Thus neither tangent to $\mathcal{C}$ at $(0,0,1)$ is a component of $\widehat{\mathcal{C}}$.

As $\widehat{\mathcal{C}}$ has a unique singular point, each irreducible factor of F over γ has multiplicity 1. Suppose that the irreducible components of $\widehat{\mathcal{C}}$ are $\mathcal{C}_1,\ldots,\mathcal{C}_r$, for some $r>1$, where $\deg(\mathcal{C}_i)=n_i$ and $\mathcal{C}_i$ has multiplicity m_i at $(0,0,1)$. If, for some i, we have $m_i=n_i$ then $m_i=n_i=1$ and the component $\mathcal{C}_i$ is a line, which must therefore be a tangent to $\mathcal{C}_i$, and hence to $\mathcal{C}$, at $(0,0,1)$. This possibility has already been ruled out. Since $n_1+\ldots+n_r=10$ and $m_1+\ldots+m_r=8$, with $n_i>m_i\geq 0$ for all i, the only possibility is that $r=2$ and, without loss of generality, $(n_1,n_2)=(1,9),(2,8),(3,7),(4,6)$ or $(5,5)$ and in each case $m_i=n_i-1$.

As $(0,0,1)$ is the only singular point of $\widehat{\mathcal{C}}$, it is the unique common point of $\mathcal{C}_1$ and $\mathcal{C}_2$. In particular, $(0,0,1)$ is a point of each of $\mathcal{C}_1$ and $\mathcal{C}_2$. Hence (n_1,n_2) is different from $(1,9)$, as otherwise $m_1=n_1-1=0$.

If $\mathcal{C}_1$ and $\mathcal{C}_2$ are defined over $\mathrm{GF}(q)$, and since any tangent to $\mathcal{C}_i$ at $(0,0,1)$ is a tangent to $\mathcal{C}$ and is therefore not a line of $\mathrm{PG}(2,q)$, it follows that any line of $\mathrm{PG}(2,q)$ on $(0,0,1)$ meets $\mathcal{C}_i$ in a further point of $\mathrm{PG}(2,q)$. Then $|\mathcal{C}_1 \cup \mathcal{C}_2| = 2(q+1)+1 > q+2 = |\mathcal{C}|$, a contradiction.

Thus $\mathcal{C}_1$ and $\mathcal{C}_2$ are not defined over $\mathrm{GF}(q)$, but over some extension $\mathrm{GF}(q^s)$, for some $s > 1$. Let σ be a non-identity element of the Galois group $\mathrm{Gal}(\mathrm{GF}(q^s)/\mathrm{GF}(q))$. Then $\mathcal{C}_1^\sigma = \mathcal{C}_2$, which implies that $n_1 = n_2 = 5$. By [6], Lemma 10.1.1, $|\mathcal{C}_i| \le 5^2$, so $|\mathcal{C}| \le 2(25) - 1 = 49$. We have already shown that $|\mathcal{C}| = q+2$ and $q > 64$, so the contradiction proves the result. ■

Lemma 8 If $q > 64$ then $\mathrm{P\Gamma L}(3,q)_{\mathcal{H}} \le \mathrm{P\Gamma L}(3,q)_{\widehat{\mathcal{C}}}$.

Proof: Let $\theta \in \mathrm{P\Gamma L}(3,q)_{\mathcal{H}}$. Since $\mathcal{H}^\theta = \mathcal{H}$ and $\mathcal{C} = \mathcal{H}$ as sets of points in $\mathrm{PG}(2,q)$, we know that $\mathcal{H} = \mathcal{C}^\theta$. Suppose, aiming for a contradiction, that $\widehat{\mathcal{C}}^\theta \ne \widehat{\mathcal{C}}$. Since $\mathcal{H} \subseteq \widehat{\mathcal{C}}^\theta \cap \widehat{\mathcal{C}}$, and taking account of multiplicities, we see that

$$\sum_{P \in \widehat{\mathcal{C}}^\theta \cap \widehat{\mathcal{C}}} m_P(\widehat{\mathcal{C}}^\theta) m_P(\widehat{\mathcal{C}}) \ge q + 16.$$

By Result 3 and since $\mathcal{C}$ and $\mathcal{C}^\theta$ are both absolutely irreducible, if $\widehat{\mathcal{C}}^\theta \ne \widehat{\mathcal{C}}$ then $q+16 \le 100$, implying that $q \le 64$. We conclude that $\widehat{\mathcal{C}}^\theta = \widehat{\mathcal{C}}$ so that $\theta \in \mathrm{P\Gamma L}(3,q)_{\widehat{\mathcal{C}}}$. ■

Lemma 9 Let $\theta \in \mathrm{P\Gamma L}(3,q)_{\mathcal{H}}$. Then θ fixes the point $(0,0,1)$ and fixes the set of lines (in a quadratic extension of $\mathrm{PG}(2,q)$) determined by the equation $x^2 + dxy + y^2 = 0$.

Proof: First, $\theta \in \mathrm{P\Gamma L}(3,q)_{\mathcal{H}} \le \mathrm{P\Gamma L}(3,q)_{\widehat{\mathcal{C}}}$, by Lemma 8. Since $(0,0,1)$ is the unique point of multiplicity greater than 1 on $\widehat{\mathcal{C}}$, it must be fixed by θ (see Result 2). So the pair of tangents to $\mathcal{C}$ at $(0,0,1)$ is also fixed by θ. ■

3.2 The case $q = 2^h$ where $h \equiv 0$ (mod 4)

In this case, we show that the known collineation group of order $2h$ stabilising $\mathcal{H}$ is the full collineation stabiliser.

