Adv. Geom. **3** (2003), 1–21

Advances in Geometry

A unified construction of finite geometries associated with q-clans in characteristic 2

William E. Cherowitzo, Christine M. O'Keefe and Tim Penttila*

(Communicated by G. Korchmáros)

Dedicated to Louis Reynolds Antoine Casse

Abstract. Flocks of Laguerre planes, generalized quadrangles, translation planes, ovals, BLT-sets, and the deep connections between them, are at the core of a developing theory in the area of geometry over finite fields. Examples are rare in the case of characteristic two, and it is the purpose of this paper to contribute a fifth infinite family. The approach taken leads to a unified construction of this new family with three of the previously known infinite families, namely those satisfying a symmetry hypothesis concerning cyclic subgroups of $\mathrm{PGL}(2,q)$. The calculation of the automorphisms of the associated generalized quadrangles is sufficient to show that these generalized quadrangles and the associated flocks and translation planes do not belong to any previously known family.

Key words. Flocks, ovals, herds, hyperovals, Adelaide q-clans, translation planes, generalized quadrangles.

2000 Mathematics Subject Classification. Primary 51E21, 51E20, 51E12, 51E15; Secondary 05B25

1 Introduction

The last twenty years have seen extensive activity in the area of finite geometry, with the publication of many papers dealing with the connections between flocks of Laguerre planes, generalized quadrangles, translation planes, ovals and BLT-sets. In this setting, we identify some significant papers as follows. First, the sequence of exchanges between Kantor and Payne delineated the evolution of the concept of a q-clan and the construction of generalized quadrangles as group coset geometries [14, 23, 33, 15, 24], while Thas [40] recognised the connection between flocks of Laguerre planes and generalized quadrangles. In the case of odd characteristic, Bader, Lunardon and Thas [2] introduced BLT-sets and Knarr [16] developed a geo-

* This work was supported by the Australian Research Council.

metric construction of the generalized quadrangle from the BLT-set. In the case of even characteristic, Payne and Cherowitzo, Penttila, Pinneri and Royle [24, 6] introduced herds of ovals and elucidated their connection with the generalized quadrangles. The sequence of papers by Thas [41, 42, 43] on translation generalized quadrangles of order (s, s^2) culminated in a geometric construction of the generalized quadrangle from the flock in all characteristics. Finally, the connection between ovals and flocks of translation Laguerre planes was explained by Cherowitzo [5].

In the case of odd characteristic, the BLT-set and the Knarr construction provide useful insights into the connections between the geometries mentioned above, while recent constructions of families [34, 18] as well as many sporadic examples over small fields [38, 17] suggest that there may in fact be an embarassment of riches. The situation in characteristic two stands in stark contrast: there are only four known families, to which we add a fifth in this paper, and no known sporadic example. In compensation for this paucity of examples in characteristic two, there is a rich association with ovals and hyperovals which is missing in odd characteristic. The ovals so arising, in turn, lead to further generalized quadrangles and Laguerre planes. Furthermore, characterisation theorems have been proved in characteristic two [13, 9, 19, 39, 20], suggesting that the rarity of examples in characteristic two is not merely temporary.

Despite the recent activity and advances, there is much work still to be done, even in characteristic two. In this case, O'Keefe and Penttila [20] obtained characterisations with symmetry hypotheses concerning subgroups of order q and $q-1$ of $\mathrm{PGL}(2, q)$, leaving the (cyclic) subgroups of order $q+1$ still to be dealt with. The cyclic hypothesis was first suggested by the Subiaco examples [6, 27, 1, 30] and the examples for $q = 4^3$ and 4^4 discovered by Penttila and Royle [37]. The different approach to automorphism calculations possible in characteristic two [28] led to a further exploration by Payne, Penttila and Royle [31] and to further examples for $q = 4^5, 4^6, 4^7$ and 4^8. In this paper we generalise these six examples to a new infinite family. We remark that the cyclic hypothesis is satisfied by three of the previously known families (the exception is the family of Payne [24]), and this paper contributes a unified construction of these three families with the new family. This work should contribute to an eventual classification in this case, characterising these four families by the cyclic hypothesis.

Finally, another persistent thread in the recent literature concerns the automorphisms of the associated geometries investigated by Payne and several others [32, 26, 27, 1, 30, 28, 29, 22]. The recent results by O'Keefe and Penttila [20] allow the interpretation of the cyclic hypothesis in the herd model. This interpretation is important because it led to the unified construction contained in this paper, as was suggested at the end of the introduction of [20]. In the current context, we also use O'Keefe and Penttila's techniques [20] to calculate the groups of the geometries we construct, and hence to show that the associated generalized quadrangles, flocks and translation planes are new. We do not yet have a proof that the associated hyperovals do not belong to the previously known families, although this is true for those over the fields of orders 4^3 and 4^4. Such a proof would require more information concerning the groups of the hyperovals. Here it is appropriate to note that the groups of the Cherowitzo hyperovals [4] have yet to be determined, although the partial results of

O'Keefe and Thas [21] were enough for Penttila and Pinneri [35] to show that the Cherowitzo hyperovals were new.

