Groups of hyperovals in Desarguesian planes

Luke Bayens William Cherowitzo Tim Penttila

Dedicated to our friend and colleague, Gabor Korchmáros, on the occasion of the 60th birthday, from whom we have learnt so much about hyperovals.

Abstract

We show that if a hyperoval $\mathcal{H}$ of $\mathsf{PG}(2,q)$, $q > 4$, admits an insoluble group G, then G fixes a subplane π_0 of order $q_0 > 2$, $\mathcal{H}$ meets π_0 in a regular hyperoval of π_0 on which $G \cap \mathsf{PGL}(3,q)$ induces $\mathsf{PGL}(2,q_0)$, and if $\mathcal{H}$ is not regular then $q > q_0^2$. We also bound above the order of the homography stabilizer of a non-translation hyperoval of $\mathsf{PG}(2,q)$ by $3(q-1)$. Finally, we show that the homography stabilizer of the Cherowitzo hyperovals is trivial for $q > 8$.

Keywords: hyperoval, group

MSC 2000: 51E20, 51E21

1. Introduction

Studying symmetries of configurations in finite Desarguesian projective planes need not involve the use of deep group theory, since the subgroup structure of the collineation groups of these planes has been known since the work of Howard H. Mitchell in 1911 for odd characteristic, and of his student R. W. Hartley in 1925 for characteristic two. Despite this advantage, we still know very little about even the symmetries of highly studied objects like hyperovals. We do not even know whether or not the regular hyperovals are characterized (for planes of order greater than 2) by the property of admitting an insoluble group. Indeed, the results of Section 3 of this paper can be viewed as a failed attempt at such a characterization. The rich man/poor man result in Section 4 can be considered a post facto explanation of the fact that all hyperovals of finite

Desarguesian projective planes discovered since 1957 have such small groups. The last section deals with the original motivating purpose for this paper — the calculation of the groups of the last family of known hyperovals for which the problem is still open — those of Cherowitzo (1998). In [4], an infinite family of hyperovals in $\mathsf{PG}(2,q)$, $q=2^h$, $h=2e+1$, was constructed, generally known as the *Cherowitzo hyperovals*,

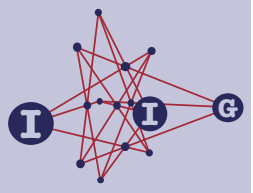
$$\{(1,t,t^\sigma+t^{\sigma+2}+t^{3\sigma+4}) \mid t\in \mathsf{GF}(q)\}\cup\{(0,1,0),(0,0,1)\}$$

where $\sigma=2^{e+1}$.

The groups of the Adelaide hyperovals of Cherowitzo-O'Keefe-Penttila (2003) [5] were calculated by Payne-Thas (2005) in [19], the groups of the Subiaco hyperovals of Cherowitzo-Penttila-Pinneri-Royle (1996) [6] were calculated by combined results of O'Keefe-Thas (1996) in [16] and Payne-Penttila-Pinneri (1995) in [18], and the groups of the hyperovals of Payne (1985) [17] were calculated by Thas-Payne-Gevaert (1988) in [23], with all three using the beautiful method of associating a curve of fixed degree with the hyperoval and using Bezout's theorem. (For earlier hyperovals, see, for example [14]). But the attempt of O'Keefe-Thas (1996) to apply this method to the Cherowitzo hyperovals only gave partial results, leading to the technical difficulties and subtlety of the proof of Penttila-Pinneri (1999) [20] that the Cherowitzo hyperovals are new for fields of order greater than 8. Subtlety is only necessary when faced with paucity of knowledge, and their results are an immediate corollary of our determination of the groups of the Cherowitzo hyperovals in the final section of this paper. But our methods are far from beautiful. We apply the magic action of O'Keefe-Penttila (2002) [15], to perform fiendishly difficult computations in order to show that the homography groups of the Cherowitzo hyperovals are trivial. We resort to the use of the computer algebra packages Mathematica and Magma at crucial stages in the computations. The preceding sections form yet another failed attempt to perform this computation purely theoretically.

It seems that we still understand these hyperovals poorly. It is of note that it took 14 years to prove the generalization of the first examples found to an infinite family, and that the proof is lengthy and involved. Perhaps a beautiful proof exists and merely eludes us, owing to our poor understanding of these mysterious objects.

To be more exact about the general results about stabilizers of hyperovals that we obtain, combining Theorem 3.6 and the Remark that follows it shows that if a hyperoval $\mathcal{H}$ of $\mathsf{PG}(2,q)$, $q>4$ admits an insoluble group G, then there is a subplane π_0 of order $q_0>2$ meeting $\mathcal{H}$ in a regular hyperoval such that $G\cap\mathsf{PGL}(3,q)$ induces $\mathsf{PGL}(2,q_0)$ on π_0, and if $\mathcal{H}$ is irregular, then $q>q_0^2$. We also (sharply) bound above the order of the homography stabilizer of a non-translation hyperoval of $\mathsf{PG}(2,q)$ by $3(q-1)$ in Theorem 3.8.



2. Background results

The mainstay of our approach to groups of hyperovals of Desarguesian planes are the following two fundamental results of Hartley (1925) on groups of homographies of Desarguesian planes.

