

The Stabilizer of the Adelaide Oval

S. E. Payne

and

J. A. Thas

27 June 02

1 Introduction

Throughout this article $q = 2^e$, $e \geq 1$. The reader is assumed to have a general familiarity with GQ (see [10] for a thorough introduction), and in particular to be familiar with the construction of a GQ starting with a q -clan. (These GQ are often called *flock* GQ because of the connection between flocks of a quadratic cone and q -clans first pointed out in [13].) For a thorough introduction to this construction when $q = 2^e$, see the Subiaco Notebook [6], which is available on the web page of the first author. This unpublished “monograph” is based on several articles by a variety of authors, but we refer the reader to [6] for specific references. When q is even, the existence of the GQ is equivalent to the existence of a family of ovals, called a *herd* of ovals, whose official definition we really do not need here. Later on we will give a specific construction of the ovals in the cases we wish to study.

S. E. Payne, T. Penttila and G. F. Royle [9] used a computer to generate several specific GQ of order (q^2, q) , the largest with $q = 65536$. Some of the smaller examples had already been discovered earlier. These GQ were called *cyclic* because they admit a group of collineations acting as a single cycle on the $q + 1$ lines through the point (∞) . The classical GQ, the so-called FTWKB GQ, and the Subiaco GQ were already well known to be cyclic in this sense, and the new ones seemed certain to belong to a new infinite family. W. E. Cherowitzo, C. M. O’Keefe and T. Penttila [1] discovered a new infinite family that included the examples given in [9], and they gave the name *Adelaide* to all the new associated geometries, i.e., the GQ, the

flocks of the quadratic cone, the ovals, etc. Remarkably they gave a unified construction that included the three previously known infinite families as well as the new Adelaide family. (See [11] for a rather complete survey of the known flock GQ and for q even the associated herds of ovals, as well as much other material related to ovals.)

However, in [1] there is no proof that the unified construction always gives cyclic GQ. This is shown in [7] and will also appear in [2]. Moreover, in [2] there is a proof that for each q there arises just one new GQ and just one new oval (up to isomorphism). On the other hand, the computations in [1] provide a cyclic group of order $2e$ stabilizing the new Adelaide oval. It is the purpose of this note to show that this stabilizer induced by the collineations of the GQ is in fact the complete stabilizer of the Adelaide oval.

2 The q -Clan Functions

Let $F = GF(q) \subseteq GF(q^2) = E$, $q = 2^e$. Write $\bar{x} = x^q$ for $x \in E$. So $x = \bar{x}$ iff $x \in F$. Let ζ be a primitive element of E , so the multiplicative order $|\zeta|$ of ζ is $|\zeta| = q^2 - 1$. Put $\beta = \zeta^{(q-1)}$, so $|\beta| = q + 1$. Then $\bar{\beta} = \beta^q = \beta^{-1}$. Put $\delta = \beta + \bar{\beta}$. More generally, for rational numbers a, b, c in reduced form with denominator relatively prime to $q + 1$ we use the following notation and results:

Lemma 2.1 *The following have easy proofs:*

- (i) $[a] := \beta^a + \bar{\beta}^a$; $\delta = [1]$; $0 = [0]$.
- (ii) $[a] = [b]$ iff $a \equiv \pm b \pmod{q + 1}$.
- (iii) $[a] \cdot [b] = [a + b] + [a - b]$; $[a] + [b] = \left[\frac{a+b}{2}\right] \cdot \left[\frac{a-b}{2}\right]$.
- (iv) $[a]^\sigma = [\sigma a]$ for $\sigma = 2^i \in \text{Aut}(F)$.
- (v) $\left[\frac{a+c}{2}\right] \left[\frac{a}{2}\right] \left[\frac{c}{2}\right] = [a + c] + [a] + [c]$.
- (vi) *The map $\frac{[j+1]}{[j]} \mapsto \frac{[j+1+1]}{[j+1]}$, for all $j \pmod{q + 1}$, permutes the elements of \tilde{F} in a cycle of length $q + 1$. Moreover, this map is the same as the map $t \mapsto t^{-1} + \delta$.*

Write $T(x) = x + \bar{x}$ for $x \in E$, $a(t) = \beta^{\frac{1}{2}}t + \bar{\beta}^{\frac{1}{2}}$, $\nu(t) = t + (\delta t)^{\frac{1}{2}} + 1$, and let $tr : F \rightarrow GF(2)$ be the absolute trace function. Also put $\mathcal{N} = \{\gamma \in E : \gamma^{q+1} = 1 \neq \gamma\}$. In [7] and [2] the original construction of [1] was modified to the following equivalent one.

Theorem 2.2 (*W. E. Cherowitzo, C. M. O’Keefe and T. Penttila*) *Let m be a nonzero residue modulo $q + 1$ for which*

$$tr \left(\frac{T(\gamma^m)}{T(\gamma)} \right) = tr(1) \text{ for all } \gamma \in \mathcal{N}.$$

For $t = \frac{[k+1]}{[k]}$ put

$$f(t) = f \left(\frac{[k+1]}{[k]} \right) = \frac{\left[\frac{(k+1)(m-1)}{2} \right] \left[\frac{k(m+1)}{2} \right]}{[k]} + \left(\frac{[k+1]}{[k]\delta} \right)^{\frac{1}{2}},$$

and

$$g(t) = g \left(\frac{[k+1]}{[k]} \right) = \frac{\left[\frac{(k+1)(m+1)}{2} \right] \left[\frac{k(m-1)}{2} \right]}{[k]} + \left(\frac{[k+1]}{[k]\delta} \right)^{\frac{1}{2}}.$$

Then

$$\mathcal{C} = \left\{ A_t = \begin{pmatrix} f(t) & t^{\frac{1}{2}} \\ 0 & g(t) \end{pmatrix} : t \in F \right\}$$

is a q -clan.

