Hyperovals

Tim Penttila

Department of Mathematics, University of Western Australia,
Nedlands 6009, Western Australia, Australia
e-mail: penttila@maths.uwa.edu.au

Ivano Pinneri

Dipartimento di Matematica,
Universita di Roma 'La Sapienza', 2-00185 Roma, Italy
e-mail: ivano@maths.uwa.edu.au

Abstract

We investigate elations and generalised homologies stabilising hyperovals in arbitrary projective planes of even order. In particular, examples of such stabilisers are given which include the known hyperovals in $PG(2,q)$ and the recently constructed hyperovals in the projective planes of order 16 [18]. We also give a proof that the infinite family of hyperovals constructed by Cherowitzo [3, 2] are new.

1 Introduction

A k-**arc** in a projective plane of order q is a set of k points with no three collinear. If q is odd then a k-arc can have size at most $q+1$ and is called an **oval**. It is well known that a non-degenerate conic (the zeroes of a non-degenerate quadratic form) is an oval in $PG(2,q)$ (the Desarguesian projective plane of order q). A famous theorem of Segre's [21] asserts that conics are the only ovals in the projective plane $PG(2,q)$ when q is odd.

When q is even any oval can be extended to a $q+2$-arc by the addition of a unique point called the **nucleus** of the oval — being the intersection of all tangent lines to the oval. The resulting $(q+2)$-arc (the maximum possible size for a k-arc) is called a **hyperoval**. A non-degenerate conic, together with its nucleus forms a hyperoval called the **regular** hyperoval. Unfortunately there is no analogy of Segre's theorem, characterising hyperovals in $PG(2,q)$, and in fact several infinite families of hyperovals are known. Classification of hyperovals is of great interest, partly due to their connections with other combinatorial objects particularly ovoids, inversive planes, generalised quadrangles and flocks of the quadratic cone. One approach of classification is to determine the possible configurations that can stabilise a hyperoval. Further background to ovals and hyperovals in $PG(2,q)$ may be found in Hirschfeld [7].

This paper shows the possible geometric configuration that one or two elations can have stabilising a hyperoval. (Three elations are investigated briefly.) Examples of hyperovals stabilised by each of the possible configurations are given. The configurations for two elations are stated in Theorem 11. Part (3) of this Theorem motivates our study of generalised homologies stabilising hyperovals (Section 4). Theorem 15 summarises all the above results. For the rest of this paper we work in $PG(2,q)$ where q is even and not a square. We summarise most of the known hyperovals together with their full stabiliser groups (Table 1) which, in turn, are needed in the the proof that the Cherowitzo hyperovals are new.

2 Introduction to Collineation Groups

Unless otherwise stated in Sections 1 to 4, q is not necessarily of prime power order.

Let $g \in \operatorname{Aut} \pi$ for a projective plane π. The we say g **fixes a point**, P, if $gP = P$. We say g **fixes a line** if it fixes the line setwise. We denote by $\operatorname{Fix}(g)$ the fixed configuration of g.

Further information on collineation groups for projective planes may be found in [5].

Theorem 1 ([6]). *In a finite projective plane a collineation fixes the same number of points and lines.*

Hence a group generated by a collineation has the number of fixed points equal to the number of fixed lines.

If g fixes a line l pointwise then we say g has **axis** l. If g fixes a point linewise then we say that g has **centre** P. If $g \neq 1$ then it has at most one centre and one axis, else it would fix the whole plane.

Let $g \neq 1$ have axis l and centre P. Then g is an **elation** if $P \in l$ and a **homology** otherwise. (By convention the identity is both an elation and a homology.)

The (cyclic) group generated by an elation or a homology acts semiregularly on points not equal to the centre and not on the axis. Hence in a projective plane of order q the order of an elation divides q and the order of a homology divides $q-1$. Consequently, a non-trivial homology does not stabilise a hyperoval.

We say l is a **translation line** if for all P incident with l we have for every pair of distinct points Q, R where Q, R, P collinear and Q, R not on l, there exists an elation g with centre P and axis l such that $gQ = R$.

If a projective plane, π, has a translation line then we say π is a **translation plane**. The projective plane $PG(2,q)$ is a translation plane where every line is a translation line.