Theorem 2.1 ([10]). *A proper subgroup of* $\mathsf{PSL}(3,q)$, q *even, fixes a point, a line, a triangle, a subplane or a classical unital, or is contained in the normalizer of a Singer cycle, or* $q=4$ *and the subgroup fixes a hyperoval.*

Theorem 2.2 ([10]). *A proper subgroup of* $\mathsf{PSU}(3,q)$, q *even and a square, fixes a point, a line, a triangle or a subplane, or is contained in the normalizer of a Singer cycle, or* $q=4$ *and the order of the subgroup is 36.*

A group of collineations of a projective plane is *irreducible* if it fixes no point, line or triangle. It is *strongly irreducible* if it is irreducible and fixes no proper subplane.

Corollary 2.3. *A strongly irreducible proper subgroup* G *of* $\mathsf{PSL}(3,q)$, q *even,* $q>4$, *is contained in the normalizer of a Singer cycle, or* q *is a square and* $G=\mathsf{PSU}(3,q)$.

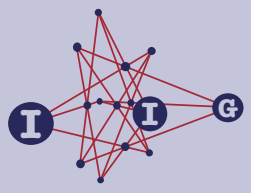
We also need information about the subgroups of $\mathsf{PGL}(2,q)$, q even, for which a convenient reference is [7], although the result is due, independently, to Wiman and Moore.

Theorem 2.4 ([7]). *The only non-abelian composition factors of subgroups of* $\mathsf{PGL}(2,q)$, q *even, are* $\mathsf{PSL}(2,q_0)$, *with* q *a power of* q_0. *The subgroups of* $\mathsf{PGL}(2,q)$, q *even,* $q>8$, *of order greater than* $3(q-1)$ *contain a Sylow 2-subgroup of* $\mathsf{PGL}(2,q)$.

Corollary 2.5. *The only non-abelian composition factors of subgroups of* $\mathsf{P\Gamma L}(3,q)$, q *even, are* $\mathsf{PSL}(3,q_0)$, $\mathsf{PSL}(2,q_0)$, $\mathsf{PSU}(3,q_0)$ *and* A_6, *where* q *is a power of* q_0.

Proof. Let H be an insoluble subgroup of $\mathsf{P\Gamma L}(3,q)$, q even. Then $H\cap\mathsf{PSL}(3,q)$ is insoluble. By Theorems 2.1, 2.2 and 2.4, either $H\cap\mathsf{PSL}(3,q)$ contains $\mathsf{PSL}(3,q_0)$ or $\mathsf{PSU}(3,q_0)$ or A_6, since the stabilizer of a triangle is soluble, and the groups of collineations with centre a point or axis a line are soluble, and the group induced by the stabilizer of a point in $H\cap\mathsf{PSL}(3,q)$ on the lines through that point is a subgroup of $\mathsf{PGL}(2,q)$. □

We now survey elementary results on groups of hyperovals that also apply in the non-Desarguesian case. Deeper results, using theorems about simple groups, can be found in the papers of Korchmáros.



Involutions play an important role. Their action on projective planes is determined by the following result of Baer (1946).

Theorem 2.6 ([1]). *An involutory collineation of a projective plane of order q, q even, is either an elation or a Baer involution, in which case q is a square.*

More can be said when the involution is an elation and fixes a hyperoval.

Theorem 2.7 ([2]). *A non-trivial central collineation of a projective plane of order q, q even, fixing a hyperoval is necessarily an involutory elation with centre not on the hyperoval.*

Proof. Since the orbits of a point, not the centre, not on the axis are collinear, and have length the order of the collineation, any point on the hyperoval, not on the axis, not the centre, has an orbit of length 2, and so the collineation is involutory. By Theorem 2.6, it is an elation. Since there is a point on the hyperoval not on the axis, the orbit of that point, together with the centre, forms a collinear triple; so the centre is not on the hyperoval. □

The following result of Hughes (1957) controls involutions for planes of order 2 modulo 4.

Theorem 2.8 ([12]). *A projective plane of order $q > 2$, $q \equiv 2 \pmod 4$, has no involutory collineations.*

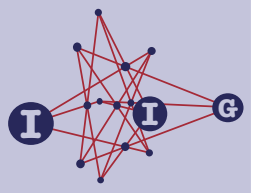
Further control of elations fixing hyperovals follows from the next result of Penttila-Royle (1995).

Theorem 2.9 ([21]). *A non-trivial central collineation of a finite projective plane of even order $q > 2$ fixing a hyperoval $\mathcal{H}$, is necessarily an elation with axis secant to $\mathcal{H}$ and centre not on $\mathcal{H}$.*

Proof. By Theorem 2.7, we need only show that the axis is a secant line for $q > 2$. By [12], $q \equiv 0 \pmod 4$. So the number of points on the hyperoval $\equiv 2 \pmod 4$. Thus the number of secant lines on any point P on the axis, not the centre, and not on the hyperoval, is odd. Hence a secant line is fixed. But the only fixed line on P is the axis, so it follows that the axis is a secant line. □

The following elementary observation of Biliotti-Korchmáros (1987) about two elations fixing a hyperoval is fundamental.

Theorem 2.10 ([2]). *Two non-trivial central collineations of a finite projective plane of even order $q > 4$ fixing a hyperoval have different centres.*



More detailed information is given in the next result of Biliotti-Korchmáros (1987), an alternative proof of which appears in Penttila-Pinneri (1999).