3 The Induced Oval Stabilizer

When $m = \pm 1, \pm \frac{q}{2}, \pm 5$, respectively, the classical, the FTWKB, the Subiaco, respectively, GQ are obtained. When $m = \pm \frac{q-1}{3}$ the new Adelaide examples are obtained. (In [9] it is shown that replacing m with $-m$ is equivalent to interchanging the two elements on the main diagonal of each matrix in the q -clan, which gives isomorphic GQ. Hence it suffices to choose either sign.) Before restricting ourselves to the Adelaide case we consider a particular oval stabilizer in the general case. Keep in mind that this oval stabilizer is completely representative of all ovals except in the case of the Subiaco GQ with $e \equiv 2 \pmod{4}$, in which case there are two orbits of ovals.

In [2] (or see [7]) it is shown that the associated $GQ(\mathcal{C})$ is cyclic. In fact, using Theorem 4.4.1 of [7] (or see [2]) it is clear that certain computations

in [1] determine the full collineation group of $GQ(\mathcal{C})$. In the present note all we need to determine the complete Adelaide stabilizer is the group fixing the line $[A(\infty)]$.

Put

$$A = \begin{pmatrix} 1 & \delta^{-\frac{1}{2}} \\ 0 & \delta^{-\frac{1}{2}} \end{pmatrix} \text{ and } B = \frac{1}{\left[\frac{1}{4}\right]^3} \begin{pmatrix} \left[\frac{m-3}{4}\right] & \left[\frac{m-1}{4}\right] \\ \left[\frac{m+1}{4}\right] & \left[\frac{m+3}{4}\right] \end{pmatrix}.$$

Specifically, (using the notation of [9], [6] and [7]) we know that $\theta = \theta(2, A \otimes B)$ generates a cyclic group (of collineations of $GQ(\mathcal{C})$) of order $2e$ stabilizing the oval \mathcal{O}_α where $\alpha = \left(\left[\frac{m+1}{4}\right], \left[\frac{m-1}{4}\right]\right)$. In fact, it is an easy exercise to check that $\alpha^{(2)}B = \lambda\alpha$, where $\lambda = \left[\frac{1}{4}\right]$. (Here $(a, b)^{(2)}$ means (a^2, b^2) .) Now use Eq. 4.9 of [7] (dividing the right hand image by λ^2) to determine the induced oval stabilizer:

$$\begin{aligned} \hat{\theta} : (1, t, g_t(\alpha)) &\mapsto ((1, t^2)A^{(2)}, \frac{\delta^{-\frac{1}{2}}}{\delta^{\frac{1}{2}}}(g_t(\alpha))^{(2)} + 1 \cdot g_{\left(\frac{1}{\delta}\right)}(\alpha) + 0) = \\ &= \left(1, \frac{1+t^2}{\delta}, \frac{1}{\delta}(\alpha A_t \alpha^T)^{(2)} + \alpha A_{\left(\frac{1}{\delta}\right)} \alpha^T\right). \end{aligned}$$

At this point put $t = \frac{[j+1]}{[j]}$, so $\frac{1+t^2}{\delta} = \frac{[2j+1]}{[2j]}$, and $\frac{1}{\delta} = \frac{[-2+1]}{[-2]}$. Then compute

$$\begin{aligned} \alpha A_t \alpha^T &= \left(\left[\frac{m+1}{4}\right], \left[\frac{m-1}{4}\right]\right) \begin{pmatrix} f(t) & t^{\frac{1}{2}} \\ 0 & g(t) \end{pmatrix} \begin{pmatrix} \left[\frac{m+1}{4}\right] \\ \left[\frac{m-1}{4}\right] \end{pmatrix} = \\ &= \left[\frac{m+1}{2}\right] f(t) + \left[\frac{m+1}{4}\right] \left[\frac{m-1}{4}\right] t^{\frac{1}{2}} + \left[\frac{m-1}{2}\right] g(t) = \\ &= \left[\frac{m+1}{2}\right] \left\{ \frac{\left[\frac{(j+1)(m-1)}{2}\right] \left[\frac{j(m+1)}{2}\right]}{[j]} + \left(\frac{[j+1]}{[j][1]}\right)^{\frac{1}{2}} \right\} + \frac{\left[\frac{m+1}{4}\right] \left[\frac{m-1}{4}\right] \left[\frac{j+1}{2}\right]}{\left[\frac{j}{2}\right]} + \\ &\quad + \left[\frac{m-1}{2}\right] \left\{ \frac{\left[\frac{(j+1)(m+1)}{2}\right] \left[\frac{j(m-1)}{2}\right]}{[j]} + \left(\frac{[j+1]}{[j][1]}\right)^{\frac{1}{2}} \right\} = \\ &= \frac{[jm][1] + [m][j] + [j+1] + [j] + [1]}{[j]}, \text{ after a couple routine steps.} \end{aligned}$$