First, let $\mathrm{PG}(2,q)/(0,0,1)$ denote the quotient space of lines on $(0,0,1)$, so that $\mathrm{PG}(2,q)/(0,0,1) \cong \mathrm{PG}(1,q)$ in the natural way. By Lemma 9, an element $\theta \in \mathrm{P\Gamma L}(3,q)_{\mathcal{H}}$ acts on $\mathrm{PG}(2,q)/(0,0,1) \cong \mathrm{PG}(1,q)$ as an element of $\mathrm{P\Gamma L}(2,q)$, fixing setwise a pair of (conjugate) points $\ell, \overline{\ell}$ in a quadratic extension $\mathrm{PG}(1,q^2)$. Further, such an action is faithful since no non-trivial element of $\mathrm{P\Gamma L}(3,q)$ is a central collineation with centre $(0,0,1)$ (for otherwise, since $(0,0,1) \in \mathcal{H}$, such a collineation would be an element of $\mathrm{PGL}(3,q)$ fixing $\mathcal{H}$, and hence a quadrangle, pointwise). Thus $\mathrm{P\Gamma L}(3,q)_{\mathcal{H}} \le \mathrm{P\Gamma L}(2,q)_{\{\ell,\overline{\ell}\}}$.

Lemma 10 ([16], proof of VI.13) $\mathrm{P\Gamma L}(2,q)_{\{\ell,\overline{\ell}\}} = C_{q+1} \rtimes C_{2h}$. ■

As a corollary of Lemmas 9 and 10, it follows that $\mathrm{P\Gamma L}(3,q)_{\mathcal{H}}$ is a subgroup of $C_{q+1} \rtimes C_{2h}$. We will show that $\mathrm{P\Gamma L}(3,q)_{\mathcal{H}}$ contains no non-trivial element of the cyclic subgroup C_{q+1}, so that $|\mathrm{P\Gamma L}(3,q)_{\mathcal{H}}| = 2h$, as required.

Aiming for a contradiction, we let $G = C_{q+1} \cap \mathrm{P\Gamma L}(3,q)_{\mathcal{H}}$ be a non-trivial group.

Lemma 11 The group G has a unique fixed line.

Proof: First we note that $G = C_{q+1} \cap \mathrm{P\Gamma L}(3,q)_{\mathcal{H}} = C_{q+1} \cap \mathrm{PGL}(3,q)_{\mathcal{H}}$. It is straightforward to show that C_{q+1} has a unique fixed point and a unique fixed line, not on the fixed point (see, for example, [1, Lemma 6]), so G has at least one fixed line.

Let p be a prime such that p divides $|G|$ and let $g \in G$ have order p. Since $1 \neq g \in \mathrm{PGL}(3,q)$, g has at most 3 fixed lines. Further, $q^2+q+1 \equiv 1 \pmod p$ (for p divides $|G|$ and hence divides $q+1$ so $q \equiv -1 \pmod p$), implying that g has exactly one fixed line. Thus G has at most one fixed line. ■

In the following we denote the points of the Desarguesian projective plane $\mathrm{PG}(2,q)$ by homogeneous triples (x,y,z) and denote the line of $\mathrm{PG}(2,q)$ with equation $\ell x + my + nz = 0$ by the homogeneous triple $[\ell, m, n]$.

The homography $\rho\colon (x,y,z) \mapsto (y,x,z)$ is an elation with centre $(1,1,0)$ and axis $[1,1,0]$, fixing $\mathcal{H}$. Thus $\rho \in \mathrm{P\Gamma L}(3,q)_{\mathcal{H}} \leq \mathrm{P\Gamma L}(2,q)_{\{\ell,\bar{\ell}\}}$.

Since $C_{q+1} \lhd \mathrm{P\Gamma L}(2,q)_{\{\ell,\bar{\ell}\}}$, so $\rho \in N_{\mathrm{P\Gamma L}(2,q)_{\{\ell,\bar{\ell}\}}}(C_{q+1})$. It follows that ρ permutes the fixed lines of C_{q+1}, and hence fixes the unique fixed line of C_{q+1} . Now the fixed lines of ρ are $[0,0,1]$ and $[1,1,c]$ for $c \in \mathrm{GF}(q)$, so the fixed line of C_{q+1} (and hence also the fixed line of G) must be one of these lines.

If the fixed line of G is $[0,0,1]$, then G fixes $(0,0,1)$ (Lemma 9) and also fixes $[0,0,1] \cap \mathcal{H} = \{(0,1,0),(1,0,0)\}$. If a generator g of G interchanges $(0,1,0)$ and $(1,0,0)$, then g induces an involution on $[0,0,1]$, so g fixes a point on $[0,0,1]$, hence g and also G fixes a line through $(0,0,1)$, contrary to Lemma 11. Thus g and hence G fixes $(0,1,0)$ and $(1,0,0)$, and consequently G also fixes the lines $[1,0,0]$ and $[0,1,0]$, contrary to Lemma 11.