3 Collineation Groups Stabilising Hyperovals

In a projective plane, π, of order q a **translation q-arc**, is a q-arc whose stabiliser in the full automorphism group of π contains a group of elations acting transitively on its q points. A **translation hyperoval** is a hyperoval that contains a translation q-arc $\mathcal{K}$. Since the group is transitive, the axis of the group of elations is external to $\mathcal{K}$.

A **semi-translation hyperoval** [18] is a hyperoval with an elation group with common axis in its stabiliser each of whose orbits not on the axis, together with the points of the hyperoval on the common axis forms a translation hyperoval of a Baer subplane (cf. Ostrom's definition [14] of a semi-translation plane).

We now begin investigating the behaviour of elations with respect to the hyperovals they stabilise.

An **involution** is a collineation of order 2.

Theorem 2. *An elation stabilising a hyperoval is involutory.*

Proof. The group generated by the elation acts semi-regularly on the non-fixed points, but interchanges the points of secancy on any non-axial secant line on the centre; thus the group has order 2. □

Example. The complement of a line is a hyperoval in $PG(2,2)$. It is stabilised by all elations with centre on the line. Those with axis different from the line have axis secant to the hyperoval, while those with axis equal to the line have axis external to the hyperoval. The stabiliser of the hyperoval is S_4. The elations with axis external to the hyperoval generate a Klein four group C_2^2. The elations with axis secant to the hyperoval generate the whole stabiliser. Each point not on the hyperoval is the centre of exactly three elations stabilising the hyperoval.

Theorem 3 ([8])**.** *If π is a projective plane of order $q \equiv 2 \pmod 4$ and if π possesses an elation, then $q = 2$.*

Theorem 4 ([17])**.** *An elation stabilising a hyperoval has centre not on the hyperoval and, if the plane has order greater than two, has axis secant to the hyperoval.*

Proof. By the proof of Theorem 2, the centre is not on the hyperoval. By Theorems 2 and 3, the order of the plane is not congruent to 2 modulo 4 if it is bigger than 2. Thus, there are an odd number of secant lines on the fixed point not equal to the centre of the elation, from which it follows that the unique fixed line on this point (namely, the axis) is a secant line. □

We now investigate the possibilities of two distinct non-identity elations stabilising a hyperoval.

Theorem 5. *A planar collineation fixing a hyperoval either has its fixed subplane disjoint from the hyperoval or they intersect in a hyperoval of the fixed subplane.*

Proof. If a fixed line contains a fixed point on the hyperoval, then it is a secant line, so it contains two fixed points. Thus the set of fixed points on the hyperoval is set of points of the fixed subplane of class $[0,2]$, so is either empty or a hyperoval. □

Example. A regular hyperoval in $PG(2,4)$ has stabiliser isomorphic to S_6. It has three types of involutions in its stabiliser: Baer involutions fixing no points of the hyperoval, Baer involutions fixing four points of the hyperoval and elations fixing two points of the hyperoval. Each point not on the hyperoval is the centre of exactly three elations stabilising the hyperoval.

Theorem 6 ([1]). *Two distinct nonidentity elations stabilising a hyperoval in a projective plane of order q with $q > 4$ have distinct centres.*

Proof. If not, then, for each secant line on the common centre that is not the axis of either of the elations, the points of secancy are interchanged by both elations, so their product fixes an arc of size at least $q-2$ which is greater than $\sqrt{q}+2$, so lies in no proper subplane. Thus their product is the identity, contrary to their being distinct. □

Theorem 7 ([1]). *Two distinct Baer involutions fixing a hyperoval have distinct fixed planes.*

Proof. If not, any point P of the hyperoval not in the common fixed subplane has the line joining it and its image (under either of the involutions) in the subplane. This is a secant line and the image of P under each involution must therefore be the other point of secancy, so P is fixed by the product of the involutions; thus the fixed configuration of the product of the involutions is the whole plane, that is, the product is the identity, that is, the involutions are not distinct. □

Theorem 8 ([20]). *The product of two involutorial elations, the centre of each of which is not incident with the axis of the other, fixes no point not on the line joining the two centres and not equal to the intersection of the two axes.*

Proof. Suppose not and let g be the product of the two involutions. Then, since the intersection P of the axes, the line l joining the centres, and some point Q not on the line are fixed by g, g fixes the line $m = PQ$, and so the point R of intersection of l and m. Thus g fixes three collinear points on m. It follows that if g is not planar, then m is the unique line containing more than two fixed points of g. The elations invert g, but do not both fix m, so g is planar. Thus the elations fix the fixed subplane π_0 of g. They induce involutions of π_0 with all fixed points collinear, so these must be elations. But these induced involutions commute, contrary to the original hypothesis. □