2 Preliminaries

Let $\mathscr{C} = \{A_t : t \in \mathrm{GF}(q)\}$ be a collection of 2×2 matrices with entries from $\mathrm{GF}(q)$. Following Payne [25], we call $\mathscr{C}$ a *q-clan* if $A_s - A_t$ is anisotropic (that is, the equation $(x, y)(A_s - A_t)(x, y)^T = 0$ has only the trivial solution $(x, y) = (0, 0)$) for all $s, t \in \mathrm{GF}(q)$ with $s \neq t$.

We will use the (absolute) trace function on $\mathrm{GF}(q)$, $q = 2^e$, as follows. Let trace : $\mathrm{GF}(q) \to \mathrm{GF}(q)$ be defined by $\mathrm{trace}(x) = x + x^2 + \cdots + x^{2^{e-1}}$.

As is discussed by Cherowitzo, Penttila, Pinneri and Royle [6, 2.1], without loss of generality we can assume that

$$A_t = \begin{pmatrix} f(t) & t^{1/2} \\ 0 & ag(t) \end{pmatrix}$$

where $a \in \mathrm{GF}(q)$ satisfies $\mathrm{trace}(a) = 1$, $f, g : \mathrm{GF}(q) \to \mathrm{GF}(q)$ are functions satisfying $f(0) = g(0) = 0$ and $f(1) = g(1) = 1$ and

$$\mathrm{trace}\left(\frac{a(f(s) + f(t))(g(s) + g(t))}{s + t}\right) = 1 \tag{2.1}$$

for all $s, t \in \mathrm{GF}(q)$ with $s \neq t$.

Conversely, if there exist functions $f, g : \mathrm{GF}(q) \to \mathrm{GF}(q)$ with $f(0) = g(0) = 0$ and $f(1) = g(1) = 1$ and an element $a \in \mathrm{GF}(q)$ with $\mathrm{trace}(a) = 1$ such that Equation (2.1) holds, then the set of matrices $\left\{\begin{pmatrix} f(t) & t^{1/2} \\ 0 & ag(t) \end{pmatrix} : t \in \mathrm{GF}(q)\right\}$ is a q-clan.

We call a q-clan *normalised* if it is written in this standard form and note that it follows immediately from Equation (2.1) that f and g are permutation polynomials.

In the following subsections we show how q-clans, q even, can be used to construct various important geometric structures, thus motivating their study. We then survey the known q-clans, q even, to the time of preparation of this paper.

2.1 Flocks of quadratic cones. Let $\mathscr{O}$ be an oval in $\mathrm{PG}(2, q)$, and let $\mathrm{PG}(2, q)$ be embedded as a hyperplane in $\mathrm{PG}(3, q)$. For a point $v \in \mathrm{PG}(3, q) \backslash \mathrm{PG}(2, q)$, the union of the points on the lines incident with v and a point of $\mathscr{O}$ is the *cone* with *vertex* v and *base* $\mathscr{O}$. A *quadratic cone* is a cone with base $\mathscr{O}$ a (non-degenerate) conic. A *flock* of a cone $\mathscr{K}$ with vertex v is a set of q planes which partitions $\mathscr{K} \backslash \{v\}$ into disjoint ovals. If L is a line of $\mathrm{PG}(3, q)$ having no point in common with $\mathscr{K}$ then the q planes through L and not v form a flock. Such a flock is called *linear*, and for $q = 2, 3$ and 4 every flock of a cone is linear [40].

Theorem 2.1 ([24, 40]). *Let q be even and let $\mathscr{K}$ be the quadratic cone in* $\mathrm{PG}(3, q)$ *with equation $X_0X_1 = X_2^2$; thus the vertex is $v = (0, 0, 0, 1)$. The set of planes $\mathscr{F} =$*

$\{a_tX_0 + c_tX_1 + b_tX_2 + X_3 = 0 : t \in \mathrm{GF}(q)\}$ *is a flock of* $\mathcal{K}$ *if and only if* $b_t \neq b_s$ *for* $s \neq t$ *and*

$$\mathrm{trace}\left(\frac{(a_s + a_t)(c_s + c_t)}{(b_s + b_t)^2}\right) = 1 \quad \textit{for all } s \neq t.$$

By Equation (2.1), with q even, we have: $\mathcal{C} = \left\{\begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} : t \in \mathrm{GF}(q)\right\}$ is a q-clan if and only if $\mathcal{F} = \{a_tX_0 + c_tX_1 + b_tX_2 + X_3 = 0 : t \in \mathrm{GF}(q)\}$ is a flock of the quadratic cone $\mathcal{K}$ in $\mathrm{PG}(3,q)$ with equation $X_0X_1 = X_2^2$.