Thus the fixed line of C_{q+1} is $[1,1,c]$ for some $c \in \mathrm{GF}(q)$; since the fixed line of C_{q+1} does not contain $(0,0,1)$ we have $c \neq 0$. Let p be a prime such that p divides $|G|$ and let $g \in G$ have order p. The homography g fixes the pencil $\mathcal{P}$ of conics

$$\mathcal{C}_s:\ (x+y+cz)^2 + s(x^2+dxy+y^2) = 0, \quad s \in \mathrm{GF}(q) \cup \{\infty\}.$$

Since p divides $q+1$, so is odd, and since $\mathcal{C}_0 :\ (x+y+cz)^2 = 0$ and $\mathcal{C}_\infty :\ x^2+dxy+y^2 = 0$ are fixed by g, at least one more conic $\mathcal{C}_s$ is fixed by g. Since at least three elements of $\mathcal{P}$ are fixed by g, each element of $\mathcal{P}$ is fixed by g. In particular, $\mathcal{O} = \mathcal{C}_1 :\ c^2z^2 + dxy = 0$ is fixed by g. We have

$$\mathcal{O} = \left\{ \left(1, t, \frac{d^{1/2}}{c} t^{1/2}\right) : t \in \mathrm{GF}(q) \right\} \cup \{(0,1,0)\}.$$

(Note that G also fixes the nucleus $(0,0,1)$ of the conic $\mathcal{O}$.)

Lemma 12 If p is any prime dividing $|G|$, then $p \in \{3,5,7\}$.

Proof: Let p be a prime dividing $|G|$ and let $g \in G$ have order p. Since $\langle g \rangle \leq C_{q+1}$, $\langle g \rangle$ acts semi-regularly on $\mathrm{PG}(2,q) \setminus \{(0,0,1)\}$, as the stabiliser in G of any of these points is trivial. Thus any point in $\mathrm{PG}(2,q) \setminus \{(0,0,1)\}$ lies in an orbit of length p. Now $\langle g \rangle$ fixes $\mathcal{O}$ and $\mathcal{H}$; so fixes $\mathcal{O} \cap \mathcal{H}$, which must therefore be a union of orbits of $\langle g \rangle$, each of length p (as $(0,0,1) \notin \mathcal{O}$). Hence p divides $\mathcal{O} \cap \mathcal{H}$.

Next we determine $|\mathcal{O} \cap \mathcal{H}|$. Certainly, $(0,1,0) \in \mathcal{O} \cap \mathcal{H}$. Further, $(1, t, \frac{d^{1/2}}{c} t^{1/2}) \in \mathcal{H}$

$$\begin{aligned}
&\Leftrightarrow \quad \frac{d^{1/2}}{c} t^{1/2} = \frac{d^2(t^4+t) + d^2(1+d+d^2)(t^3+t^2)}{(t^2+dt+1)^2} + t^{1/2} \\
&\Leftrightarrow \quad d^2t^4 + d^2(1+d+d^2)(t^3+t^2) + d^2t + \left(1 + \frac{d^{1/2}}{c}\right) t^{1/2}(t^4 + d^2t^2 + 1) = 0 \\
&\Leftrightarrow \quad d^4t^8 + d^4(1+d^2+d^4)(t^6+t^4) + d^4t^2 + \left(1 + \frac{d}{c^2}\right) t(t^8 + d^4t^4 + 1) = 0.
\end{aligned}$$

Now this is a polynomial over $\mathrm{GF}(q)$ in the variable t of degree at most 9, so has at most 9 solutions in $\mathrm{GF}(q)$. Thus $|\mathcal{O} \cap \mathcal{H}| \leq 10$. Since $q+1$ is odd, and p divides $q+1$, then p is odd and the result follows. ∎

If $p = 3$, then 3 divides $q+1$, which happens if and only if $q = 2^h$ where h is odd, contrary to assumption. If $p = 5$, then 5 divides $q+1$, which happens if and only if $q = 2^h$ where $h \equiv 2 \pmod 4$, again contrary to assumption. Further, $p = 7$ implies $2^h \equiv -1 \equiv 6 \pmod 7$, but the powers of 2 modulo 7 are $\{1, 2, 4\}$, a contradiction.

We conclude that the group $G = C_{q+1} \cap \mathrm{P\Gamma L}(3,q)_{\mathcal{H}}$ is trivial.

Theorem 13 Let $q = 2^h$ where $h \equiv 0 \pmod 4$ and $q > 64$. The collineation stabiliser $\mathrm{P\Gamma L}(3,q)_{\mathcal{H}}$ of the Subiaco hyperoval $\mathcal{H} = \mathcal{D}(f)$ described above is a cyclic group of order $2h$. The homography stabiliser of $\mathcal{H}$ is a cyclic group of order 2, generated by ρ.

Proof: The preceding arguments show that the collineation stabiliser of $\mathcal{H}$ is a cyclic group of order $2h$. Comparing orders with Theorem 1 (2), we see that this group coincides with the stabiliser induced by the collineation group of the associated generalised quadrangle and the rest of the statement follows. ∎

Corollary 14 The collineation stabiliser of a Subiaco hyperoval in $\mathrm{PG}(2,q)$, where $q = 2^h$, $h \equiv 0 \pmod 4$ and $q \geq 256$ is a cyclic group of order $2h$. Further, its homography stabiliser is a cyclic group of order 2.