Theorem 2.11 ([2, 20]). *Let $\mathcal{H}$ be a hyperoval in a projective plane π of order q, and suppose that two distinct non-trivial elations of π stabilize $\mathcal{H}$. Then one of the following holds:*

(i) *the elations have different centres but the same axis, which is secant to $\mathcal{H}$, and the product of the elations is an involutory elation with the same axis but a different centre;*

(ii) *the axes are distinct and meet at a point of $\mathcal{H}$, 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) *an external line, and the product of the elations has order dividing $q+1$;*

(iii) *the axes are distinct secant lines which meet at a point not on $\mathcal{H}$, the centres are distinct and the line joining the centres is external to $\mathcal{H}$, the product of the elations has order 3, and $q \equiv 1 \pmod 3$;*

(iv) $q = 2$ *or* 4.

Corollary 2.12. *No hyperoval of a projective plane of order q, with $q \not\equiv 1 \pmod 3$, is stabilized by 3 non-trivial elations with axes forming a triangle.*

A bound on the order of the homography stabilizer of a hyperoval of a Desarguesian plane is given by O'Keefe-Penttila (1991).

Theorem 2.13 ([13]). *The stabilizer in $\mathrm{P\Gamma L}(3,q)$ of a hyperoval in $\mathrm{PG}(2,q)$, $q > 2$, has order dividing $(q+2,3)(q+1)q(q-1)$.*

This result allows greater control of one of Hartley's cases, when a hyperoval is fixed.

Corollary 2.14. *A subgroup of the normalizer in $\mathrm{PGL}(3,q)$, q even, of a Singer cycle stabilizing a hyperoval is a 3-group, and fixes a point or a triangle.*

Proof. The greatest common divisor of $(q+2,3)(q+1)q(q-1)$ and $3(q^2+q+1)$ divides 9. □

3. General results

Lemma 3.1. *A strongly irreducible proper subgroup of $\mathrm{PSL}(3,4)$ that does not fix a classical unital is the stabilizer A_6 in $\mathrm{PSL}(3,4)$ of a hyperoval of $\mathrm{PG}(2,4)$.*

Proof. By Theorem 2.1, the only case to eliminate is that of a subgroup of the normalizer of a Singer cycle. But when $q = 4$, the intersection of the normalizer in $\mathrm{PGL}(3, q)$ of a Singer cycle with $\mathrm{PSL}(3, q)$ fixes a subplane. □

The following Lemma is reminiscent of results in [3]. The reader may find it helpful to compare and contrast the approaches.

Lemma 3.2. *If the stabilizer G in $\mathrm{PGL}(3, q)$ of a hyperoval in $\mathrm{PG}(2, q)$, $q > 4$, is irreducible, then $G \cap \mathrm{PSL}(3, q)$ is irreducible.*

Proof. Suppose $G \cap \mathrm{PSL}(3, q)$ is not irreducible. If $G \neq G \cap \mathrm{PSL}(3, q)$, then $|G : G \cap \mathrm{PSL}(3, q)| = 3$. Suppose $G \cap \mathrm{PSL}(3, q)$ fixes a point P. Then $G_P \geq G \cap \mathrm{PSL}(3, q)$, and so the orbit of P under G has length 1 or 3, a contradiction. Hence $G \cap \mathrm{PSL}(3, q)$ does not fix a point, and dually, $G \cap \mathrm{PSL}(3, q)$ does not fix a line. So $G \cap \mathrm{PSL}(3, q)$ fixes a triangle Δ, and $G_\Delta = G \cap \mathrm{PSL}(3, q)$. We show that $G_{(\Delta)}$ is a 3-group. Suppose not. Let p be a prime dividing $|G_{(\Delta)}| \Big| |\mathrm{PGL}(3, q)_{(\Delta)}| = (q-1)^2$. Then $p \neq 2$, since elations do not pointwise fix a triangle. So $p > 3$. Let $1 \neq P \in \mathrm{Syl}_p G_{(\Delta)}$. Since P is not generated by a homology, $|P| \Big| q-1$. Hence $\mathrm{Fix}(P) = \Delta$. However, $\mathrm{PGL}(3, q)_{(\Delta)} = C_{q-1} \times C_{q-1}$ is abelian, so P is its unique Sylow p-subgroup. Therefore P char $G_{(\Delta)} \lhd G \cap \mathrm{PSL}(3, q) \lhd G$. Hence $P \lhd G$, and so G fixes Δ, a contradiction.

Without loss of generality, $\Delta = \{(1,0,0), (0,1,0), (0,0,1)\}$. For all $a \in \mathrm{GF}(q)^*$ such that there exists $b \in \mathrm{GF}(q)^*$ with $\left(\begin{smallmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in G_{(\Delta)}$, b is unique (otherwise $G_{(\Delta)}$ would contain a homology). So

$$G_{(\Delta)} = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & f(a) & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid a \in S \right\}$$

where $S \leq \mathrm{GF}(q)^*$ and $f : S \to \mathrm{GF}(q)^*$ is a homomorphism. Since S is the unique cyclic group of $\mathrm{GF}(q)^*$ of order $|S|$, and $f(S) \leq S$, it follows that $f(x) = x^n$ for some n. Hence

$$G_{(\Delta)} = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & a^n & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid a \in S \right\}.$$

But

$$\begin{pmatrix} a^n & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{pmatrix} = \begin{pmatrix} a^{n-1} & 0 & 0 \\ 0 & a^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \in G_{(\Delta)},$$

and so $a^{n(n-1)} = a^{-1}$, forcing $n^2 - n + 1 \equiv 0 \pmod{|S|}$. Since there are no solutions to this congruence modulo 9, it follows that $|S| = 3$. But now $|G| = 9$ or 18, and up to conjugacy $G \leq \mathsf{PGU}(3,4)$, and G fixes a triangle, a contradiction. □