So with $t = \frac{[j+1]}{[j]}$, the preceding equality says that

$$g_t(\alpha) = \frac{[jm][1] + [m][j] + [j+1] + [j] + [1]}{[j]}. \quad (1)$$

Then with $t = \frac{1}{\delta} = \frac{[-2+1]}{[-2]}$, we have:

$$g_{(\frac{1}{\delta})}(\alpha) = \frac{[2m] + [m][1] + [1]}{[1]}. \quad (2)$$

We finally see that

$$\hat{\theta} : (1, t, g_t(\alpha)) \mapsto (1, t, g_t(\alpha))^{(2)} \begin{pmatrix} 1 & \frac{1}{\delta} & g_{(\frac{1}{\delta})}(\alpha) \\ 0 & \frac{1}{\delta} & 0 \\ 0 & 0 & \frac{1}{\delta} \end{pmatrix},$$

which turns out to be the same as

$$\hat{\theta} : (1, t, g_t(\alpha)) \mapsto (1, \frac{[2j+1]}{[2j]}, \frac{[2jm][1] + [m][2j] + [2j+1] + [2j] + [1]}{[2j]}). \quad (3)$$

If we put

$$p_j = ([j], [j+1], [jm][1] + [m][j] + \left\lfloor \frac{j+1}{2} \right\rfloor \left\lfloor \frac{j}{2} \right\rfloor \left\lfloor \frac{1}{2} \right\rfloor),$$

for j modulo $q+1$, then

$$\mathcal{O}_\alpha = \{p_j : j \pmod{q+1}\}$$

is the oval and $\hat{\theta} : p_j \mapsto p_{2j}$. Since $2^e = q \equiv -1 \pmod{q+1}$, $\hat{\theta}^e : p_j \mapsto p_{-j} = ([j], [j-1], [jm][1] + [m][j] + \left\lfloor \frac{j-1}{2} \right\rfloor \left\lfloor \frac{j}{2} \right\rfloor \left\lfloor \frac{1}{2} \right\rfloor)$.

Put

$$D = \begin{pmatrix} 1 & \frac{1}{\delta} & g_{(\frac{1}{\delta})}(\alpha) \\ 0 & \frac{1}{\delta} & 0 \\ 0 & 0 & \frac{1}{\delta} \end{pmatrix}$$

and

$$E = \begin{pmatrix} 1 & 0 & \frac{[m]+1}{\delta} \\ 0 & 1 & \delta^{-1} \\ 0 & 0 & \delta^{-1} \end{pmatrix}, \quad \text{so } E^{-1} = \begin{pmatrix} 1 & 0 & [m]+1 \\ 0 & 1 & 1 \\ 0 & 0 & \delta \end{pmatrix}.$$

Use the linear map $(x, y, z) \mapsto (x, y, z)E$ to replace the oval \mathcal{O}_α with the oval

$$\mathcal{O}'_\alpha = \{p'_j = ([j], [j+1], [jm]+1) : j \pmod{q+1}\}.$$

Then $\hat{\theta}$ induces the map $\hat{\theta}'$ on \mathcal{O}'_α given by

$$(x, y, z) \mapsto (x, y, z)^{(2)}(E^{-1})^{(2)}DE = (x^2, y^2, z^2) \begin{pmatrix} 1 & \delta^{-1} & 0 \\ 0 & \delta^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Up to this point there are no general results putting restrictions on those m for which the cyclic construction actually works, although for small fields the four examples known are indeed the only ones. However, since for the m that give q -clans we also have the oval \mathcal{O}'_α , it would be interesting to see if there is an easy way to check for which m the set \mathcal{O}'_α is an oval. This is if and only if for distinct a, b and $c \pmod{q+1}$ it is always true that

$$0 \neq \begin{vmatrix} [a] & [a+1] & [am]+1 \\ [b] & [b+1] & [bm]+1 \\ [c] & [c+1] & [cm]+1 \end{vmatrix},$$

which is if and only if

$$[am][b-c] + [bm][c-a] + [cm][a-b] \neq \left[\frac{a-b}{2} \right] \left[\frac{b-c}{2} \right] \left[\frac{c-a}{2} \right]. \quad (4)$$

This is as far as we have progressed on this problem.

From now on we assume that $m = \frac{q-1}{3}$, so we are in the Adelaide case. The unique linear map known that stabilizes the oval \mathcal{O}'_α is the involution given by

$$([j], [j+1], [jm]+1) \mapsto ([j], [j+1], [jm]+1) \begin{pmatrix} 1 & [1] & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = ([j], [j-1], [jm]+1).$$

The fixed points of this involution are the points of the line $x = 0$, i.e., the points $(0, y, z)$. But clearly the unique oval point on this line is the

point $(0, \delta, 1)$, hence this line is a tangent line. The generator of the known stabilizer is $\hat{\theta}'$, which acts on the points of this line as $(0, y, z) \mapsto (0, \frac{y^2}{\delta}, z^2)$, from which it follows that exactly three points on this line are fixed: the oval point $(0, \delta, 1)$ and two others: $(0, 1, 0)$ and $(0, 0, 1)$. But the secant line through p'_j and p'_{-j} passes through the point $(0, 1, 0)$, implying that the nucleus must be $(0, 0, 1)$. Hence

$$\text{The line } [[j+1], [j], 0]^T \text{ is the tangent at } ([j], [j+1], [jm]+1). \quad (5)$$

4 Algebraic Plane Curves

An *algebraic plane curve of degree n* ($n \geq 1$) in $PG(2, q)$ is a set of points $C = V(f) = \{(x, y, z) \in PG(2, q) : f(x, y, z) = 0\}$, where f is an homogeneous nonzero polynomial of degree n in the variables x, y, z . If f is irreducible over $F = GF(q)$, then C is *irreducible*, and if f is irreducible over the algebraic closure \hat{F} of $F = GF(q)$, then C is *absolutely irreducible*. It turned out that each Subiaco hyperoval is the pointset of an absolutely irreducible degree ten algebraic curve in $PG(2, q)$. (This was shown in [5] for $q = 2^e$ with $e \not\equiv 2 \pmod{4}$ and in [8] for $e \equiv 2 \pmod{4}$. Both cases are treated in [6].)