Proof: Since there is one orbit of Subiaco hyperovals under $\mathrm{P\Gamma L}(3,q)$ for these values of q, the result follows. ∎

3.3 The case $q = 2^h$ where h is odd

Since h is odd, by Theorem 1 (2), we can choose $d = 1$ since $\mathrm{trace}(1) = 1$ and $1+1+1 \neq 0$. In this case, the Subiaco hyperoval can be written as $\mathcal{H} = \mathcal{D}(f)$ where

$$f(t) = \frac{t^4+t^3+t^2+t}{(t^2+t+1)^2} + t^{\frac{1}{2}}$$

and the curve $\mathcal{C} = V(F)$ is such that

$$\begin{aligned} F(x,y,z) &= (z^2+xy)(x^2+xy+y^2)^4 + x^2y^8 + x^8y^2 + x^4y^6 + x^6y^4 \\ &= (x^2+y^2+z^2+xy)(x^2+xy+y^2)^4 + x^{10} + y^{10} \\ &= (x^2+xy+y^2)^5 + z^2(x^2+xy+y^2)^4 + x^{10} + y^{10}. \end{aligned} \tag{1}$$

As in Theorem 1, we already know that $\mathcal{H}$ is stabilised by a group of order $2h$. We will show that this is the full collineation stabiliser, first concentrating on the homography stabiliser.

Lemma 15 Let $q = 2^h$, where h is odd, and let $\mathcal{H} = \mathcal{D}(f)$ be the Subiaco hyperoval as described above. Then $\mathrm{PGL}(3,q)_{\mathcal{H}}$ is a group of order 2 generated by the homography $\rho\colon (x,y,z) \mapsto (y,x,z)$.

Proof: Let $\theta \in \mathrm{PGL}(3,q)_{\mathcal{H}}$, so θ can be written as a 3×3 matrix, which we also denote by θ. By Lemma 9, θ fixes $(0,0,1)$, so θ^{-1} is of the form

$$\theta^{-1} = \begin{pmatrix} a & b & 0 \\ e & f & 0 \\ g & h & 1 \end{pmatrix}$$

for some $a,b,e,f,g,h \in \mathrm{GF}(q)$. Further, over the algebraic closure γ of $\mathrm{GF}(q)$, θ fixes $\{(x,y,z)\colon x^2+xy+y^2=0\}$; so we have

$$\begin{aligned} & (ax+by)^2 + (ax+by)(ex+fy) + (ex+fy)^2 \\ =\ & x^2(a^2+ae+e^2) + xy(af+be) + y^2(b^2+bf+f^2) \\ =\ & \alpha(x^2+xy+y^2) \end{aligned} \tag{2}$$

for some $\alpha \in \mathrm{GF}(q)$, by [6, 2.6(v)]. It follows that

$$a^2+ae+e^2 = af+be = b^2+bf+f^2 = \alpha.$$

Since θ fixes $\mathcal{H} = \mathcal{C}$, if $F(x,y,z) = 0$ then $F((x,y,z)^{\theta^{-1}}) = 0$ also. Hence we obtain, using Equation (2) for simplification at the first step and substituting for $z^2(x^2+xy+y^2)^4$ using Equation (1) at the second step:

$$\begin{aligned} & F((x,y,z)^{\theta^{-1}}) = 0 \\ \Rightarrow\ & \alpha^5(x^2+xy+y^2)^5 + (gx+hy+z)^2\alpha^4(x^2+xy+y^2)^4 + (ax+by)^{10} \\ & \quad +(ex+fy)^{10} = 0 \\ \Rightarrow\ & \alpha^5(x^2+xy+y^2)^5 + \alpha^4(x^2+xy+y^2)^4(g^2x^2+h^2y^2) \\ & \quad +\alpha^4((x^2+xy+y^2)^5 + x^{10}+y^{10}) \\ & \quad +(a^5x^5 + ab^4xy^4 + a^4bx^4y + b^5y^5 + e^5x^5 \\ & \quad +ef^4xy^4 + e^4fx^4y + f^5y^5)^2 = 0 \quad \forall x,y \in \mathrm{GF}(q) \\ \Rightarrow\ & x^{10}(\alpha^5 + g^2\alpha^4 + a^{10} + e^{10}) + x^9y(\alpha^5+\alpha^4) \\ & \quad +x^8y^2(\alpha^5+\alpha^4+h^2\alpha^4+a^8b^2+e^8f^2) + x^6y^4(\alpha^5+g^2\alpha^4+\alpha^4) \\ & \quad +x^5y^5(\alpha^5+\alpha^4) + x^4y^6(\alpha^5+h^2\alpha^4+\alpha^4) \\ & \quad +x^2y^8(\alpha^5+\alpha^4+g^2\alpha^4+a^2b^8+e^2f^8) + xy^9(\alpha^5+\alpha^4) \\ & \quad +y^{10}(\alpha^5+h^2\alpha^4+b^{10}+f^{10}) = 0 \end{aligned}$$

for all $x, y \in \mathrm{GF}(q)$, not both zero. Thus each coefficient in the last equation must be zero. In particular, the coefficient of x^9y is $\alpha^5 + \alpha^4 = \alpha^4(\alpha+1) = 0$, implying that $\alpha = 0$ or 1. But if $\alpha = 0$ then the matrix θ is singular (since the determinant of θ^{-1} is $af + be = \alpha$), which is not possible. Thus $\alpha = 1$, and the coefficients of x^6y^4 and x^4y^6 imply that $g = h = 0$, respectively. We are left with the following four equations, corresponding to the coefficients $x^{10}, x^8y^2, x^2y^8, y^{10}$:

$$
\begin{aligned}
a^5 + e^5 &= 1, & (3)\\
a^4b + e^4f &= 0, & (4)\\
ab^4 + ef^4 &= 0, & (5)\\
b^5 + f^5 &= 1. & (6)
\end{aligned}
$$