Theorem 9 ([20]). *The group H generated by the product of two involutorial elations g and h, the centre of each of which is not incident with the axis of the other, acts semiregularly on the points not on the line joining the two centres and not equal to the intersection of the two axes.*

Proof. Let G be the group generated by g and h. Then G is a dihedral group with H as a cyclic subgroup of index 2. Each nonidentity element of H is the product of two distinct elements of G that are not in H. Each of the elements of G that are not in H are involutions that are conjugate either to g or to h, and so are elations. Moreover, any two such have the property that the centre of each of them is not incident with the axis of the other. Thus Theorem 8 applies, and any nonidentity element of H fixes no point not on the line joining the two centres and not equal to the intersection of the two axes. □

Theorem 10 ([20]). *The product of two involutorial elations g and h of a projective plane of order q, the centre of each of which is not incident with the axis of the other, has order dividing $q^2 - 1$ and not equal to one.*

Proof. This follows from Theorem 9. □

We can now characterise the way two elations can stabilise a hyperoval.

Theorem 11 ([1]). *If two distinct elations stabilise a hyperoval in a plane of order q, then one of the following situations occurs:*

1. *the elations have different centres but the same axis, which is a secant line to the hyperoval, and the product of the two elations is an involutory elation with the same axis but a different centre; or*
2. *the axes are distinct and meet at a point of the hyperoval, the centres are distinct and the line joining the centres is*
   (a) *a secant line and the product of the elations has order dividing $q - 1$; or*
   (b) *external line, and the product of the elations has order dividing $q + 1$; or*
3. *the axes are distinct secant lines which meet at a point not on the hyperoval, the centres are distinct and the line joining them is external to the hyperoval, the product of the elations has order 3, and q is congruent to 1 modulo 3; or*
4. *q is 2 or 4.*

Proof. Suppose that $q > 4$, so that we are not in case (4). Then by Theorem 4, the axes are secant lines. If they are not distinct, then, by Theorem 6, they have different centres and case (1) arises. If they are distinct then their intersection is not the centre of either of the elations, as then, conjugating the first elation (which has centre the intersection of the two axes) by the second elation we obtain an elation with the same centre as the first elation but a different axis. Thus there would be two elations with the same centre fixing the hyperoval contrary to Theorem 6. Now Theorems 9 and 10, apply, and the group generated by their product has order dividing $q^2 - 1$ and acts semi-regularly on the points of the hyperoval not on the line joining the centres and not the intersection of the axes. If the axes meet at a point of the hyperoval, then either the line joining the centres is secant and the order of the product divides $q - 1$ or the line joining the centres is external and the order of the product divides $q+1$, which are cases (2)(a) and (2)(b), respectively. If the axes meet at a point not on the hyperoval, then the line joining the centres cannot be a secant line, for then the order of the product would be a nontrivial divisor of q^2-1 and q, which are coprime. So it is external and the order of the product is a nontrivial divisor of q^2-1 and $q+2$, from which it follows that it is 3 and that q is congruent to 1 modulo 3. This is case (3). □

The examples after Theorems 2 and Theorem 5 show that case (4) in the above theorem is genuinely exceptional.

Examples. For details about the hyperovals listed below see Section 5 or references [4, 19].

1. Translation hyperovals and semi-translation hyperovals give examples of (1) of Theorem 11.

2. Regular hyperovals in the Desarguesian plane give examples of (2)(a) of Theorem 11.

3. Regular hyperovals and the first class of Subiaco hyperovals, for $q=4^e$, e odd, give examples of (2)(b) of Theorem 11.

4. The regular hyperoval in $PG(2,4)$ and the Lunelli-Sce hyperoval in $PG(2,16)$ give examples of (3) of Theorem 11.

The work on when three distinct nonidentity elations can stabilise a hyperoval is still preliminary. Of use are Theorems 12 and 13.