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

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

Recall that an element $g \in P\Gamma L(3, q)$ is of the form $g : p \mapsto p^\sigma B$, where $p = (x, y, z) \in PG(2, q)$, $B \in GL(3, q)$, and $\sigma \in \mathcal{A}$. The image C^g of an algebraic curve $C = V(f)$ under g is the curve $C^g = \{(x, y, z)^g : (x, y, z) \in C\}$. If we want to write $C^g = V(h)$ for some homogeneous polynomial $h = f^g$,

we write

$$f^g(x, y, z) = h(x, y, z) = (f((x, y, z)^{g^{-1}}))^g.$$

Also note that f_x, f_y, f_z denote the partial derivatives of f with respect to x, y, z , respectively.

Let p be a point of the algebraic plane curve $C = V(f)$ of $PG(2, q)$, and let L be a line containing p . Let $p' \in L \setminus \{p\}$; let $p(x, y, z)$ and let $p'(x', y', z')$. If $f(x + tx', y + ty', z + tz') = F(t)$, then the *intersection multiplicity* of L and C at p , denoted $m_p(L, C)$, is the multiplicity of the root $t = 0$ of $F(t)$; see 2.7 of [3]. If $F(t)$ is the zero polynomial then we say that $m_p(L, C) = \infty$. This intersection multiplicity $m_p(L, C)$ is invariant under the action of $PGL(3, q)$. Let \hat{F} denote the algebraic closure of $F = GF(q)$, so that $\hat{C} = V(f)$ is an algebraic plane curve in $PG(2, \hat{F})$. The *multiplicity* of p on C , denoted $m_p(C)$, is the minimum of $m_p(L, \hat{C})$ for all lines L through p in $PG(2, \hat{F})$. Then p is a *singular* point of C if $m_p(C) > 1$ and a *simple* point of C if $m_p(C) = 1$. The curve C is called *singular* or *non-singular* according as C does or does not have a singular point. A line L of $PG(2, \hat{F})$ containing p is a *tangent* line to C at p or *touches* C at p if $m_p(L, \hat{C}) > m_p(C)$. The point p is singular if and only if $f_x(p) = f_y(p) = f_z(p) = 0$. If p is simple, then $f_x(p)x + f_y(p)y + f_z(p)z = 0$ is the equation of the unique tangent line of C at p .

Theorem 4.1 ([3], 2.7, 2.8) *Let $C = V(f)$ 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) *If $f^{(0)} = f^{(1)} = \dots = f^{(m-1)} = 0$ but $f^{(m)} \neq 0, 1 \leq m \leq n$, then C has a point of multiplicity m at $(0, 0, 1)$.*
- (ii) *With m as in (i), there exists $k \leq m$ such that the curve $V(f^{(m)})$ consists of m lines in $PG(2, q^k)$ each of which is a tangent line to C at $(0, 0, 1)$. Here a line corresponding to a linear factor of $f^{(m)}$ with multiplicity s is counted s times, and is said to have multiplicity s at $(0, 0, 1)$. These multiplicities are invariant under the action of $PGL(3, q)$.*

Let $C_1 = V(f_1)$ and $C_2 = V(f_2)$ be algebraic plane curves in $PG(2, q)$ of degrees n_1 and n_2 , respectively, and let $p \in C_1 \cap C_2$. Let \hat{F} denote the

algebraic closure of $F = GF(q)$, so that $\hat{C}_1 = V(f_1)$ and $\hat{C}_2 = V(f_2)$ are algebraic plane curves of degrees n_1 and n_2 in $PG(2, \hat{F})$. Assume $|\hat{C}_1 \cap \hat{C}_2| < \infty$, that is, \hat{C}_1 and \hat{C}_2 have no common component. Coordinates are chosen in such a way that $p(0, 0, 1)$, $(1, 0, 0) \notin C_1 \cap C_2$, and such that any line of $PG(2, \hat{F})$ containing $(1, 0, 0)$ has at most one point in common with $\hat{C}_1 \cap \hat{C}_2$. Let $R_{x_0}(f_1, f_2)$ be the resultant of f_1 and f_2 with respect to x_0 ; so $R_{x_0}(f_1, f_2)$ has degree $n_1 n_2$. If x_1^s is the largest power of x_1 which divides $R_{x_0}(f_1, f_2)$, then s is called the *intersection multiplicity* of C_1 and C_2 at p , denoted $I(p, C_1 \cap C_2)$. If \hat{C}_1 and \hat{C}_2 have a common component, but p does not belong to a common component of \hat{C}_1 and \hat{C}_2 , then delete the common components, which yields curves C'_1 and C'_2 of $PG(2, q)$, and define $I(p, C_1 \cap C_2) = I(p, C'_1 \cap C'_2)$. This intersection multiplicity is invariant under the action of $PGL(3, q)$; see e.g., [12]. Also, this definition of intersection multiplicity is consistent with the definition of $m_p(L, C)$.