Multiplying Equation (5) by b we obtain: $ab^5 + ebf^4 = 0$, hence $a(1+f^5) + ebf^4 = 0$ and so $f^4(af + be) + a = 0$, thus $a = f^4$. Similarly, multiplying Equation (4) by a yields $b = e^4$. Substituting for a in Equation (5) gives $f^4(b^4 + e) = 0$, so either $f = 0$ or $e = b^4$. If $f = 0$ then $a = f^4 = 0$ and Equations (3, 6) yield $b^5 = e^5 = 1$. Thus $b = e = 1$, since the greatest common divisor $(2^h - 1, 5) = 1$ (as h is odd and an odd power of 2 modulo 5 is never 1). In this case θ is the collineation ρ and it is straightforward to verify that ρ fixes $\mathcal{H}$. In a similar way, using Equation (4), it follows that either $e = 0$ or $f = a^4$. If $e = 0$ then analogous arguments show that θ is the identity collineation.

We are left to consider the case in which $e = b^4$ and $f = a^4$. Since $b = e^4$ and $a = f^4$, it follows that $a^{15} = e^{15} = 1$; hence $a = e = 1$, since the greatest common divisor $(15, q-1) = (2^4-1, 2^h-1) = (4, h) = 1$ as h is odd. It follows that $b = f = 1$ and

$$
\theta^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
$$

which is impossible since then the determinant of θ^{-1} would be 0. ■

Theorem 16 In $\mathrm{PG}(2, q)$, where $q = 2^h$, h is odd and $q > 64$, let $\mathcal{H} = \mathcal{D}(f)$ be the Subiaco hyperoval described above. Then $\mathrm{P\Gamma L}(3, q)_{\mathcal{H}}$ is a cyclic group of order $2h$, generated by ρ and the automorphic collineation $(x, y, z) \mapsto (x^2, y^2, z^2)$. The homography stabiliser of $\mathcal{H}$ is a cyclic group of order 2, generated by ρ.

Proof: By Lemma 15, the homography stabiliser of $\mathcal{H}$ is $\langle\rho\rangle$, a cyclic group of order 2. Further, since $f(t)$ has coefficients in $\mathrm{GF}(2)$, it follows that $\mathcal{H}$ is fixed by the group A of automorphic collineations, so the homography stabiliser of $\mathcal{H}$ has index h in the collineation stabiliser. Thus the collineation stabiliser of $\mathcal{H}$ is $\langle\langle\rho\rangle, A\rangle = \langle\rho\rangle \times A$. This is a cyclic group of order $2h$. ■

Corollary 17 The collineation stabiliser of a Subiaco hyperoval in $\mathrm{PG}(2, q)$, where $q = 2^h$, $q \geq 32$ and h is odd, is a cyclic group of order $2h$. Further, its homography stabiliser is a cyclic group of order 2.

Proof: The case $q = 32$ was discussed in Section 1. Suppose $q \geq 128$. A Subiaco hyperoval is equivalent to the hyperoval $\mathcal{H}$ above, its collineation (respectively homography) stabiliser is conjugate in $\mathrm{P\Gamma L}(3, q)$ (respectively $\mathrm{PGL}(3, q)$) to the stabiliser of $\mathcal{H}$, and the result follows. ■

4 Collineations of Cherowitzo hyperovals and sets

For this section, we suppose that $q = 2^h$ where $h \geq 5$ is odd. Let $\sigma \in \mathrm{AutGF}(q)$ be such that $\sigma^2 \equiv 2 \pmod{q-1}$, and define a *Cherowitzo set* to be the set of points

$$\mathcal{H} = \{(1, t, f(t)) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0), (0,0,1)\}$$

where $f(t) = t^\sigma + t^{\sigma+2} + t^{3\sigma+4}$. For $5 \leq h \leq 15$, a Cherowitzo set is a Cherowitzo hyperoval [4].

In the following we write $h = 2e+1$, so that $\sigma = 2^{e+1}$. Taking account of [10], we only need consider $h \geq 7$, that is, $e \geq 3$.

4.1 Cherowitzo sets and algebraic curves

In homogeneous coordinates (x, y, z), the point $(1, t, f(t))$ satisfies the equation $F(x, y, z) = 0$, with

$$F(x,y,z) = x^{3\sigma+3}z + x^{2\sigma+4}y^\sigma + x^{2\sigma+2}y^{\sigma+2} + y^{3\sigma+4}.$$

We define the algebraic curves $\mathcal{C} = V(F)$ in $\mathrm{PG}(2, q)$ and $\widehat{\mathcal{C}} = V(F)$ in $\mathrm{PG}(2, \gamma)$ where γ is the algebraic closure of $\mathrm{GF}(q)$.

Lemma 18 In $\mathrm{PG}(2, q)$, we have $\mathcal{C} \cup \{(0,1,0)\} = \mathcal{H}$.

Proof: First, $\mathcal{C}$ and $\mathcal{H}$ coincide on the set of points (x, y, z), $x \neq 0$. Further, the line $x = 0$ meets $\mathcal{C}$ in the unique point $(0,0,1)$ and meets $\mathcal{H}$ in the points $(0,1,0), (0,0,1)$. ∎

Lemma 19 The curve $\widehat{\mathcal{C}}$ has a unique multiple point $(0,0,1)$ of multiplicity $3\sigma+3$. The line $x = 0$ is the unique tangent to $\widehat{\mathcal{C}}$ at $(0,0,1)$. Further, each tangent to $\widehat{\mathcal{C}}$ passes through the point $(0,1,0)$.