2.2 Elation generalized quadrangles. Let $\mathcal{G} = \{(\alpha, c, \beta) : \alpha, \beta \in \mathrm{GF}(q)^2, c \in \mathrm{GF}(q)\}$, with multiplication defined as:

$$(\alpha, c, \beta)(\alpha', c', \beta') = (\alpha + \alpha', c + c' + \beta \circ \alpha', \beta + \beta'),$$

where (since α, β are 2-tuples of elements of $\mathrm{GF}(q)$) we define:

$$\beta \circ \alpha = \sqrt{\beta P \alpha^T}, \quad \text{with } P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let $\mathcal{C} = \{A_t : t \in \mathrm{GF}(q)\}$ be a normalised q-clan, and define the following subgroups of $\mathcal{G}$:

$$A(\infty) = \{(0, 0, \beta) : \beta \in \mathrm{GF}(q)^2\} \quad \text{and}$$
$$A(t) = \{(\alpha, \sqrt{\alpha A_t \alpha^T}, t^{1/2}\alpha) : \alpha \in \mathrm{GF}(q)^2\}, \quad t \in \mathrm{GF}(q).$$

For each $t \in \mathrm{GF}(q) \cup \{\infty\}$ we define $A^*(t) = A(t)Z$ where $Z = \{(0, c, 0) : c \in \mathrm{GF}(q)\}$ is the centre of $\mathcal{G}$. Then $\mathcal{F} = \{A(t) : t \in \mathrm{GF}(q) \cup \{\infty\}\}$ is a 4-*gonal family* for $\mathcal{G}$ [24], see [33, 10.4].

Starting with this 4-gonal family, Kantor's [14] construction gives an elation generalized quadrangle of order (q^2, q) (with base point (∞)) on which $\mathcal{G}$ acts by left multiplication as a group of elations, see [33, 8.2], as follows:

points: (i) elements $g \in G$, (ii) cosets $gA^*(t)$ for $g \in G$, $t \in \mathrm{GF}(q) \cup \{\infty\}$ and (iii) a symbol (∞),

lines: (a) cosets $gA(t)$ for $g \in G$, $t \in \mathrm{GF}(q) \cup \{\infty\}$ and (b) symbols $[A(t)]$ for $t \in \mathrm{GF}(q) \cup \{\infty\}$.

(Here we use left cosets, in contrast to some of the literature which uses right cosets, because *throughout this paper* groups are acting on the left.) A point g of type (i) is incident with each line $gA(t)$ for $t \in \mathrm{GF}(q) \cup \{\infty\}$. A point $gA^*(t)$ of type (ii) is incident with the line $[A(t)]$ and with each line $hA(t)$ contained in $gA^*(t)$. The point (∞) is incident with each line $[A(t)]$ for $t \in \mathrm{GF}(q) \cup \{\infty\}$. There are no further incidences.

We have therefore outlined a process by which a (normalised) q-clan $\mathscr{C}$ gives rise to a 4-gonal family for the group $\mathscr{G}$ above, and hence to an elation generalized quadrangle $\mathrm{GQ}(\mathscr{C})$ of order (q^2, q).

2.3 Herds of ovals. A *herd* [6] of ovals in $\mathrm{PG}(2,q)$, q even, is a family of $q+1$ ovals $\{\mathscr{O}_s : s \in \mathrm{GF}(q) \cup \{\infty\}\}$, each of which has nucleus $(0,0,1)$, contains the points $(1,0,0), (0,1,0)$ and $(1,1,1)$, and is such that

$$\begin{aligned} \mathscr{O}_\infty &= \{(1,t,g(t)) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0)\} \quad \text{and} \\ \mathscr{O}_s &= \{(1,t,f_s(t)) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0)\}, \end{aligned}$$

where

$$f_s(t) = \frac{f_0(t) + asg(t) + s^{1/2}t^{1/2}}{1 + as + s^{1/2}}$$

for some $a \in \mathrm{GF}(q)$ satisfying $\mathrm{trace}(a) = 1$.

Theorem 2.2 ([24, 6]). *Let q be even. Let $f_0, g : \mathrm{GF}(q) \to \mathrm{GF}(q)$ be functions with $f_0(0) = g(0) = 0$ and $f_0(1) = g(1) = 1$. There exists $a \in \mathrm{GF}(q)$ with* $\mathrm{trace}(a) = 1$ *and such that*

$$\mathrm{trace}\left(\frac{a(f_0(s) + f_0(t))(g(s) + g(t))}{(s+t)}\right) = 1 \quad \textit{for all } s \neq t$$

if and only if $\{\mathscr{O}_s : s \in \mathrm{GF}(q) \cup \{\infty\}\}$ is a herd, where

$$\begin{aligned} \mathscr{O}_\infty &= \{(1,t,g(t)) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0)\} \quad \textit{and} \\ \mathscr{O}_s &= \left\{\left(1, t, \frac{f_0(t) + asg(t) + s^{1/2}t^{1/2}}{1 + as + s^{1/2}}\right) : t \in \mathrm{GF}(q)\right\} \cup \{(0,1,0)\}. \end{aligned}$$

By Equation (2.1), with q even, we have: $\mathscr{C} = \left\{\begin{pmatrix} f_0(t) & t^{1/2} \\ 0 & ag(t) \end{pmatrix} : t \in \mathrm{GF}(q)\right\}$ is a q-clan if and only if $\{\mathscr{O}_s : s \in \mathrm{GF}(q) \cup \{\infty\}\}$ is a herd.