Theorem 12 ([1][16]). *If q is not congruent to 1 modulo 3 and not equal to 2 then there is no hyperoval in a projective plane of order q which is stabilised by three elations whose axes form a triangle.*

Proof. In these cases, (1), (3) and (4) cannot apply to any two of these elations, so that (2) holds. But now two of the elations generate a dihedral group containing an odd number of elations, all with distinct axes, all meeting at a point on the hyperoval; the third elation cannot have axis meeting all of these axes on the hyperoval. □

Theorem 13 ([20]). *In a group of a projective plane of order $q>4$ containing involutory elations and fixing no point or line all elations are conjugate.*

4 Generalised Homologies

Let $g \in \mathrm{Aut}\,\pi$, with $t+1$ fixed points on l and $t+1$ fixed lines on C, with $C \notin l$. Then g is a **generalised homology (of order t)**. We say g has **pseudo-axis** l and **pseudo-centre** C. If $t=2$ then the centre and axis are not unique for a generalised homology (since we have a triangle cf. Theorem 12). Of course when $t=q$ we have a homology. Similarly we can define a **generalised elation (of order t)** with pseudo-centre C incident with pseudo-axis l.

Below we show that even though homologies can not stabilise hyperovals, some generalised homologies can.

Theorem 14 **([16]).** *Any nonidentity generalised homology of prime order stabilising a hyperoval in a projective plane of order q has at most $(q+2)/2$ fixed points. If it has more than three fixed points, then it has order* 3*, and q is congruent to* 1 *modulo* 3*.*

Proof. A generalised homology of a projective plane containing a hyperoval has odd order. Thus, if the generalised homology is not the identity, every orbit of points on a fixed line that is not just a fixed point contains a triple of collinear points. If the generalised homology has more than three fixed points then it has unique pseudo-centre and pseudo-axis, the pseudo-centre is not on the hyperoval and the pseudo-axis is external to the hyperoval. (If the pseudo-centre were on the hyperoval, then each fixed line on the pseudo-centre would be secant to the hyperoval, so each fixed point of the pseudo-axis would be on the hyperoval, so the pseudo-axis would meet the hyperoval in more than two points. So the pseudo-centre is not on the hyperoval, making the fixed lines on the pseudo-centre external, and so the pseudo-axis external.) There are $(q+2)/2$ secant lines on the pseudo-centre, none of which are fixed. So there are at most $q/2$ fixed lines on the pseudo-centre, giving at most $(q+2)/2$ fixed points. The group generated by the generalised homology acts semi-regularly on the $(q{+}2)/2$ secant lines through the pseudo-centre. Thus the generalised homology has order 3, since a generalised homology of prime order has order dividing $q-1$. □

Example **([18]).** In the dual Hall plane of order 16, there is a hyperoval stabilised by a generalised homology of order 3 with 6 fixed points. The full stabiliser is dihedral of order 6 with the involutions being Baer. In the dual Dempwolff plane of order 16, there is a hyperoval stabilised by a generalised homology of order 3 with 9 fixed points, which gives equality in the bound. The full stabiliser is cyclic of order 6 with the involution being Baer. In the semifield plane of order 16 with kernel $GF(2)$, there is a hyperoval stabilised by a generalised homology of order 3 with 6 fixed points. In this case, the full stabiliser has order 3. These are the only hyperovals in the known planes of order 16 stabilised by generalised homologies with more than three fixed points.

In summary we can organise the statements of Sections 3 and 4 into the below theorem.

Theorem 15. *Let $\mathcal{H}$ be a hyperoval in the projection plane π of order q, and let g be an element of prime order p in the stabiliser of $\mathcal{H}$ in* $\operatorname{Aut}\pi$*. Then one of the following holds:*

1. *g is planar with* $\operatorname{Fix}(g)$ *a subplane of order n and p divides $q-n$*

   (a) *if $p=2$ then either*

      (i) *n is even and* $\operatorname{Fix}(g)$ *intersect $\mathcal{H}$ is a hyperoval of* $\operatorname{Fix}(g)$*; here each line of* $\operatorname{Fix}(g)$ *is secant to $\mathcal{H}$, or;*

(ii) Fix(g) *is disjoint from $\mathcal{H}$; here exactly $(q+2)/2$ of the lines of* Fix(g) *are secant to $\mathcal{H}$.*

(b) *if $p \neq 2$ then either*

(i) *exactly $(n+2)(n+1)/2$ of the secant lines are fixed, if the fixed plane meets the hyperoval, or;*

(ii) *none of the secant lines are fixed, if the fixed plane is disjoint from the hyperoval;*