Proof: The multiple points of $\widehat{\mathcal{C}}$ are the solutions of the following system of equations:

$$\begin{aligned} F(x,y,z) &= 0, \\ F_x(x,y,z) &= x^{3\sigma+2}z = 0, \\ F_z(x,y,z) &= x^{3\sigma+3} = 0, \end{aligned}$$

noting that $F_y(x, y, z) = 0$. The only solution is $x = y = 0$, and we have found the multiple point $(0,0,1)$, of multiplicity $3\sigma+3$. The tangent $x = 0$ to $\widehat{\mathcal{C}}$ at $(0,0,1)$ has multiplicity $3\sigma+3$ and passes through $(0,1,0)$. The tangent to $\widehat{\mathcal{C}}$ at the point (x_0, y_0, z_0) is the line with equation $x_0^{3\sigma+2}z_0 x + x_0^{3\sigma+3}z = 0$, which passes through $(0,1,0)$. ∎

Lemma 20 The curve $\mathcal{C}$ is absolutely irreducible.

Proof: Since $\widehat{\mathcal{C}}$ has a unique singular point, each irreducible factor of F over γ has multiplicity one. Suppose that $\widehat{\mathcal{C}}$ has irreducible components $\mathcal{C}_1, \dots, \mathcal{C}_r$, $r > 1$, with $\deg(\mathcal{C}_i) = n_i$. Since $\widehat{\mathcal{C}}$ has order $3\sigma + 4$ and $(0, 0, 1)$ is a point of multiplicity $3\sigma + 3$, it follows that $(0, 0, 1)$ has multiplicity n_i for $r - 1$ of these irreducible components, say $\mathcal{C}_1, \dots, \mathcal{C}_{r-1}$ (for $\mathcal{C}_i$ has a point of multiplicity m_i at $(0, 0, 1)$, where $n_i \geq m_i$, $n_1 + \dots + n_r = 3\sigma + 4$ and $m_1 + \dots + m_r = 3\sigma + 3$). Since $\mathcal{C}_i$ is irreducible, each of the curves $\mathcal{C}_1, \dots, \mathcal{C}_{r-1}$ is a line through $(0, 0, 1)$, necessarily coinciding with the unique tangent $x = 0$ to $\widehat{\mathcal{C}}$ at $(0, 0, 1)$. But $x = 0$ is not a component of $\widehat{\mathcal{C}}$; a contradiction. ■

4.2 Collineations of Cherowitzo sets

Lemma 21 Let $\theta \in \mathrm{PGL}(3, q)_{\mathcal{H}}$, $q = 2^{2e+1}$ with $e \geq 3$. If θ fixes the point $(0, 0, 1)$ then θ is the identity collineation.

Proof: Suppose, aiming for a contradiction, that $\widehat{\mathcal{C}}^{\theta} \neq \widehat{\mathcal{C}}$. The point $(0, 0, 1)$ is a point of multiplicity $3\sigma + 3$ on each of the curves $\widehat{\mathcal{C}}$ and $\widehat{\mathcal{C}}^{\theta}$. Further, since θ fixes $\mathcal{H}$, it follows that $\widehat{\mathcal{C}}$ and $\widehat{\mathcal{C}}^{\theta}$ have at least $q - 1$ further common points, each of multiplicity one on each curve. Thus, by Result 3,

$$(3\sigma + 4)^2 \geq \sum_{P \in \widehat{\mathcal{C}} \cap \widehat{\mathcal{C}}^{\theta}} m_P(\widehat{\mathcal{C}}^{\theta}) m_P(\widehat{\mathcal{C}}) \geq (3\sigma + 3)^2 + q - 1,$$

hence

$$2^{2e-2} - 3.2^{e-1} - 1 \leq 0,$$

which is impossible for $e \geq 3$. Thus $\widehat{\mathcal{C}}^{\theta} = \widehat{\mathcal{C}}$, and, since $(0, 1, 0)$ is the point of intersection of the tangents to $\widehat{\mathcal{C}}$, it follows that $(0, 1, 0)$ is also fixed by θ.

We can assume without loss of generality that

$$\theta^{-1} = \begin{pmatrix} a & 0 & 0 \\ b & c & 0 \\ d & 0 & 1 \end{pmatrix}$$

for some $a, b, c, d \in \mathrm{GF}(q)$ satisfying $ac \neq 0$. Since θ fixes $\mathcal{C}$, if $F(x, y, z) = 0$ then $F((x, y, z)^{\theta^{-1}}) = 0$. Hence,

$$\begin{aligned}
& F((x, y, z)^{\theta^{-1}}) = 0 \\
\Rightarrow\ & (ax)^{3\sigma+3}(dx + z) + (ax)^{2\sigma+4}(bx + cy)^{\sigma} + (ax)^{2\sigma+2}(bx + cy)^{\sigma+2} \\
& \quad +(bx + cy)^{3\sigma+4} = 0 \qquad \text{and } F(x, y, z) = 0 \\
\Rightarrow\ & x^{3\sigma+4}(a^{3\sigma+3}d + a^{2\sigma+4}b^{\sigma} + a^{2\sigma+2}b^{\sigma+2} + b^{3\sigma+4}) + x^{3\sigma+2}y^2(a^{2\sigma+2}b^{\sigma}c^2) \\
& +x^{3\sigma}y^4(b^{3\sigma}c^4) + x^{2\sigma+4}y^{\sigma}(a^{3\sigma+3} + a^{2\sigma+4}c^{\sigma} + a^{2\sigma+2}b^2c^{\sigma} + b^{2\sigma+4}c^{\sigma}) \\
& +x^{2\sigma+2}y^{\sigma+2}(a^{3\sigma+3} + a^{2\sigma+2}c^{\sigma+2}) \\
& +x^{2\sigma}y^{\sigma+4}(b^{2\sigma}c^{\sigma+4}) + x^{\sigma+4}y^{2\sigma}(b^{\sigma+4}c^{2\sigma}) \\
& \quad +x^{\sigma}y^{2\sigma+4}(b^{\sigma}c^{2\sigma+4}) + x^4y^{3\sigma}(b^4c^{3\sigma}) + y^{3\sigma+4}(a^{3\sigma+3} + c^{3\sigma+4}) = 0,
\end{aligned}$$