Theorem 3.3. *The stabilizer G in $\mathsf{PGL}(3,q)$ of a hyperoval in $\mathsf{PG}(2,q)$ fixes a point, line, triangle, or a subplane π_0 of order 4. If G is irreducible, then either $q = 4$ and $G \cong \mathsf{A}_6$, or $q > 4$ and the group induced by G on π_0 is a subgroup of $\mathsf{PGU}(3,4)$.*

Proof. Suppose $q > 4$ and G is irreducible. Then $G \cap \mathsf{PSL}(3,q)$ is irreducible by Lemma 3.2. Since $\mathsf{PSU}(3,q_0)$ contains a group of order q_0 of elations with the same centre, $G \cap \mathsf{PSL}(3,q)$ cannot induce $\mathsf{PSU}(3,q_0)$ on any subplane of order $q_0 > 2$ by Theorem 2.10, and is not contained in the normalizer of a Singer cycle by Corollary 2.14. Hence, $G \cap \mathsf{PSL}(3,q)$ is a proper subgroup of $\mathsf{PSL}(3,q)$, and fixes a subplane by Corollary 2.3.

Let π_0 be a minimal non-trivial subplane of order q_0 fixed by $G \cap \mathsf{PSL}(3,q)$ and let L be the group induced by $G \cap \mathsf{PSL}(3,q)$ on π_0. Then L is strongly irreducible, and by Corollary 2.3 applied to $L \cap \mathsf{PSL}(3,q_0)$, it follows that π_0 has order 4. (Note that a group inducing a subgroup of the normalizer of a Singer cycle of π_0 either fixes a triangle of $\mathsf{PG}(2,q)$, or is a subgroup of the normalizer of a Singer cycle of $\mathsf{PG}(2,q)$, which eliminates this case.) If $L \cap \mathsf{PSL}(3,q)$ is not a subgroup of $\mathsf{PSU}(3,4)$, then $L \cap \mathsf{PSU}(3,4)$ fixes a hyperoval of $\mathsf{PG}(2,4)$ by Lemma 3.1 and Theorem 2.1. Thus $L \cap \mathsf{PSL}(3,4) = \mathsf{A}_6$ or $\mathsf{PSL}(2,5)$, however both of these contain distinct elations with the same centre, contradicting Theorem 2.10. Since G normalizes $G \cap \mathsf{PSL}(3,q)$, it follows that in this case $G = G \cap \mathsf{PSL}(3,q)$ and has order 36 by Theorem 2.2. □

Which insoluble groups can act on hyperovals of Desarguesian planes? The following example is instructive.

Example 3.4. $\mathsf{PGL}(2,q_0) \leq \mathsf{PGL}(3,q)_{\mathcal{H}}$, where

$$\mathcal{H} = \{(1,t,t^2) \mid t \in \mathsf{GF}(q)\} \cup \{(0,1,0),(0,0,1)\}$$

is a regular hyperoval and $q = q_0^h$. Moreover, it is the stabilizer of the subplane

$$\pi_0 = \{(x,y,z) \mid x,y,z \in \mathsf{GF}(q_0)\}$$

in $\mathsf{PGL}(3,q)_{\mathcal{H}}$, and $\pi_0 \cap \mathcal{H}$ is a regular hyperoval of π_0, consisting of a conic $\mathcal{C}_0$ and its nucleus N. The points of π_0 are of three kinds: N, the points of $\mathcal{C}_0$, and the centres of elations of $\mathsf{PGL}(2,q_0)$. The lines of π_0 are of three kinds: the tangent lines to $\mathcal{C}_0$, the secant lines to $\mathcal{C}_0$ and the external lines to $\mathcal{C}_0$.

In the theorem that follows we need to deduce the existence of an invariant subplane from knowledge of a group fixing a hyperoval. The preceding example allows us to construct this subplane from the group *without needing its action on the plane*.

Example 3.5. The incidence structure $\mathcal{I}(G)$ with points

(i) ∞

(ii) Sylow 2-subgroups T of G

(iii) involutions t of G

and lines

(a) Sylow 2-subgroups $[T]$ of G

(b) dihedral subgroups U of order $2(q_0 - 1)$ of G

(c) dihedral subgroups V of order $2(q_0 + 1)$ of G

with incidence

$$\begin{array}{lll} \infty \,\mathrm{I}\, [T], & T \,\mathrm{I}\, [T], & t \,\mathrm{I}\, [T] \iff t \in T \\ \infty \not\mathrm{I}\, U, & T \,\mathrm{I}\, U \iff \langle T, U\rangle \cong \mathsf{AGL}(1, q_0), & t \,\mathrm{I}\, U \iff t \in U \\ \infty \not\mathrm{I}\, V, & T \not\mathrm{I}\, V, & t \,\mathrm{I}\, V \iff t \in V \end{array}$$

is isomorphic to $\mathsf{PG}(2, q_0)$, since the correspondence

$$\begin{array}{rcl} \infty & \longleftrightarrow & N \\ T & \longleftrightarrow & \mathrm{Fix}(T) \cap (\pi_0 \cap \mathcal{H}) \\ t & \longleftrightarrow & \text{centre of } t \\ [T] & \longleftrightarrow & \text{tangent line to } \pi_0 \cap \mathcal{H} \text{ at } \mathrm{Fix}(T) \cap (\pi_0 \cap \mathcal{H}) \\ U & \longleftrightarrow & \text{unique fixed line of } U \\ V & \longleftrightarrow & \text{unique fixed line of } V \end{array}$$

is an isomorphism with π_0.