2. *g fixes exactly three non-collinear points, p divides $q-1$ and the three fixed points of g are on $\mathcal{H}$.*

3. *g is a generalised homology with pseudo-axis external to $\mathcal{H}$ and pseudo-centre not on $\mathcal{H}$ fixing m points with m congruent to 0 modulo 3 and m at most $(q+2)/2$; here $p=3$ and q is congruent to 1 modulo 3.*

4. *g is an elation, $p=2$, the centre of g is not in $\mathcal{H}$ and either*

   (a) *axis is a secant line of $\mathcal{H}$, or;*

   (b) *axis is external to $\mathcal{H}$ and $q=2$.*

5. *g fixes exactly one point and p divides $q+1$.*

6. *g has no fixed points, $p=3$ and q is congruent to 1 modulo 3.*

5 Hyperovals in $PG(2,q)$

We now investigate hyperovals in $PG(2,q)$.

The group $PGL(3,q)$ acts regularly on the ordered quadrangles (i.e. 4-arcs) of $PG(2,q)$ and therefore any hyperoval is equivalent to a hyperoval containing the **fundamental quadrangle** $\{(0,0,1),(0,1,0),(1,0,0),(1,1,1)\}$. The following result shows that such hyperovals can be described by a permutation polynomial.

Theorem 16 ([22]). *A hyperoval in $PG(2,q)$ (where $q>2$ is even) containing the fundamental quadrangle can be written as*

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

where f is a permutation polynomial of degree at most $q-2$ satisfying $f(0)=0$ and $f(1)=1$.

The permutation polynomials which describe hyperovals are called **o-polynomials**. When an o-polynomial $f(t)=x^n$ then we describe the hyperoval $\mathcal{D}(f)$ as $\mathcal{D}(n)$.

Table 1 shows the list of all known infinite families of hyperovals. There are other family of sporadic hyperovals: the O'Keefe-Penttila hyperoval in $PG(2,32)$ [10] and the hyperovals in $PG(2,64)$, $PG(2,256)$, $PG(2,1024)$, $PG(2,4096)$ and $PG(2,16384)$ associated with cyclic q-clans [15].

6 Cherowitzo Hyperovals

Let $f_C(x) = x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$. Then we have the Cherowitzo hyperovals ([3] and [2]) equivalent to $\mathcal{D}(f_C)$, where $q = 2^e$ with e odd and σ is an automorphism of $GF(q)$ with $\sigma^2 \equiv 2 \pmod{q-1}$. The order of the stabiliser in $P\Gamma L(3,q)$, $q = 2^e$, for $e = 5$ is e [12] and for $e \geq 7$ is divisible by e [3]. It should be added that only recently has $\mathcal{D}(f_C)$ been proved to be a hyperoval for all e odd [2].

We will prove that the Cherowitzo hyperovals are new; the below Theorem will be central to that proof.

Theorem 17 ([13]). *Let $q = 2^e$ where $e \geq 7$ is odd. Let $\mathcal{H}$ be a Cherowitzo hyperoval. A collineation which fixes $\mathcal{H}$ and which fixes either $(0,1,0)$ or $(0,0,1)$ must be an automorphic collineation.*

Lemma 18 ([12]). *For $q = 32$ the Cherowitzo hyperoval is not equivalent to the listed hyperovals.*

Theorem 19. *The Cherowitzo hyperovals in $PG(2,q)$, $q = 2^e$, e odd, are new for $e > 3$.*

Proof. We show the Cherowitzo hyperovals, $\mathcal{C} = \mathcal{D}(f_C)$, are new by first showing that for any known non-Cherowitzo hyperoval, $\mathcal{H}$, in $PG(2,2^e)$, e odd, if $\mathcal{C} \cong \mathcal{H}$ then the equivalence is a homography stabilising the fundamental quadrangle (FQ), and then using Theorem 17.

By [9] the only o-polynomials over $GF(2)$, $q > 8$ representing regular hyperovals are x^2, $x^{1/2}$ and $x^2 + x^4 + \cdots + x^{q-2}$. Hence $\mathcal{C}$ is not equivalent to a regular hyperoval, for $q > 8$.