2.4 Translation planes. Thas [8] and Walker [44] independently showed how to construct a translation plane from a flock of a quadratic cone. We now give a brief outline of this construction, and note that relevant details and background can be found in [10, 12].

Let $\mathscr{F}(\mathscr{C})$ be the flock of the quadratic cone $\mathscr{K}$ of $\mathrm{PG}(3,q)$ with equation $X_0X_1 = X_2^2$, associated with the q-clan $\mathscr{C}$. Embed $\mathscr{K}$ into the Klein Quadric $\mathrm{Q}^+(5,q)$

in $\mathrm{PG}(5,q)$ and let $\perp$ denote the polarity of $\mathrm{PG}(5,q)$ associated with $\mathrm{Q}^+(5,q)$. The set of points $\Omega = \bigcup_{\pi \in \mathscr{F}(\mathscr{C})} \pi^\perp \cap \mathrm{Q}^+(5,q)$ is an ovoid of $\mathrm{Q}^+(5,q)$, and we let $\mathscr{S}$ be the spread of $\mathrm{PG}(3,q)$ associated with Ω via the Klein correspondence. By the André–Bruck Bose correspondence, from $\mathscr{S}$ there arises a translation plane $\pi(\mathscr{C})$ of order q^2 with kernel containing $\mathrm{GF}(q)$.

2.5 The known *q*-clans, *q* even. In this section we list the known q-clans with $q = 2^e$, up to isomorphism of the associated generalized quadrangle.

The *classical* q-clan associated with a linear flock [40], for all $q = 2^e$, is

$$\mathscr{C} = \left\{ \begin{pmatrix} t^{1/2} & t^{1/2} \\ 0 & at^{1/2} \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$$

for $a \in \mathrm{GF}(q)$ with $\mathrm{trace}(a) = 1$. The associated GQ is isomorphic to the GQ comprising the points and lines of the Hermitian variety $\mathrm{H}(3,q^2)$ (see [33, 3.1.1]) and the associated translation plane is Desarguesian. The associated herd is $\{\mathscr{O}_s : s \in \mathrm{GF}(q) \cup \{\infty\}\}$, where $\mathscr{O}_s = \{(1,t,t^{1/2}) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0)\}$ for all $s \in \mathrm{GF}(q) \cup \{\infty\}$.

The *FTWKB* q-clan, for $q = 2^e$ with e odd, is

$$\mathscr{C} = \left\{ \begin{pmatrix} t^{1/4} & t^{1/2} \\ 0 & t^{3/4} \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$$

and is classical if and only if $q = 2$. The associated flock arises by the geometrical construction of Fisher and Thas [8, Theorem 3.10]; in this case the corresponding translation plane was discovered by Walker [44] (using flocks) and independently by Betten [3]. The GQ was discovered by Kantor [14] and the herd comprises $q+1$ translation ovals, each projectively equivalent to $\{(1,t,t^{1/4}) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0)\}$.

The *Payne* q-clan [24], for $q = 2^e$ with e odd, is

$$\mathscr{C} = \left\{ \begin{pmatrix} t^{1/6} & t^{1/2} \\ 0 & t^{5/6} \end{pmatrix} : t \in \mathrm{GF}(q) \right\}.$$

It is classical if and only if $q = 2$, and FTWKB if and only if $q = 8$. The herd comprises two Segre–Bartocci ovals (equivalent to $\{(1,t,t^{1/6}) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0)\}$) and $q-1$ further ovals now known as Payne ovals. In this case there is (up to isomorphism) one associated GQ and translation plane, but two associated flocks, see [26].