Theorem 3.6. *If the stabilizer G in $\mathsf{P\Gamma L}(3, q)$ of a hyperoval $\mathcal{H}$ is insoluble, then either $q = 4$ and $G \cong \mathsf{S}_6$, or G fixes a subplane π_0 of order $q_0 > 2$. In the latter case, $\pi_0 \cap \mathcal{H}$ is a regular hyperoval of π_0 and G has a normal subgroup isomorphic to $\mathsf{PGL}(2, q_0)$.*

Proof. Suppose $q > 4$. By Theorem 3.3, G is reducible, since both $\mathsf{P\Gamma U}(3, 4)$ and the pointwise stabilizer of a subplane are soluble. Since the stabilizer of a triangle is also soluble, G fixes a point or line. $G \cap \mathsf{PSL}(3, q)$ is insoluble, and

so by [9][1] and Theorem 2.6, $G \cap \mathrm{PSL}(3,q)$ contains an elation. Suppose G fixes no point. Then G fixes a line ℓ. If ℓ is not the axis of any non-trivial elation in G, then G acts faithfully on ℓ, and hence G is isomorphic to a subgroup of $\mathrm{P\Gamma L}(2,q)$. Since G is insoluble, G has a normal subgroup N isomorphic to $\mathrm{PGL}(2,q_0)$, for $q_0 > 2$, $q = q_0^h$, by Theorem 2.4. Since N contains at least two non-trivial elations that commute, by Theorem 2.11 ℓ is the common axis, a contradiction. Thus ℓ is the axis of some non-identity elation in G, hence secant to $\mathcal{H}$ by Theorem 2.9. This implies that the stabilizer of $\ell \cap \mathcal{H}$ is soluble, contradicting the insolubility of G.

Therefore G fixes a point P which is on the axis of every elation of $G \cap \mathrm{PSL}(3,q)$. By Theorem 2.10, if P is not on $\mathcal{H}$, then P is not the centre of a non-trivial elation fixing $\mathcal{H}$. If P is on $\mathcal{H}$, then P is not the centre of any non-trivial elation by Theorem 2.7. Hence G acts faithfully on the lines through P, and as above, G is isomorphic to a subgroup of $\mathrm{P\Gamma L}(2,q)$, and has a normal subgroup N isomorphic to $\mathrm{PGL}(2,q_0)$, for $q_0 > 2$, q a power of q_0. If P is not on $\mathcal{H}$, then G acts on the $q/2$ external lines through P, contrary to the action of $\mathrm{PGL}(2,q_0)$ on $\mathrm{PG}(1,q_0)$. Hence P is on $\mathcal{H}$.

Let $\mathcal{C}_0$ be the intersection of $\mathcal{H}$ with the orbit of length q_0+1 of N on the subpencil of lines through P. Then $\mathcal{I}(N) \cong \mathrm{PG}(2,q_0)$, but also $\mathcal{I}(N)$ is isomorphic to the incidence structure with points

(i) P

(ii) the points of $\mathcal{C}_0$

(iii) centres of involutions of N

and lines

(a) PQ, where $Q \in \mathcal{C}_0$

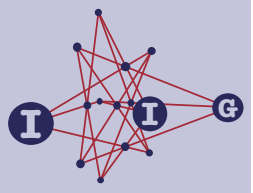
(b) QQ', where $Q, Q' \in \mathcal{C}_0$, $Q \neq Q'$

(c) the unique line fixed by V, where $V \leq N$, $V \cong D_{2(q_0+1)}$

with incidences inherited from $\mathrm{PG}(2,q)$, by applying Theorem 2.11. Hence G fixes the subplane $\pi_0 = \mathcal{I}(N)$, and $\pi_0 \cap \mathcal{H}$ is a hyperoval $\mathcal{H}_0$ of π_0. By [14, Theorem 3.3], $\mathcal{H}_0$ is regular. □

Remark 3.7. If $q = q_0^2$, then the hyperoval is regular, for an orbit of $\mathrm{PGL}(2,q_0)$ on points of the hyperoval not in $\mathrm{PG}(2,q_0)$ has length at most $q_0^2 - q_0$, but elements of order $q_0 - 1$ have all fixed points in $\mathrm{PG}(2,q_0)$. Such an orbit consists of points stabilized by a cyclic $q_0 + 1$, and there are 2 such points (for each cyclic q_0+1) and they must lie on a regular hyperoval. Hence, if the stabilizer is

[1] We only need the fact that all subgroups of $\mathrm{PGL}(3,q)$ of odd order are soluble, which is much easier to prove.



insoluble and the hyperoval is not regular, then the homography stabilizer has order less than $q-1$.

The following result gives a rich man/poor man classification of hyperovals of $\mathsf{PG}(2,q)$.