Let $\mathcal{H}$ be an irregular translation hyperoval. Then the stabiliser, H, of $\mathcal{H}$ in $P\Gamma L(3,q)$ is isomorphic to $A\Gamma L(1,q)$. Since the group has orbits on $\mathcal{H}$ of lengths 1, 1 and q, and is 2-transitive on the orbit of length q, it follows that all quadrangles on $\mathcal{H}$ containing the two fixed points are equivalent under the stabiliser of $\mathcal{H}$.

Now suppose that f is an o-polynomial over $GF(2)$ representing a hyperoval $\mathcal{D}(f)$ equivalent to $\mathcal{H}$. Then the stabiliser, H', of $\mathcal{D}(f)$ is conjugate in $P\Gamma L(3,q)$ to H. Since H' contains the automorphic collineations, which fix only the points of the fundamental quadrangle, H must contain a group A conjugate to the automorphic collineations fixing a quadrangle on $\mathcal{H}$, and no further points. Thus A fixes a quadrangle on the fixed points of $\mathcal{H}$. Without loss of generality, $\mathcal{H} = \mathcal{D}(\alpha)$, for some generator $\alpha \in \operatorname{Aut} GF(q)$. By the transitivity on quadrangles containing the fixed points noted above, without loss of generality, A fixes the FQ. Thus the equivalence between $\mathcal{D}(f)$ and $\mathcal{D}(\alpha)$ stabilises the FQ and, without loss of generality, is a homography. If $\mathcal{C} \cong \mathcal{H}$ then $\mathcal{C}$ is stabilised by an involution fixing the FQ and two points of the FQ. Hence by Theorem 17 we have the homography being the map $(x,y,z) \mapsto (x,z,y)$, that is, we have $f_C = f_C^{-1}$. By lemma 18 in [2] we have that if $f(x) = x + x^{\sigma-1} + x^{\sigma+1}$ then

$$f^{-1}(x) = \frac{x^{\sigma+1}}{1 + x^2 + x^{\sigma}}.$$

Now $g(x) = x^{\sigma+2}$ then we have $f_{\mathcal{C}} = f \circ g$. Hence $f_{\mathcal{C}}^{-1} = g^{-1} \circ f^{-1}$ so

$$\begin{aligned} f_{\mathcal{C}}^{-1}(x) &= \left(\frac{x^{\sigma+1}}{1+x^2+x^\sigma}\right)^{\frac{1}{\sigma+2}} \\ &= \left(\frac{x^{\sigma+1}}{1+x^2+x^\sigma}\right)\left(\frac{1+x^2+x^\sigma}{x^{\sigma+1}}\right)^{\frac{1}{\sigma}} \\ &= \frac{x^{\sigma+1}(1+x^\sigma+x)}{(1+x^2+x^\sigma)(x^{1+\frac{1}{\sigma}})} \\ &= \frac{x^{\sigma-\frac{1}{\sigma}}(1+x+x^\sigma)}{1+x^2+x^\sigma}. \end{aligned}$$

Hence

$$f_{\mathcal{C}}^{-1}(x) = \frac{x^{1/\sigma}(1+x+x^\sigma)}{1+x^2+x^\sigma}.$$

So if $f_{\mathcal{C}}(x) = f_{\mathcal{C}}^{-1}(x)$ then

$$x^{1/\sigma} + x^{1+1/\sigma} + x^{\sigma+1/\sigma} = x^\sigma + x^{2\sigma} + x^{\sigma+4} + x^{2\sigma+2} + x^{3\sigma+4} + x^{3\sigma+6} + x^{4\sigma+4}.$$

Hence the right hand side must collapse to three terms. That is, we require two more cancellations. It is easy to verify that the required cancellations only occur when $q \leq 8$.

Now suppose $\mathcal{H}$ is a Payne hyperoval. Then by [23] [12] the stabiliser of the Payne hyperoval in $PG(2,q)$, $q = 2^e$, e odd is cyclic of order $2e$. The group has an involution fixing the FQ and moving two points. If $\mathcal{C} \cong \mathcal{H}$ then by [13] the involution is $(x,y,z) \mapsto (x,z,y)$ so we have $f_{\mathcal{C}} = f_{\mathcal{C}}^{-1}$. From above we see that this only occurs when $q \leq 8$.

Let $\mathcal{H}$ be the Subiaco hyperoval. We are only interested in the case when $q = 2^e$, e odd. We argue as for the Payne hyperoval.