for all $x, y \in \mathrm{GF}(q)$. It follows that each coefficient in this expression must be zero. As $ac \neq 0$, considering the coefficient of $x^{3\sigma}y^4$, we see that $b = 0$. Looking at the coefficient of $x^{3\sigma+4}$ implies that $d = 0$. Then the coefficients of $x^{2\sigma+4}y^{\sigma}$ and $x^{2\sigma+2}y^{\sigma+2}$ together show that $a = c$, and the coefficient of $y^{3\sigma+4}$ is used to show that $a = 1$. Thus θ is the identity collineation. ∎

Lemma 22 Let $\theta \in \mathrm{PGL}(3,q)_{\mathcal{H}}$, $q = 2^{2e+1}$ with $e \geq 3$. If θ fixes the point $(0,1,0)$ then θ is the identity collineation.

Proof: First, we calculate the intersection multiplicity at $(1,t,f(t))$ of $\widehat{\mathcal{C}}$ with the tangent $\ell_t : (t^{\sigma} + t^{\sigma+2} + t^{3\sigma+4})x + z = 0$ to $\widehat{\mathcal{C}}$ at the point $(1,t,f(t))$, $t \in \mathrm{GF}(q)$. A point (x,y,z) is in the intersection of $\widehat{\mathcal{C}}$ and ℓ_t if and only if

$$\begin{aligned} & x^{3\sigma+3}(t^{\sigma} + t^{\sigma+2} + t^{3\sigma+4})x + x^{2\sigma+4}y^{\sigma} + x^{2\sigma+2}y^{\sigma+2} + y^{3\sigma+4} = 0 \\ \Leftrightarrow\quad & t^{\sigma} + t^{\sigma+2} + t^{3\sigma+4} = Y^{\sigma} + Y^{\sigma+2} + Y^{3\sigma+4}, \qquad \text{where } Y = y/x \\ \Leftrightarrow\quad & Y^{\sigma} + t^{\sigma} + (Y^{\sigma})^{1+\sigma} + (t^{\sigma})^{1+\sigma} + (Y^{\sigma})^{3+2\sigma} + (t^{\sigma})^{3+2\sigma} = 0 \\ \Leftrightarrow\quad & (Y+t)^{\sigma}\left(1 + \sum_{i=0}^{\sigma}(Y^{\sigma})^{\sigma-i}(t^{\sigma})^{i} + \sum_{i=0}^{2\sigma+2}(Y^{\sigma})^{2+2\sigma-i}(t^{\sigma})^{i}\right) = 0. \end{aligned}$$

The factor $(Y+t)^{\sigma}$ contributes σ to the intersection multiplicity at the point $(1,t,f(t))$, since this is the point for which $Y = t$. There is a further contribution to this intersection multiplicity if and only if

$$\begin{aligned} & 1 + \sum_{i=0}^{\sigma}(t^{\sigma})^{\sigma-i}(t^{\sigma})^{i} + \sum_{i=0}^{2\sigma+2}(t^{\sigma})^{2+2\sigma-i}(t^{\sigma})^{i} = 0 \\ \Leftrightarrow\quad & 1 + \sum_{i=0}^{\sigma} t^{\sigma^2} + \sum_{i=0}^{2\sigma+2} t^{2\sigma+2\sigma^2} = 0 \\ \Leftrightarrow\quad & 1 + t^2 + t^{2\sigma+4} = 0. \end{aligned}$$

Since in $\mathrm{PG}(3,q)$ the plane $z = 0$ is tangent to the Tits ovoid with equation $z = xy + x^{\sigma+2} + y^{\sigma}$ at the point $(1,0,0,0)$ ([7, Theorem 16.4.5]), it follows that $(0,0)$ is the only solution of the equation $xy + x^{\sigma+2} + y^{\sigma} = 0$. Putting $y = 1$, we see that the equation $1 + x + x^{\sigma+2} = 0$ has no solution, hence, putting $x = t^2$, the equation $1 + t^2 + t^{2\sigma+4} = 0$ has no solution; so the multiplicity of the intersection of $\widehat{\mathcal{C}}$ with the tangent ℓ_t to $\widehat{\mathcal{C}}$ at the point $(1,t,f(t))$, $t \in \mathrm{GF}(q)$, is exactly σ at $(1,t,f(t))$.