Theorem 3.8. *A hyperoval of* $\mathsf{PG}(2,q)$ *with homography stabilizer greater than* $3(q-1)$ *is a translation hyperoval.*

Proof. Let G be the homography stabilizer of the hyperoval $\mathcal{H}$, with $|G|$ greater than $3(q-1)$. If G fixes a subplane of order 4, then $|G|=36$ by Theorem 2.2, so $q=4$, a contradiction. If not, G fixes a point, line or triangle by Theorem 3.3. By the above remark and Theorem 3.6, we can assume G is soluble. If G fixes a point or line, G induces a soluble subgroup of $\mathsf{PGL}(2,q)$ on the lines through the point (points on the line). By [14, Theorem 3.6], Theorems 2.13 and 2.4, it follows that G has order divisible by q, in which case $\mathcal{H}$ is translation. Suppose G fixes a triangle Δ. By Theorem 2.7, $G_{(\Delta)}$ contains no homologies. Hence $G_{(\Delta)}$ acts faithfully on any side of Δ, and so $|G|$ divides $6(q-1)$. If $|G|=6(q-1)$, then since $G_{(\Delta)}$ acts semiregularly on points on no side of Δ, it follows that Δ is a subset of $\mathcal{H}$. Since $G_{(\Delta)}$ acts transitively on $\mathcal{H}\setminus\Delta$, it follows from [14, Lemma 3.8], that $\mathcal{H}$ is monomial, contradicting [14, Theorem 4.4]. □

Examples 3.9. The known hyperovals that achieve equality in the above bound are the hyperovals of Segre-Bartocci (1971) [22] in $\mathsf{PG}(2,32)$ and Eich-Payne-Hirschfeld-Glynn (1972) [8] in $\mathsf{PG}(2,128)$ (see [14]).

4. The stabilizer of the Cherowitzo hyperoval

In order to calculate the group of the title of this section, we first need to discuss the representation of hyperovals by o-polynomials (and o-permutations).

By the transitivity of $\mathsf{P\Gamma L}(3,q)$ on ordered quadrangles of $\mathsf{PG}(2,q)$, we can assume that a given oval has nucleus $(0,0,1)$ and contains the points $(1,0,0)$, $(0,1,0)$ and $(1,1,1)$. Such an oval can be written in the form

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

where f is a permutation polynomial of degree less than $q-1$ satisfying $f(0)=0$, $f(1)=1$ and such that for each $s\in\mathsf{GF}(q)$, the function f_s where $f_s(0)=0$, $f_s(x)=(f(x+s)+f(s))/x$ is a permutation (see, for example, [11]). Conversely, any polynomial f satisfying the above conditions gives rise to an oval $\mathcal{D}(f)$ with nucleus $(0,0,1)$. Such a polynomial is called an *o-polynomial*.

If we drop the condition that $f(1) = 1$ (or equivalently, we drop the condition that the oval contain $(1,1,1)$) but retain the other conditions, then f is an o-permutation. Associated with an o-polynomial are $q-1$ o-permutations, namely the non-zero multiples of the o-polynomial. With an o-permutation f, is associated a unique o-polynomial $(1/f(1))f$. If f is an o-polynomial then $\langle f \rangle$ comprises the zero polynomial together with the $q-1$ o-permutations associated with f. Clearly, the $q-1$ ovals $\mathcal{D}(f_i)$, where the f_i are o-permutations associated with an o-polynomial f are equivalent under $\mathsf{PGL}(3,q)$.

We now turn to a method for computing an *oval* stabilizer (and hence hyperoval stabilizer).

Let $\mathcal{F}$ denote the collection of all functions $f\colon \mathsf{GF}(q) \to \mathsf{GF}(q)$ such that $f(0) = 0$. Note that each element of $\mathcal{F}$ can be expressed as a polynomial in one variable of degree at most $q-1$ and that $\mathcal{F}$ is a vector space over $\mathsf{GF}(q)$. If $f(x) = \sum a_i x^i \in \mathcal{F}$ and $\gamma \in \mathrm{Aut}(\mathsf{GF}(q))$ then we write $f^\gamma(x) = \sum a_i^\gamma x^i$ or equivalently, $f^\gamma(x) = (f(x^{1/\gamma}))^\gamma$. As usual, we write x^γ for componentwise action by $\gamma \in \mathrm{Aut}(\mathsf{GF}(q))$ on x in $\mathsf{GF}(q^n)$.

Lemma 4.1 ([15]). *For each $f \in \mathcal{F}$ and $\psi \in \mathsf{P\Gamma L}(2,q)$, where $\psi\colon \mathsf{GF}(q)^2 \to \mathsf{GF}(q)^2$, $x \mapsto Ax^\gamma$ for $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathsf{GL}(2,q)$ and $\gamma \in \mathrm{Aut}(\mathsf{GF}(q))$, let the image of f under ψ be the function $\psi f\colon \mathsf{GF}(q) \to \mathsf{GF}(q)$ such that*

$$\psi f(x) = |A|^{-1/2}\left[(bx+d)f^\gamma\left(\frac{ax+c}{bx+d}\right) + bxf^\gamma\left(\frac{a}{b}\right) + df^\gamma\left(\frac{c}{d}\right)\right].$$

Then this definition yields an action of $\mathsf{P\Gamma L}(2,q)$ on $\mathcal{F}$, which is called the magic action.

We remark that in each term in the formula of the magic action, the denominator of the argument of f^γ is always a factor. Thus, for example, $df^\gamma(c/d)$ is interpreted as 0 if $d = 0$ and so on.

The following result elucidates the relationship between o-permutations that are equivalent under the magic action of $\mathsf{P\Gamma L}(2,q)$ and ovals that are equivalent under the natural action of $\mathsf{P\Gamma L}(3,q)$ on $\mathsf{PG}(2,q)$. We remark that Theorem 4.2 holds for $\mathsf{PGL}(3,q)$ in place of $\mathsf{P\Gamma L}(3,q)$.