Let $\mathcal{H}$ be a known monomial, non-translation hyperoval. In [11] the group H of any known monomial non-translation hyperoval $\mathcal{H}$ in $PG(2,q)$ is shown to be isomorphic to $\Gamma L(1,q)$ for $q > 128$. Since this group has orbits on $\mathcal{H}$ of lengths 1, 1, 1, $q-1$, and is transitive on the orbit of length $q-1$, it follows that all quadrangles on $\mathcal{H}$ containing the three fixed points are equivalent under the stabiliser of $\mathcal{H}$.

Now suppose that f is an o-polynomial over $GF(2)$ representing a hyperoval $\mathcal{D}(f)$ equivalent to $\mathcal{H}$. Then the stabiliser H' of $\mathcal{D}(f)$ is conjugate in $P\Gamma L(3,q)$ to H. Since H' contains the automorphic collineations, which fix only the points of the FQ, H must contain a group A conjugate to the automorphic collineations fixing a quadrangle on $\mathcal{H}$, and no further points. Thus A fixes a quadrangle on the fixed points of $\mathcal{H}$. Without loss of generality, let $\mathcal{H} = \mathcal{D}(n)$ where n is 6, $\sigma + \lambda$ or $2\sigma + 4$ where σ and λ are defined as for the Glynn hyperoval. By transitivity on quadrangles containing the fixed points, as noted above, then without loss of generality, A fixes the fundamental quadrangle. Thus the equivalence between $\mathcal{D}(f)$ and $\mathcal{D}(n)$ stabilises the FQ, and without loss of generality, is a homography. So if $\mathcal{C} \cong \mathcal{H}$ then there is a homography taking the FQ to the FQ. But $\mathcal{D}(n)$ has homography group C_{q-1} fixing three points of the FQ. Thus there exists a nontrivial homography of $\mathcal{C}$ fixing three points of the FQ. Hence at least one of $(0,1,0)$ and $(0,0,1)$ is fixed contrary to Theorem 17.

For $q = 32$ and $q = 128$ the stabiliser, H, of some non-translation monomial hyperoval has order $3(q-1)$ [11]. This hyperoval, $\mathcal{H}$, is equivalent to $\mathcal{D}(6)$ for $q = 32$ and equivalent to $\mathcal{D}(20)$ for $q = 128$. Now suppose that f is an o-polynomial over $GF(2)$ representing a hyperoval $\mathcal{D}(f)$ equivalent to $\mathcal{H}$ for $q = 32$ or 128. As in the previous paragraph, H must contain a group A conjugate to the automorphic collineations fixing a quadrangle on $\mathcal{H}$, and no further points. Thus A fixes a quadrangle on the fixed point of $\mathcal{H}$. We have $|A|$ being 5 or 7 for $q = 32$ or $q = 128$, respectively, so the set of four fixed points of H must be those fixed by A. Now 31 and 127 are prime, and 3 is coprime to 5 and 7, so any subgroup conjugate to A is a Sylow 5-subgroup or Sylow 7-subgroup for $q = 32$ or $q = 128$, respectively. For $h \in H$ the fixed points of hAh^{-1} is equal to h(fixed points of A) which is equal to

$$h(\text{orbit of length 3}) \cup \{P\} = (\text{orbit of length 3}) \cup \{P'\}$$

for points P, P' on $\mathcal{H}$. We have $A \leq H' = P\Gamma L(3,q)_{\mathcal{D}(f)}$. For $g \in P\Gamma L(3,q)$ we have $gAg^{-1} \leq H$. Since for $A \in \mathrm{Syl}_e(H)$ then $gAg^{-1} \in \mathrm{Syl}_e(H)$ for $e = 5$, 7. This implies that $gAg^{-1} = hAh^{-1}$ for some $h \in H$. So if $\mathcal{C} \cong \mathcal{H}$ we have that there exists a nontrivial homography of $\mathcal{C}$ fixing 3 points of the FQ. Hence at least one of $(0,1,0)$ and $(0,0,1)$ is fixed, contrary to Theorem 17. □