The *Subiaco* q-clan [6], for $q = 2^e$, is

$$\mathscr{C} = \mathscr{C}_\delta = \left\{ \begin{pmatrix} f_0(t) & t^{1/2} \\ 0 & ag(t) \end{pmatrix} : t \in \mathrm{GF}(q) \right\},$$

where, for some $\delta \in \mathrm{GF}(q)$ with $\delta^2 + \delta + 1 \neq 0$ and $\mathrm{trace}(1/\delta) = 1$, we have

$$a = \frac{\delta^2 + \delta^5 + \delta^{1/2}}{\delta(1 + \delta + \delta^2)}$$

$$f_0(t) = \frac{\delta^2(t^4 + t) + \delta^2(1 + \delta + \delta^2)(t^3 + t^2)}{(t^2 + \delta t + 1)^2} + t^{1/2} \quad \text{and}$$

$$g(t) = \frac{\delta^4 t^4 + \delta^3(1 + \delta^2 + \delta^4)t^3 + \delta^3(1 + \delta^2)t}{(\delta^2 + \delta^5 + \delta^{1/2})(t^2 + \delta t + 1)^2} + \frac{\delta^{1/2}}{(\delta^2 + \delta^5 + \delta^{1/2})} t^{1/2}.$$

It is classical if and only if $q = 2$ and is FTWKB (or Payne) if and only if $q = 8$. There is (up to isomorphism) one associated flock and GQ, and if $e \equiv 2 \pmod 4$ then there are two associated ovals, otherwise only one. The flock in the case $q = 16$ is due to De Clerck and Herssens [7], and the associated herd comprises 17 Lunelli–Sce ovals. In the general case, the associated herd comprises $q + 1$ ovals which are now known as Subiaco ovals.

Finally, there are further examples for $q = 4^3, 4^4, 4^5, 4^6, 4^7$ and 4^8 discovered in the series of three papers [36, 37, 31]. The main result of this paper is the construction of an infinite family of q-clans which includes these examples. Our construction in fact gives a unified presentation of the classical, FTWKB, Subiaco and the new infinite family of q-clans.

3 The Adelaide q-clans

The purpose of this section is to prove our main theorem, Theorem 3.1. After the statement, we will proceed via a sequence of lemmas.

Theorem 3.1. *Let* $\mathrm{GF}(q^2)$ *be a quadratic extension of* $\mathrm{GF}(q)$ *with* $q = 2^e$. *Let* $\beta \in \mathrm{GF}(q^2)\backslash\{1\}$ *be such that* $\beta^{q+1} = 1$, *and let* $T(x) = x + x^q$ *for all* $x \in \mathrm{GF}(q^2)$. *Let* $a \in \mathrm{GF}(q)$ *and the functions* $f, g : \mathrm{GF}(q) \to \mathrm{GF}(q)$ *be defined by*:

$$a = \frac{T(\beta^m)}{T(\beta)} + \frac{1}{T(\beta^m)} + 1$$

$$f(t) = f_{m,\beta}(t) = \frac{T(\beta^m)(t+1)}{T(\beta)} + \frac{T((\beta t + \beta^q)^m)}{T(\beta)(t + T(\beta)t^{1/2} + 1)^{m-1}} + t^{1/2}$$

and

$$ag(t) = ag_{m,\beta}(t) = \frac{T(\beta^m)}{T(\beta)} t + \frac{T((\beta^2 t + 1)^m)}{T(\beta)T(\beta^m)(t + T(\beta)t^{1/2} + 1)^{m-1}} + \frac{1}{T(\beta^m)} t^{1/2}$$

and let

$$\mathscr{C} = \mathscr{C}_{m,\beta} = \left\{ \begin{pmatrix} f(t) & t^{1/2} \\ 0 & ag(t) \end{pmatrix} : t \in \mathrm{GF}(q) \right\}.$$

If $m \equiv \pm 1 \pmod{q+1}$ *then* $\mathscr{C}$ *is the classical* q*-clan for all* $q = 2^e$ *and for all* β. *If* $q = 2^e$ *with* e *odd and* $m \equiv \pm\frac{q}{2} \pmod{q+1}$ *then* $\mathscr{C}$ *is the FTWKB* q*-clan for all*

β. If $q = 2^e$ with $e > 2$ and $m \equiv \pm 5 \pmod{q+1}$ then $\mathscr{C}$ is the Subiaco q-clan for all β such that if λ is a primitive element of $\mathrm{GF}(q^2)$, so that $\beta = \lambda^{k(q-1)}$, then $q+1 \nmid km$. If $q = 2^e$ with $e > 2$ even and $m \equiv \pm \frac{q-1}{3} \pmod{q+1}$ then $\mathscr{C}$ is a q-clan, which we call the Adelaide q-clan, for all β.

First we introduce some notation which will be used throughout this section. Let $K = \mathrm{GF}(q^2)$ be an extension field of $F = \mathrm{GF}(q)$ with $q = 2^e$. We let the relative trace function from K to F be denoted by T, that is, $T : K \to F$ is defined by $T(x) = x + x^q$ and let the absolute trace function on F be denoted by trace_F.