Theorem 4.2 ([15]). *Let f and g be o-permutations for $\mathsf{PG}(2,q)$ and suppose that $\mathcal{D}(f)$ and $\mathcal{D}(g)$ are equivalent under $\mathsf{P\Gamma L}(3,q)$. Then there exists $\psi \in \mathsf{P\Gamma L}(2,q)$ such that $\psi f \in \langle g \rangle$. Moreover, there is a one-to-one correspondence between $\{\varphi \in \mathsf{P\Gamma L}(3,q) \mid \varphi\mathcal{D}(f) = \mathcal{D}(g)\}$ and $\{\psi \in \mathsf{P\Gamma L}(2,q) \mid \psi f \in \langle g \rangle\}$.*

We now outline our strategy. From now on let $f(t) = t^\sigma + t^{\sigma+2} + t^{3\sigma+4}$, so that $\mathcal{H} = \mathcal{D}(f) \cup \{(0,0,1)\}$ is the Cherowitzo hyperoval. We determine $\mathsf{PGL}(3,q)_\mathcal{H}$ by finding

$$\{g \in \mathsf{PGL}(3,q)_\mathcal{H} \mid g(0,0,1) = P\}$$

for each $P \in \mathcal{H}$; that is

$$\left\{ g \in \mathsf{PGL}(3,q)_{\mathcal{H}} \mid g\mathcal{D}(f) = \mathcal{H} \setminus \{P\} \right\}.$$

Since $\mathcal{D}(f)$ and $\mathcal{H} \setminus \{P\}$ are *ovals*, we may apply the magic action by finding an o-permutation h such that $\mathcal{D}(f)$ is equivalent to $\mathcal{H} \setminus \{P\}$ under $\mathsf{PGL}(3,q)$. This reduces our calculation to a calculation with 2 by 2 matrices. In fact, there is a slight subtlety that complicates our approach which will be apparent below (this revolves around the difficulty of computing an explicit formula for the inverse of a certain function). We only give the details for the case $P = (1, t, f(t))$ below. Those for $P = (0,0,1)$ and $P = (0,1,0)$ are similar (but much simpler), and also follow from the results of O'Keefe-Thas [16], although we independently checked this.

Two admissions belong here. The calculations are fiendishly difficult, so require the use of computer algebra software. Also, fields of small order (namely 32, 128 and 512) need to be treated separately. Fortunately, a straighforward stabilizer calculation in Magma is feasible for these orders and resolves the issue. The other calculation was performed in Mathematica, in characteristic 2, with variables for the unknown quantities, thereby avoiding the need to compute in infinitely many finite fields. We give some of the details below.

Our tactics involved equating the coefficients of the polynomial equations that result from the magic action (after reducing modulo $x^q + x$). Indeed, for small field orders the exponents coalesce, which is why we resort to Magma in these cases.

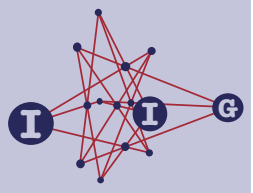
Theorem 4.3. *Let $g \in \mathsf{PGL}(3,q)_{\mathcal{H}}$, $q > 512$. Then $g(0,0,1) \neq (1,t,f(t))$ for any $t \in \mathsf{GF}(q)$.*

Proof. Suppose $g(0,0,1) = (1,t,f(t))$ for $g \in \mathsf{PGL}(3,q)_{\mathcal{H}}$ and $t \in \mathsf{GF}(q)$. Define the permutation $h\colon \mathsf{GF}(q) \to \mathsf{GF}(q)$ by $h(0) = 0$, $h\colon x \mapsto x\big(f(x^{-1}+t) + f(t)\big)$ and let $\phi \in \mathsf{PGL}(3,q)$ be $\phi\colon x \mapsto Ax$, where

$$A = \begin{pmatrix} t & 1 & 0 \\ f(t) & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \in \mathsf{GL}(3,q).$$

Then $(\phi\, g)\mathcal{D}(f) = \mathcal{D}(h^{-1})$, and so by Theorem 4.2 there exists $\psi \in \mathsf{PGL}(2,q)$ such that $\psi f \in \langle h^{-1} \rangle$. Let $\psi\colon x \mapsto Bx$, where $B = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathsf{GL}(2,q)$. From the definition of the magic action it follows that $\psi f h$ is a rational function, and so we can write $\psi f h = \nu/\delta$, for $\nu, \delta \in \mathcal{F}$. Hence, for some $k \in \mathsf{GF}(q)^*$ we have

$$\nu(x) = kx\delta(x) \tag{1}$$



for all $x \in \mathsf{GF}(q)$. A technical calculation shows that the terms appearing in (1) are distinct when $q > 512$, and we can therefore equate coefficients modulo $q-1$ to deduce conditions on ψ. Without loss of generality, $b \neq 0$ and $d \neq 0$. Consideration of the x^{-14} coefficients of (1) gives

$$k(c^{1/2}d^{3\sigma+3}t^{6\sigma} + a^{1/2}b^{6\sigma+9}d^{3\sigma+7/2}t^{6\sigma}) = 0$$