Theorem 4.2 (*Theorem of Bézout; see [12]*) *Let $C_1 = V(f_1)$ and $C_2 = V(f_2)$ be algebraic plane curves of degrees n_1 and n_2 , respectively. Let \hat{F} denote the algebraic closure of $F = GF(q)$, so that $\hat{C}_1 = V(f_1)$ and $\hat{C}_2 = V(f_2)$ are algebraic plane curves of degrees n_1 and n_2 in $PG(2, \hat{F})$. If \hat{C}_1 and \hat{C}_2 have no common component, then*

$$\sum_{p \in \hat{C}_1 \cap \hat{C}_2} I(p, \hat{C}_1 \cap \hat{C}_2) = n_1 n_2. \quad (6)$$

Corollary 4.3 ([3], 2.8)

$$\sum_{p \in \hat{C}_1 \cap \hat{C}_2} m_p(\hat{C}_1) m_p(\hat{C}_2) \leq n_1 n_2. \quad (7)$$

5 A Polynomial Equation for the Adelaide Oval

Throughout this section we assume that $q = 2^e$ with e even and $m = \frac{q-1}{3} \equiv \frac{-2}{3} \pmod{q+1}$. If $q = 4$, clearly $m = 1$ and the GQ is classical. If $q = 16$, $m = 5$ and the GQ is the Subiaco GQ. Hence we assume from now on that $q \geq 64$. Since $(m, q+1) = 1$, all the ovals in the herd are projectively equivalent to the following oval:

$$\mathcal{O} = \{([j], [j+1], [jm] + 1) : j \pmod{q+1}\}, \quad (8)$$

with known cyclic stabilizer of order $2e$ generated by

$$\theta : (x, y, z) \mapsto (x^2, \frac{x^2 + y^2}{\delta}, z^2). \quad (9)$$

It is easy to check that for $0 \not\equiv j \pmod{q+1}$

$$T^2 + \delta[j]T + [2j] + \delta^2 = 0 \text{ has the two roots } [j+1] \text{ and } [j-1].$$

Hence

$$0 = \text{tr} \left(\frac{[j]^2 + \delta^2}{\delta^2[j]^2} \right) = \text{tr} \left(\frac{1}{\delta^2} + \frac{1}{[j]^2} \right)$$

for all $j \not\equiv 0 \pmod{q+1}$. But $x^2 + \delta x + 1 = 0$ has roots β and $\bar{\beta}$ which are not in F , so $\text{tr} \left(\frac{1}{\delta^2} \right) = 1$. This implies that

$$\text{tr} \left(\frac{1}{[j]} \right) = 1 \text{ for all } 0 \not\equiv j \pmod{q+1}. \quad (10)$$

Note: Since $[a] = [b]$ iff $a \equiv \pm b \pmod{q+1}$, this means that all $q/2$ elements of F with trace 1 are of the form $\frac{1}{[j]}$.

It is easy to check that $[a]^3 = [3a] + [a]$ for all $a \pmod{q+1}$. So

$$[jm]^3 = \left[\frac{-2j}{3} \right]^3 = [2j] + [jm],$$

implying

$$([jm] + 1)^3 = [jm]^3 + [jm]^2 + [jm] + 1 = [2j] + ([jm] + 1)^2,$$

from which we get

$$([jm] + 1)^3 + ([jm] + 1)^2 + [2j] = 0. \quad (11)$$

So fix $j \not\equiv 0 \pmod{q+1}$ and put

$$G(T) = T^3 + T^2 + [2j].$$

Then $G(T) = 0$ has the root $T = [jm] + 1 = z_1$. Divide $G(T)$ by $T - z_1$ to obtain

$$G(T) = (T - z_1)(T^2 + T(1 + z_1) + (1 + z_1)z_1) = (T - z_1)H(T).$$

The quadratic factor $H(T)$ is irreducible over F , because

$$\text{tr} \left(\frac{(1 + z_1)z_1}{(1 + z_1)^2} \right) = \text{tr} \left(\frac{z_1}{1 + z_1} \right) = \text{tr} \left(\frac{[jm] + 1}{[jm]} \right) = \text{tr} \left(1 + \frac{1}{[jm]} \right) = 0 + 1 = 1,$$

by Eq. 10 and the fact that e is even. This proves that

$$[jm] + 1 \text{ is the unique root in } F \text{ of } T^3 + T^2 + [2j] = 0. \quad (12)$$

The line $[[jm] + 1, 0, [j]]^T$ is a secant line to \mathcal{O} containing the two oval points $([j], [j + 1], [jm] + 1)$ and (replace j with $-j$) $([j], [j - 1], [jm] + 1)$. So if $([j], y_1, [jm] + 1)$ and $([j], y_2, [jm] + 1)$ are these two points, we know $y_1 + y_2 = [j + 1] + [j - 1] = \delta[j]$, and $y_1 y_2 = [j + 1][j - 1] = [j]^2 + \delta^2$. This proves

$$([j], y, [jm] + 1) \in \mathcal{O} \text{ iff } y \text{ is a root of } T^2 + \delta[j]T + [j]^2 + \delta^2 = 0. \quad (13)$$