Suppose now that θ does not fix $(0,0,1)$, and count the points in $\widehat{\mathcal{C}} \cap \widehat{\mathcal{C}}^{\theta}$, according to their multiplicities. The points $(0,0,1)$ and $(0,0,1)^{\theta}$ each contribute $3\sigma + 4$ to the intersection, and each further point of intersection is a simple point on each curve. By Lemma 4, in $PG(2,q)$, such a simple point contributes at least σ to the intersection. Thus

$$\begin{aligned} \sum_{P \in \widehat{\mathcal{C}} \cap \widehat{\mathcal{C}}^{\theta}} m_P(\widehat{\mathcal{C}}^{\theta}) m_P(\widehat{\mathcal{C}}) & \geq 2(3\sigma + 4) + (q-1)\sigma \\ & = 2^{3e+2} + 5.2^{e+1} + 8. \end{aligned}$$

By Lemma 3, since $\mathcal{C}$ and hence also $\mathcal{C}^{\theta}$ are absolutely irreducible, if $\widehat{\mathcal{C}}^{\theta} \neq \widehat{\mathcal{C}}$ then $2^{3e+2} + 5.2^{e+1} + 8 \leq (3\sigma + 4)^2$; implying that $2^{3e+2} - 9.2^{2e+2} - 19.2^{e+1} - 8 \leq 0$; impossible for $e \geq 3$. Thus $\widehat{\mathcal{C}}^{\theta} = \widehat{\mathcal{C}}$. By Result 2, the unique multiple point $(0,0,1)$ of $\widehat{\mathcal{C}}$ is fixed by θ. This contradiction shows that $(0,0,1)$ is fixed by θ, and Lemma 21 shows that θ is the identity collineation. ∎

Theorem 23 Let $q = 2^h$ where $h \geq 7$ is odd. Let $\mathcal{H}$ be the Cherowitzo set as defined above (and hence a Cherowitzo hyperoval for $h \leq 15$). A collineation which fixes $\mathcal{H}$ and which fixes either $(0, 1, 0)$ or $(0, 0, 1)$ must be an automorphic collineation.

Proof: Lemmas 22, 21. ∎

Acknowledgement: This work was supported by the Australian Research Council and the University Research Scheme of the University of Adelaide.

References

[1] V. Abatangelo and B. Larato, A characterisation of Denniston's maximal arcs, *Geom. Dedicata* **30** (1989), 197–203.

[2] L. Bader, G. Lunardon and S.E. Payne, On q-clan geometry, $q = 2^e$, *Bull. Belgian Math. Soc. - Simon Stevin* **1** (1994), 301–328.

[3] W.E. Cherowitzo, Hyperovals in Desarguesian planes of even order, *Ann. Discrete Math.* **37** (1988), 87–94.

[4] W.E. Cherowitzo, personal communication, 1994.

[5] W. Cherowitzo, T. Penttila, I. Pinneri, G.F. Royle, Flocks and ovals, *Geom. Dedicata,* **60**(1996),17–37.

[6] J.W.P. Hirschfeld, *Projective geometries over finite fields*, Oxford University Press, Oxford, 1979.

[7] J.W.P. Hirschfeld, *Finite projective spaces of three dimensions*, Oxford University Press, Oxford, 1985.

[8] W.M. Kantor, Some generalized quadrangles with parameters (q^2, q), *Math. Z.* **192** (1986), 45–50.

[9] L. Lunelli and M. Sce, k-archi completi nei piani proiettivi desarguesiani di rango 8 e 16, *Centro di Calcoli Numerici,* Politecnico di Milano, 1958.

[10] C.M. O'Keefe, T. Penttila and C.E. Praeger, Stabilisers of hyperovals in $\mathrm{PG}(2, 32)$, in *Advances in finite geometries and designs,* Oxford University Press, Oxford, 1991, pp 337–357.

[11] S.E. Payne, Generalized quadrangles as group coset geometries, *Congr. Numer.* **29** (1980), 717–734.

[12] S.E. Payne, A new infinite family of generalized quadrangles, *Congr. Numer.* **49** (1985), 115–128.

[13] S.E. Payne, Collineations of the Subiaco generalized quadrangles, *Bull. Belgian Math. Soc. - Simon Stevin* **1** (1994), 427–438.

[14] S.E. Payne, A tensor product action on q-clan generalized quadrangles with $q = 2^e$, *Linear Alg. and Appl.* **226–228** (1995), 115–137.

[15] S.E. Payne and J.E. Conklin, An unusual generalized quadrangle of order sixteen, *J. Combin. Theory Ser. A* **24** (1978), 50–74.

[16] S.E. Payne, T. Penttila and I. Pinneri, Isomorphisms between Subiaco q-clan geometries, *Bull. Belgian Math. Soc. - Simon Stevin,* **2** (1995), 197–222.

[17] T. Penttila and I. Pinneri, Irregular hyperovals in $\mathrm{PG}(2, 64)$, *J. Geom.,* **51** (1994), 89–100.

[18] T. Penttila and G.F. Royle, On hyperovals in small projective planes, *J. Geom.,* **54** (1995), 91–104.

[19] L. Storme and J.A. Thas, k-arcs and partial flocks, *Linear Alg. and Appl.,* **226–228** (1995), 33–45.

[20] J.A. Thas, Generalized quadrangles and flocks of cones, *European J. Combin.* **8** (1987), 441–452.

[21] J.A. Thas, S.E. Payne and H. Gevaert, A family of ovals with few collineations, *European J. Combin.* **9** (1988), 353–362.

C.M. O'Keefe
Department of Pure Mathematics
The University of Adelaide
Adelaide, South Australia 5005
AUSTRALIA
cokeefe@maths.adelaide.edu.au

J.A. Thas
Department of Pure Mathematics and Computer Algebra
University of Gent
Krijgslaan 281
B-9000 Gent
BELGIUM
jat@cage.rug.ac.be