and so $t = 0$. From the x^{-9} and x^{-7} coefficients we deduce

$$b^{3\sigma+4}c^{3\sigma+4} + b^{3\sigma+4}c^{\sigma+2}d^{2\sigma+2} + b^{3\sigma+4}c^{\sigma}d^{2\sigma+4} + a^{\sigma}b^{2\sigma+4}c^{2}d^{3\sigma+2} + a^{3\sigma+4}d^{3\sigma+4} + a^{\sigma}b^{2\sigma+4}d^{3\sigma+4} = 0$$

and

$$b^{3\sigma+4}c^{3\sigma+4} + b^{3\sigma+4}c^{\sigma+2}d^{2\sigma+2} + b^{3\sigma+4}c^{\sigma}d^{2\sigma+4} + a^{3\sigma+4}d^{3\sigma+4} + a^{\sigma+2}b^{2\sigma+2}d^{3\sigma+4} + a^{\sigma}b^{2\sigma+4}d^{3\sigma+4} = 0$$

respectively. Adding these two equations forces $a = 0$. The constant terms now give $b^{3\sigma+10}c^{\sigma}d^{5\sigma+3} = 0$, and so $c = 0$. But this gives $|A| = 0$, a contradiction. □

Corollary 4.4. $\mathsf{PGL}(3,q)_{\mathcal{H}} = 1$ *and*

$$\mathsf{P\Gamma L}(3,q)_{\mathcal{H}} = \left\{(x,y,z) \mapsto (x^{\alpha}, y^{\alpha}, z^{\alpha}) \mid \alpha \in \mathrm{Aut}(\mathsf{GF}(q))\right\}.$$

Corollary 4.5 ([20])**.** *The Cherowitzo hyperovals are new.*

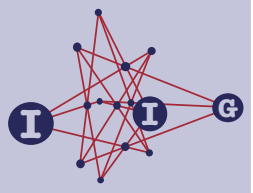
Proof. All other known hyperovals $\mathcal{H}$ have $\mathsf{PGL}(3,q)_{\mathcal{H}} \neq 1$. □

A final remark about the reasons for the difficulty in determining the stabilizers of the Cherowitzo hyperovals is in order. Since the group is so small, there are many candidates for the stabilizer above the group in the lattice of all subgorups of $\mathsf{P\Gamma L}(3,q)$. This may account for the present lack of a good proof.

References

[1] **R. Baer**, Projectivities with fixed points on every line of the plane, *Bull. Amer. Math. Soc.* **52** (1946), 273–286.

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



[3] **A. Bonisoli** and **G. Korchmáros**, Irreducible collineation groups fixing a hyperoval, *J. Algebra* **252** (2002), no. 2, 431–448.

[4] **W. Cherowitzo**, α-flocks and hyperovals, *Geom. Dedicata* **72** (1998), 221–246.

[5] **W. Cherowitzo**, **C. M. O'Keefe** and **T. Penttila**, A unified construction of finite geometries associated with q-clans in characteristic 2, *Adv. Geom.* **3** (2003), 1–21.

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

[7] **L. E. Dickson**, *Linear Groups with an Exposition of the Galois Field Theory*, 1st ed., B.G. Teubner, Leipzig, 1901.

[8] **M. Eich** and **S. E. Payne**, Nonisomorphic symmetric block designs derived from generalized quadrangles., *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei* **52** (1972), no. 8, 893–902.

[9] **W. Feit** and **J. Thompson**, Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), no. 3, 775–1029.

[10] **R. W. Hartley**, Determination of the ternary collineation groups whose coefficients lie in the $\mathsf{GF}(2^n)$, *Ann. of Math.* **27** (1925), no. 2, 140–158.

[11] **J. W. P. Hirschfeld**, *Projective Geometries over Finite Fields*, 2nd ed., Oxford University Press, Oxford, 1998.

[12] **D. R. Hughes**, Generalized incidence matrices over group algebras, *Illinois J. Math.* **1** (1957), 545–551.

[13] **C. M. O'Keefe** and **T. Penttila**, Polynomials for hyperovals of Desaguesian planes, *J. Aust. Math. Soc. Ser. A* **51** (1991), no. 3, 436–447.

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

[15] ———, Automorphism groups of generalized quadrangles via an unusual action of $\mathsf{P\Gamma L}(2, 2^h)$, *European J. Combin.* **23** (2002), 213–232.

[16] **C. M. O'Keefe** and **J. A. Thas**, Collineations of Subiaco and Cherowitzo hyperovals, *Bull. Belg. Math. Soc. Simon Stevin* **3** (1996), 177–192.

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

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

ACADEMIA PRESS

UNIVERSITEIT GENT

[19] **S .E. Payne** and **J. A. Thas**, The stabilizer of the Adelaide oval, *Discrete Math.* **294** (2005), 161–173.

[20] **T. Penttila** and **I. Pinneri**, Hyperovals, *Australas. J. Combin.* **19** (1999), 101–114.

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

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

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

Luke Bayens

Department of Mathematics, Colorado State University, Fort Collins, Colorado 80523-1874, USA

e-mail: bayens@math.colostate.edu

website: http://www.math.colostate.edu/~bayens

William Cherowitzo

Department of Mathematics, University of Colorado at Denver, Campus Box 170, P.O. Box 173364, Denver, Colorado 80217-3364, USA

e-mail: william.cherowitzo@cudenver.edu

website: http://www-math.cudenver.edu/~wcherowi

Tim Penttila

Department of Mathematics, Colorado State University, Fort Collins, Colorado 80523-1874, USA

e-mail: penttila@math.colostate.edu

website: http://www.math.colostate.edu/~penttila