Note the following: $[jm] + 1 \neq 0$ for all j modulo $q + 1$. This is clearly true for $j \equiv 0 \pmod{q + 1}$. And if $j \not\equiv 0 \pmod{q + 1}$, then $\frac{1}{[jm]} \neq 1$ since $\text{tr}(1) = 0$ and $\text{tr} \left(\frac{1}{[jm]} \right) = 1$. So if (x, y, z) is an arbitrary point of \mathcal{O} , then $z \neq 0$. If $x = 0$, then $(x, y, z) \equiv (0, \delta, 1) = \lambda(x, y, z)$ with $\lambda = z^{-1}$. If $x \neq 0$, then $(x, y, z) \equiv \left(1, \frac{y}{x}, \frac{z}{x} \right)$. There is a unique $j \pmod{q + 1}$, $j \not\equiv 0 \pmod{q + 1}$, for which $\frac{y}{x} = \frac{[j+1]}{[j]}$. Put $\lambda = \frac{[j]}{x}$. So $\lambda(x, y, z) = (\lambda x, \lambda y, \lambda z) = ([j], [j + 1], \lambda z)$ where $\lambda z (= [jm] + 1)$ is the unique root in F of $T^3 + T^2 + (\lambda x)^2 = 0$. This proves

$$\lambda = \frac{x^2 + z^2}{z^3}, \text{ and } \lambda^2 = \frac{x^4 + z^4}{z^6}. \quad (14)$$

By Eq. 13 $(\lambda y)^2 + \delta(\lambda x)(\lambda y) + (\lambda x)^2 + \delta^2 = 0$, so $\lambda^2(y^2 + \delta xy + x^2) = \delta^2$, proving

$$\lambda^2 = \frac{\delta^2}{y^2 + \delta xy + x^2}. \quad (15)$$

This is well defined since $y^2 + \delta xy + x^2 = (y + \beta x)(y + \bar{\beta} x) \neq 0$ for nonzero $x, y \in F$.

Putting the two previous equations together, we have

Lemma 5.1 *If $(x, y, z) \in \mathcal{O}$, then $\delta^2 z^6 = (z^4 + x^4)(y^2 + \delta xy + x^2)$.*

Define $G(x, y, z)$ by

$$\begin{aligned} G(x, y, z) &= \delta^2 z^6 + (z^4 + x^4)(y^2 + \delta xy + x^2) \\ &= (x^4 + z^4)y^2 + (\delta x(x^4 + z^4))y + \delta^2 z^6 + z^4 x^2 + x^6 \end{aligned} \quad (16)$$

$$\begin{aligned} &= \sum_{i=0}^6 f^{(i)}(x, z) \cdot y^{6-i}, \text{ with} \\ &f^{(0)} = f^{(1)} = f^{(2)} = f^{(3)} = 0; f^{(4)} \neq 0. \end{aligned} \quad (17)$$

This shows that $(0, 1, 0)$ is a singular point of $C : G(x, y, z) = 0$ with multiplicity 4. The line $x = z$ is the unique tangent line of C at $(0, 1, 0)$ and it has multiplicity 4 at $(0, 1, 0)$.

It is also easy to check that

$$\frac{\partial G}{\partial x} = \delta y(x^4 + z^4); \quad \frac{\partial G}{\partial y} = \delta x(x^4 + z^4); \quad \frac{\partial G}{\partial z} = 0.$$

It now follows readily that $(0, 1, 0)$ is the only point (x, y, z) satisfying

$$G(x, y, z) = \frac{\partial G}{\partial x}(x, y, z) = \frac{\partial G}{\partial y}(x, y, z) = \frac{\partial G}{\partial z}(x, y, z) = 0.$$

The unique singular point of $C : G(x, y, z) = 0$ is $(0, 1, 0)$. (18)

If (x_0, y_0, z_0) is a simple point of C , then the tangent line of C at this point has equation $\delta y_0(x_0^4 + z_0^4)x + \delta x_0(x_0^4 + z_0^4)y = 0$, so $y_0 x + x_0 y = 0$, and hence contains the point $(0, 0, 1)$ which does not belong to C .

It is of interest to check directly that the collineation θ of Eq. 9 does leave C invariant and fixes the point $(0, 1, 0)$, which is not on \mathcal{O} .

Theorem 5.2 $C = \mathcal{O} \cup \{(0, 1, 0)\}$.

Proof: We know that $\mathcal{O} \cup \{(0, 1, 0)\} \subseteq C$, so let (x, y, z) be an arbitrary point of C . If $z = 0$, then $x^4(y^2 + \delta xy + x^2) = 0$. If also $x = 0$, then we get the point $(0, 1, 0)$. If $x \neq 0$, then $y^2 + \delta xy + x^2$ cannot be 0 for $x, y \in F$. So $(0, 1, 0)$ is the only point $(x, y, z) \in C$ with $z = 0$. Suppose $z \neq 0$. If $x = 0$,

then $G(x, y, z) = 0$ implies that $y = \delta z$ and we get the point $(0, \delta, 1)$ of \mathcal{O} . So we may assume that $x \neq 0 \neq z$.