Name	f	$q = \square$	$q \neq \square$	$\lvert P\Gamma L(3,q)_{\mathcal{D}(f)}\rvert$ where $q = 2^e$	Other conditions
Regular	x^2	$\star$	$\star$	$\lvert S_4\rvert$, $q = 2$ $\lvert S_6\rvert$, $q = 4$ $\lvert P\Gamma L(2,q)\rvert$, $q \geq 8$	
Translation	x^{2^i}	$\star$	$\star$	$\lvert AGL(1,q)\rvert$, $q \geq 8$	$(e,i) = 1$, $i < e/2$
Segre	x^6		$\star$	$3(q-1)e$, $e = 5$ $(q-1)e$, $e \geq 7$	
Glynn I	$x^{3\sigma+4}$		$\star$	$(q-1)e$	$\sigma = 2^{(e+1)/2}$
Glynn II	$x^{\sigma+\lambda}$		$\star$	$3(q-1)e$, $e = 7$ $(q-1)e$, $e > 7$	$\sigma = 2^{(h+1)/2}$, $\lambda = 2^m$ if $e = 4m-1$ or $\lambda = 2^{3m+1}$ if $e = 4m+1$
Payne	$x^{1/6} + x^{3/6} + x^{5/6}$		$\star$	$2e$	
Cherowitzo	$x^\sigma + x^{\sigma+2} + x^{3\sigma+4}$		$\star$	e, $e = 5$ divisible by e, $e \geq 7$	$\sigma = 2^{(e+1)/2}$
Subiaco	$x^{1/2} + \frac{d^2(x^4+x)+d^2(1+d+d^2)(x^3+x^2)}{x^4+d^2x^2+1}$	$\star$	$\star$	$2e$, $q+1 \not\equiv 0 \pmod 5$ $10e$ and $5e/2$, $e \equiv 2 \pmod 4$	$\mathrm{trace}(1/d) = 1$ $q = 16$ gives Lunelli-Sce oval

Table 1: Known infinite families of hyperovals for $q = 2^e$, $q \geq 8$. $\star$ indicates the hyperoval exists in these fields.

References

[1] M. Biliotti and G. Korchmáros, *Hyperovals with a transitive collineation group*, Geom. Ded. **24** (1987), 269–281.

[2] W. Cherowitzo, *Alpha flocks and hyperovals*, (submitted).

[3] ———, *Hyperovals in Desarguesian planes of even order*, Annals Disc. Math. **37** (1988), 87–94.

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

[5] P. Dembowski, *Finite geometries*, Springer, 1968.

[6] M. Hall, Jr., *The theory of groups*, Macmillan Company, 1959.

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

[8] D. R. Hughes, *Generalized incidence matrices over group algebras*, Illinois Journal of Mathematics **1** (1957), 545–551.

[9] C. M. O'Keefe and T. Penttila, *Polynomials for hyperovals of Desarguesian planes*, J. Aust. Math. Soc. (A) **51** (1991), 436–447.

[10] ———, *A new hyperoval in* $PG(2,32)$, J. Geometry **44** (1992), 117–139.

[11] ———, *Symmetries of arcs*, J. Combin. Theory (A) **66** (1994), 53–67.

[12] C. M. O'Keefe, T. Penttila, and C. E. Praeger, *Stabilisers of hyperovals in* $PG(2,32)$, Advances in finite geometries and designs (J. W. P. Hirschfeld, D. R. Hughes, and J. A. Thas, eds.), Oxford University Press, 1991, pp. 337–351.

[13] C. M. O'Keefe and J. A. Thas, *Collineations of Subiaco and Cherowitzo hyperovals*, Bull. Belg. Math. Soc. Simon Stevin **3** (1996), no. 2, 177–192.

[14] T. G. Ostrom, *Semi-translation planes*, Trans. Amer. Math. Soc. **111** (1964), 1–48.

[15] S. E. Payne, T. Penttila, and G. F. Royle, *Building a cyclic q–clans*, (preprint).

[16] T. Penttila, *The Plane Equivalence Theorem*, (in preparation).

[17] T. Penttila and G. F. Royle, *Hyperovals in* $PG(2,q)$ *for small* q, J. Geometry **54** (1995), 90–104.

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

[19] I. Pinneri, *Flocks, generalised quadrangles and hyperovals*, Ph.D. thesis, University of Western Australia, 1996.

[20] F. C. Piper, *Collineation groups containing elations*, Math. Z. **92** (1966), 281–287.

[21] B. Segre, *Ovals in a finite projective plane*, Canad. J. Math. **7** (1955), 414–416.

[22] ______, *Sui k-archi nei piani finiti di caratteristica due*, Rev. Math. Pures Appl. **2** (1957), 289–300.

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

(Received 11/2/98)