Let $\beta \in K \backslash \{1\}$ be an element of norm 1 relative to F, that is, $\beta^{q+1} = 1$. We define three auxiliary functions $h_1, h_2, h_3 : F \to F$ by

$$h_1(t) = \frac{T((\beta t + \beta^q)^m)}{(t + T(\beta)t^{1/2} + 1)^{m-1}}$$

$$h_2(t) = \frac{T((\beta^2 t + 1)^m)}{(t + T(\beta)t^{1/2} + 1)^{m-1}} \quad \text{and}$$

$$h_3(t) = T(\beta^m)h_1(t) + h_2(t) = \frac{T((t + \beta^2)^m)}{(t + T(\beta)t^{1/2} + 1)^{m-1}}, \tag{3.1}$$

where $m \in \{1, \ldots, q^2 - 2\}$. Notice that $t + T(\beta)t^{1/2} + 1$ is non-zero for all $t \in F$. To see this, since the roots of $t + T(\beta)t^{1/2} + 1$ are β^2 and β^{2q}, it suffices to show that $\beta \notin F$. Let λ be a primitive element of K, so $\beta = \lambda^{k(q-1)}$ for some $k \in \{1, \ldots, q\}$. Then $\beta \in F$ if and only if $\beta^{q-1} = 1$, which is if and only if $q + 1 \mid k(q-1)^2$. But this is impossible since $(q+1, q-1) = 1$ and $k \in \{1, \ldots, q\}$.

Finally, we define $a \in \mathrm{GF}(q)$ and the functions $f, g : F \to F$ by:

$$a = \frac{T(\beta^m)}{T(\beta)} + \frac{1}{T(\beta^m)} + 1$$

$$f(t) = f_{m,\beta}(t) = \frac{T(\beta^m)}{T(\beta)}(t+1) + \frac{1}{T(\beta)}h_1(t) + t^{1/2}$$

and

$$ag(t) = ag_{m,\beta}(t) = \frac{T(\beta^m)}{T(\beta)}t + \frac{1}{T(\beta)T(\beta^m)}h_2(t) + \frac{1}{T(\beta^m)}t^{1/2}.$$

Lemma 3.2. *With the notation as above, and for all $t, s \in F$ with $t \neq s$ we have*

$$\mathrm{trace}_F\left(\frac{(f(t) + f(s))(ag(t) + ag(s))}{t + s}\right)$$
$$= \mathrm{trace}_F\left(1 + \frac{1}{T(\beta^m)} + \frac{T((M_t M_s^q)^m)}{T(M_t M_s^q)} + \frac{T(M_t^m)}{T(M_t)} + \frac{T(M_s^m)}{T(M_s)}\right),$$

where

$$M_t = \frac{t^{1/2} + \beta}{t^{1/2} + \beta^q}.$$

Proof. First, write

$$\frac{(f(t) + f(s))(ag(t) + ag(s))}{t + s} = \frac{1}{t + s} AB,$$

where

$$A = \frac{T(\beta^m)(t + s) + h_1(t) + h_1(s)}{T(\beta)} + (t + s)^{1/2} \quad \text{and}$$

$$B = \frac{T(\beta^m)(t + s) + \frac{1}{T(\beta^m)}(h_2(t) + h_2(s))}{T(\beta)} + \frac{1}{T(\beta^m)}(t + s)^{1/2}.$$

As we calculate the absolute trace of this expression we shall encounter terms of absolute trace 0 (with respect to F). Once such terms have been identified they will be accumulated in a single term denoted by C, thus C is not constant throughout the calculation, but at all times $\mathrm{trace}_F(C) = 0$. On expanding the product we obtain

$$\begin{aligned}
&\frac{T(\beta^m)^2}{T(\beta)^2}(t + s) + \frac{T(\beta^m)}{T(\beta)}(t + s)^{1/2} + \frac{h_2(t) + h_2(s)}{T(\beta)^2} + \frac{T(\beta^m)(h_1(t) + h_1(s))}{T(\beta)^2} \\
&\quad + \frac{(h_1(t) + h_1(s))(h_2(t) + h_2(s))}{T(\beta)^2 T(\beta^m)(t + s)} + \frac{h_1(t) + h_2(t) + h_1(s) + h_2(s)}{T(\beta)T(\beta^m)(t + s)^{1/2}} \\
&\quad + \frac{1}{T(\beta)}(t + s)^{1/2} + \frac{1}{T(\beta^m)}.
\end{aligned} \tag{3.2}$$

The sum of the first two terms is an element of absolute trace 0, and is thus incorporated into C. By (3.1) the sum of the third and fourth terms is $\frac{1}{T(\beta)^2}(h_3(t) + h_3(s))$. Now,

$$\begin{aligned}
h_1(t)h_2(t) &= \frac{T((\beta t + \beta^q)^m)}{(t + T(\beta)t^{1/2} + 1)^{m-1}} \cdot \frac{T((\beta^2 t + 1)^m)}{(t + T(\beta)t^{1/2} + 1)^{m-1}} \\
&= \frac{T(\beta^m)(t + T(\beta)t^{1/2} + 1)^{2m} + \beta^m(\beta^{2q}t + 1)^{2m} + \beta^{qm}(\beta^2 t + 1)^{2m}}{(t + T(\beta)t^{1/2} + 1)^{2m-2}} \\
&= T(\beta^m)(t^2 + T(\beta)^2 t + 1) + \frac{h_1^2(t) + h_2^2(t)}{T(\beta^m)}.
\end{aligned}$$