There is a unique $j \pmod{q+1}$ for which $\frac{y}{x} = \frac{[j+1]}{[j]}$. So

$$(x, y, z) \equiv \frac{[j]}{x}(x, y, z) = \left([j], [j+1], \frac{z[j]}{x} \right) \in C.$$

First check that $[j+1]^2 + [1][j][j+1] + [j]^2 = \delta^2$. Then from $G([j], [j+1], \frac{z[j]}{x}) = 0$, we have

$$\delta^2 \left(\frac{z^6 [j]^6}{x^6} \right) = \left[\left(\frac{z[j]}{x} \right)^4 + [j]^4 \right] \delta^2.$$

Divide by δ^2 to get

$$\left(\frac{z[j]}{x} \right)^6 + \left(\frac{z[j]}{x} \right)^4 + [j]^4 = 0.$$

Take the square root to find that

$$\left(\frac{z[j]}{x} \right)^3 + \left(\frac{z[j]}{x} \right)^2 + [j]^2 = 0.$$

We know by Eq. 12 that $\frac{z[j]}{x} = [jm] + 1$. Hence $(x, y, z) \in \mathcal{O}$. ■

6 Irreducibility of the Curve

Recall that if

$$G(x, y, z) = \delta^2 z^6 + (x^4 + z^4)(x^2 + \delta xy + y^2),$$

then

$$C = \{(x, y, z) \in PG(2, q) : G(x, y, z) = 0\}$$

has a unique singular point $P = (0, 1, 0)$ with multiplicity 4, and the line $[1, 0, 1]^T$ is the unique tangent line to C at P and it has multiplicity 4 there. Let \hat{F} be an algebraic closure of F and $\hat{C} = \{(x, y, z) \in PG(2, \hat{F}) : G(x, y, z) = 0\}$. Since $x + z$ does not divide $\delta^2 z^6$, the tangent line $[1, 0, 1]^T$ is not a component of \hat{C} . As \hat{C} has a unique singular point, each irreducible

factor of $G(x, y, z)$ over \hat{F} has multiplicity 1. Suppose the irreducible components of \hat{C} are $\hat{C}_1, \dots, \hat{C}_r$ for some $r > 1$, where $\deg(\hat{C}_i) = n_i$ and \hat{C}_i has multiplicity m_i at P . If for some i we have $m_i = n_i$, then $m_i = n_i = 1$ and the component \hat{C}_i is a line, which must therefore be a tangent to \hat{C}_i , and hence to \hat{C} , at $(0,1,0)$. This possibility is already ruled out. Since $n_1 + \dots + n_r = 6$ and $m_1 + \dots + m_r = 4$ with $n_i > m_i \geq 0$ for all i , so $(n_1 - m_1) + (n_2 - m_2) + \dots + (n_r - m_r) = 2$, it must be that $r = 2$, $n_1 = m_1 + 1$, $n_2 = m_2 + 1$, and without loss of generality we may assume that $(n_1, n_2) \in \{(1, 5), (2, 4), (3, 3)\}$. As P is the unique singular point of \hat{C} it is the unique common point of \hat{C}_1 and \hat{C}_2 . In particular, each of \hat{C}_1, \hat{C}_2 has the point P with multiplicity at least 1, implying $n_i \geq 2$, forcing $(n_1, n_2) = (2, 4)$ or $(3, 3)$.

Suppose that \hat{C}_1 and \hat{C}_2 are not defined over F , but rather over some extension $GF(q^s)$ with $s > 1$. Let σ be a generator of the Galois group $\text{Gal}(GF(q^s)/GF(q))$. Then $\hat{C}_1^\sigma = \hat{C}_2$, which implies $n_1 = n_2 = 3$. Let $C_i = PG(2, F) \cap \hat{C}_i$, with $i = 1, 2$. By [3], Lemma 2.24 (i), it must be that $|C_i| \leq 3^2$, so $|C| \leq 2(9) - 1 = 17$. But $|C| = q + 2$ and $q \geq 64$, so this case cannot occur. Hence \hat{C}_1 and \hat{C}_2 are defined over $F = GF(q)$.

Again let $C_i = PG(2, F) \cap \hat{C}_i$, with $i = 1, 2$. Suppose that C_1 is irreducible of degree 2 over F . Since $|C_1 \cap \mathcal{O}| \geq q$, it follows by Theorem 10.21 of [3] that the unique complete arc containing $C_1 \cap \mathcal{O}$ is $O \cup \{(0, 0, 1)\} = C_1 \cup \{\text{nucleus of } C_1\}$ and hence $(0, 1, 0) \in O$, an impossibility. So we must have $(n_1, n_2) = (3, 3)$. This means that each component C_i is an irreducible cubic having $(0, 1, 0)$ as a unique double point (singular point with multiplicity 2) with a unique tangent at $(0, 1, 0)$.

At this point we know that C_1 and C_2 are cubic curves with a cusp at $(0, 1, 0)$ (i.e., $(0, 1, 0)$ is a double point with a unique tangent). By table 11.7, p. 260 of [3], C_1 and C_2 each have $q + 1$ points with one point in common. This implies $|C| = 2q + 1$, an impossibility. This completes a proof of the following theorem.

Theorem 6.1 *The curve $C : G(x, y, z) = 0$ is absolutely irreducible.*

7 The Complete Oval Stabilizer

Lemma 7.1 $PGL(3, q)_\mathcal{O} \subseteq PGL(3, q)_{\hat{C}}$.