Hence, the fifth term of (3.2) can be written as:

$$\begin{aligned}\frac{(h_1(t)+h_1(s))(h_2(t)+h_2(s))}{T(\beta)^2T(\beta^m)(t+s)} &= \frac{\frac{h_1^2(t)+h_2^2(t)+h_1^2(s)+h_2^2(s)}{T(\beta^m)}}{T(\beta)^2T(\beta^m)(t+s)}\\ &\quad+\frac{T(\beta^m)((t+s)^2+T(\beta)^2(t+s))+h_1(t)h_2(s)+h_2(t)h_1(s)}{T(\beta)^2T(\beta^m)(t+s)}\\ &=\frac{h_1^2(t)+h_2^2(t)+h_1^2(s)+h_2^2(s)}{T(\beta)^2T(\beta^m)^2(t+s)}+\frac{t+s}{T(\beta)^2}+1+\frac{h_1(t)h_2(s)+h_2(t)h_1(s)}{T(\beta)^2T(\beta^m)(t+s)}.\end{aligned}$$

We see that the first term of this expression is the square of the sixth term in (3.2), and the second term here is the square of the seventh term in (3.2). Thus, there are two more expressions of absolute trace 0 that can be incorporated into C. Rewriting (3.2), we now obtain

$$1+\frac{1}{T(\beta^m)}+\frac{h_3(t)+h_3(s)}{T(\beta)^2}+\frac{h_1(t)h_2(s)+h_2(t)h_1(s)}{T(\beta)^2T(\beta^m)(t+s)}+C. \tag{3.3}$$

Let

$$M_t=\frac{t+\beta^2}{t+T(\beta)t^{1/2}+1}=\frac{(t^{1/2}+\beta)^2}{(t^{1/2}+\beta)(t^{1/2}+\beta^q)}=\frac{t^{1/2}+\beta}{t^{1/2}+\beta^q}.$$

It follows that

$$\begin{aligned}\frac{h_3(t)}{T(\beta)^2}&=\frac{T((t+\beta^2)^m)}{T(\beta)^2(t+T(\beta)t^{1/2}+1)^{m-1}}\\ &=\frac{(t+T(\beta)t^{1/2}+1)(M_t^m+M_t^{qm})}{T(\beta)^2}.\end{aligned}$$

Then, because

$$\begin{aligned}M_t+M_t^q&=\frac{t^{1/2}+\beta}{t^{1/2}+\beta^q}+\frac{t^{1/2}+\beta^q}{t^{1/2}+\beta}\\ &=\frac{t+\beta^2+t+\beta^{2q}}{t+T(\beta)t^{1/2}+1}=\frac{T(\beta)^2}{t+T(\beta)t^{1/2}+1},\end{aligned}$$

we have

$$\frac{h_3(t)}{T(\beta)^2}=\frac{T(M_t^m)}{T(M_t)}.$$

A simple calculation shows that:

$$\begin{aligned}
&h_1(t)h_2(s) + h_2(t)h_1(s)\\
&\quad= \frac{T(\beta^m)T(((t+\beta^2)(s+\beta^{2q}))^m + ((t+\beta^{2q})(s+\beta^2))^m)}{((t+T(\beta)t^{1/2}+1)^{m-1}(s+T(\beta)s^{1/2}+1))^{m-1}}\\
&\quad= T(\beta^m)(t+T(\beta)t^{1/2}+1)(s+T(\beta)s^{1/2}+1)T((M_tM_s^q)^m).
\end{aligned}$$

Then, because

$$\begin{aligned}
T(M_tM_s^q) &= \frac{(t^{1/2}+\beta)}{(t^{1/2}+\beta^q)}\frac{(s^{1/2}+\beta^q)}{(s^{1/2}+\beta)} + \frac{(t^{1/2}+\beta^q)}{(t^{1/2}+\beta)}\frac{(s^{1/2}+\beta)}{(s^{1/2}+\beta^q)}\\
&= \frac{(t+\beta^2)(s+\beta^{2q}) + (t+\beta^{2q})(s+\beta^q)}{(t+T(\beta)t^{1/2}+1)(s+T(\beta)s^{1/2}+1)}\\
&= \frac{T(\beta)^2(t+s)}{(t+T(\beta)t^{1/2}+1)(s+T(\beta)s^{1/2}+1)},
\end{aligned}$$

we have

$$\frac{h_1(t)h_2(s)+h_2(t)h_1(s)}{T(\beta)^2T(\beta^m)(t+s)} = \frac{T((M_tM_s^q)^m)}{T(M_tM_s^q)}.$$

We can now rewrite (3.3) as:

$$1 + \frac{1}{T(\beta^m)} + \frac{T((M_tM_s^q)^m)}{T(M_tM_s^q)} + \frac{T(M_t^m)}{T(M_t)} + \frac{T(M_s^m)}{T(M_s)} + C.$$

and applying the absolute trace function trace_F gives the desired result. □

Let $N_1 = \{\gamma \in K\backslash\{1\} \mid \gamma^{q+1} = 1\}$. Observe that for any $t \in F$ and $\beta \in N_1$ we have $M_t \in N_1$, and that for $t, s \in F$ and $\beta \in N_1$ we have $M_tM_s^q \in N_1$ provided $t \neq s$.