Proof: Let $\theta \in PGL(3, q)_{\mathcal{O}}$. Recall $C = \mathcal{O} \cup \{(0, 1, 0)\}$. Suppose $\hat{C} \neq \hat{C}^\theta$. Since $\mathcal{O} \subseteq \hat{C} \cap \hat{C}^\theta$,

$$q + 1 \leq \sum_{p \in \hat{C} \cap \hat{C}^\theta} m_p(\hat{C}) \cdot m_p(\hat{C}^\theta) \leq 6^2 = 36.$$

Hence if $q \geq 64$ then $\hat{C}^\theta = \hat{C}$, completing the proof. ■

This means that $\theta \in PGL(3, q)_{\mathcal{O}}$ must also fix the points $(0, 1, 0)$ and $(0, 0, 1)$. Since we have a collineation fixing \mathcal{O} belonging to each field automorphism, it suffices just to consider the homographies $\theta \in PGL(3, q)_{\mathcal{O}}$.

Suppose that θ is a non-identity homography

$$\theta : (x, y, z) \mapsto (x, y, z)A.$$

Since θ fixes $(0, 1, 0)$ and $(0, 0, 1)$ we may assume WLOG that

$$A = \begin{pmatrix} a & b & e \\ 0 & d & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{with } a \cdot d \neq 0.$$

But θ must also fix $(0, \delta, 1)$, the unique point of \mathcal{O} on the fixed line $x = 0$. Since $(0, \delta, 1)A = (0, d\delta, 1)$, it follows that $d = 1$.

But then it follows that θ is a perspectivity with axis the line $x = 0$. Hence θ is involutorial with center on the line $x = 0$. Consequently $a = 1$. As θ fixes the tangent line $x = z$ of C at $(0, 1, 0)$, we now have $e = 0$. So $(0, 1, 0)$ is the center of the perspectivity. By the last part of Section 4,

$$([j], [j + 1], [jm] + 1)^\theta = ([j], [j - 1], [jm] + 1),$$

implying that $b[j] = [j + 1] + [j - 1] = [j][1]$, i.e., $b = \delta$.

Of course this forces θ to be either the identity or the other linear involution that we already know stabilizes the oval \mathcal{O} . This concludes our proof of the following.

Theorem 7.2 *The complete stabilizer of the Adelaide oval is exactly the stabilizer induced by the automorphism group of the Adelaide generalized quadrangle.*

The argument used in the proof of Lemma 7.1 also shows that if θ fixes the hyperoval $\mathcal{O} \cup (0, 0, 1)$, then it also fixes the curve \hat{C} . But the point

$(0,0,1)$, as the intersection of the tangents to C at all points other than the singular point $(0,1,0)$, must also be fixed. Hence θ fixes the Adelaide oval. This proves the following:

Corollary 7.3 *The full stabilizer of the Adelaide hyperoval is the same as the stabilizer of the Adelaide oval and is induced by the collineation group of the Adelaide GQ.*

References

- [1] W. E. Cherowitzo, C. M. O’Keefe, and T. Penttila, A unified construction of finite geometries in characteristic two, preprint, 2001.
- [2] W. E. Cherowitzo and S. E. Payne, The cyclic q -clan geometries, in preparation, 2002.
- [3] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd Ed., Oxford University Press, Oxford (1998).
- [4] C. M. O’Keefe and T. Penttila, Automorphism groups of generalized quadrangles via an unusual action of $PGL(2, 2^h)$, *European J. Combin.*, 23(2002), 213 – 232.
- [5] C. M. O’Keefe and J. A. Thas, Collineations of Subiaco and Cherowitzo hyperovals, *Bull. Belg. Math. Soc. Simon Stevin*, 3(1996), 177–192.
- [6] S. E. Payne, *The Subiaco Notebook: An Introduction to q -Clan Geometry, $q = 2^e$* , available at <http://www-math.cudenver.edu/~spayne/>.
- [7] S. E. Payne, *Four Lectures in Napoli: An Introduction to q -Clan Geometry, $q = 2^e$* , Winter 2002, 63 pages.
- [8] S. E. Payne, T. Penttila and I. Pinneri, Isomorphisms between Subiaco q -clan geometries, *Bull. Belg. Math. Soc. Simon Stevin*, 2(1995), 197 – 222.
- [9] S. E. Payne, T. Penttila and G. F. Royle, Building a cyclic q -clan, in *Mostly Finite Geometries* (ed. N. L. Johnson), Marcel Dekker, 1997, pp. 365 – 378.

- [10] S. E. Payne and J. A. Thas, *Finite Generalized Quadrangles*, Pitman, 1984.
- [11] T. Penttila, Configurations of ovals, in *Combinatorics 2002: Topics in Combinatorics: Geometry, Graph Theory and Designs*, Maratea (Potenza), Italy, 2 – 8 June 2002, pp. 220 - 241.
- [12] A. Seidenberg, *Elements of the Theory of Algebraic Curves*, Addison-Wesley, Reading, Mass., 1968, 216 pp.
- [13] J. A. Thas, Generalized quadrangles and flocks of cones, *European J. Combin.*, 8(1987), 441-452.

Addresses of the Authors:

S. E. Payne
Department of Mathematics, Campus Box 170
1250 14th Street, Suite 600 (80202)
P.O.Box 173364
Denver, Colorado 80217-3364
spayne@carbon.cudenver.edu

J. A. Thas
Dept. Pure Maths & Computer Algebra
University of Ghent
Krijgslaan 281 – S22
Gent
B-9000 Belgium
jat@cage.rug.ac.be