Lemma 3.3. *For $q = 2^e$, if there exists a constant $c \in \{0, 1\}$ such that*

$$\mathrm{trace}_F\left(\frac{T(\gamma^m)}{T(\gamma)}\right) = c, \quad \textit{for all } \gamma \in N_1,$$

then

$$\mathrm{trace}_F\left(\frac{(f(t)+f(s))(ag(t)+ag(s))}{t+s}\right) = \mathrm{trace}_F\left(\frac{1}{T(\beta^m)}\right)$$

$$\textit{holds}\begin{cases} \textit{for all } e, & \textit{if } c = \mathrm{trace}_F(1);\\ \textit{for all even } e, & \textit{if } c = 0;\\ \textit{for all odd } e, & \textit{if } c = 1.\end{cases}$$

Proof. This follows immediately from Lemma 3.2, the additivity of the trace function and the fact that $\mathrm{trace}_F(1) = 1$ if and only if e is odd. $\square$

Lemma 3.4. *Let λ be a primitive element of K so that $N_1 = \{\lambda^{k(q-1)} : k = 1, \dots, q\}$. Then*

$$\mathrm{trace}_F\left(\frac{1}{T(\beta^m)}\right) = 1 \tag{3.4}$$

for all $\beta = \lambda^{k(q-1)} \in N_1$ such that $q + 1 \nmid km$. In particular, if $(m, q + 1) = 1$ then (3.4) *holds for all $\beta \in N_1$.*

Proof. First note that $\mathrm{trace}_F(1/T(\beta^m)) = 1$ if and only if the quadratic $x^2 + T(\beta^m)x + 1$ is irreducible over F. But this quadratic has roots β^m and β^{qm}, so $\mathrm{trace}_F(1/T(\beta^m)) = 1$ if and only if $\beta^m \notin F$. Now $\beta^m = \lambda^{km(q-1)} \in N_1$ is an element of F if and only if $\lambda^{km(q-1)^2} = 1$. Hence if $\beta^m \in F$ then $(q+1) \mid km$, since $(q - 1, q + 1) = 1$. We have shown that if $\beta = \lambda^{k(q-1)}$ and $m \in \{1, \dots, q^2 - 2\}$ satisfy $q + 1 \nmid km$ then $\mathrm{trace}_F(1/T(\beta^m)) = 1$, as required. Noticing that if $(m, q + 1) = 1$ then $q + 1 \nmid km$ gives the last statement. $\square$

It is immediate from this lemma that, given K, one can always find a $\beta \in N_1$ such that (3.4) holds. Although we permit the exponent m to take any value in $\{1, \dots, q^2 - 2\}$, not all values of m give different functions f and g.

Lemma 3.5. *For the functions f and g defined above, we have*

$$f(t) = f_{m,\beta}(t) = f_{m+k(q+1),\beta}(t) \quad \text{and} \quad g(t) = g_{m,\beta}(t) = g_{m+k(q+1),\beta}(t),$$

for all integers k.

Proof. This follows immediately from the following calculations.

$$\begin{aligned} T(\beta^{m+k(q+1)}) &= \beta^{m+k(q+1)} + \beta^{qm+kq(q+1)} \\ &= \beta^m(\beta^{q+1})^k + \beta^{qm}(\beta^{q+1})^{kq} \\ &= \beta^m + \beta^{qm} = T(\beta^m), \end{aligned}$$

since $\beta^{q+1} = 1$.

$$\begin{aligned} T((\beta t + \beta^q)^{m+k(q+1)}) &= (\beta t + \beta^q)^{m+k(q+1)} + (\beta^q t + \beta)^{m+k(q+1)} \\ &= (\beta t + \beta^q)^m((\beta t + \beta^q)^{q+1})^k + (\beta^q t + \beta)^m((\beta^q t + \beta)^{q+1})^k \\ &= (\beta t + \beta^q)^m((\beta t + \beta^q)(\beta^q t + \beta))^k + (\beta^q t + \beta)^m((\beta t + \beta^q)(\beta^q t + \beta))^k \\ &= (t^2 + T(\beta)^2 t + 1)^k((\beta t + \beta^q)^m + (\beta^q t + \beta)^m) \\ &= (t + T(\beta)t^{1/2} + 1)^{2k} T((\beta t + \beta^q)^m). \end{aligned}$$

Hence,

$$\begin{aligned}
h_{1,m+k(q+1),\beta}(t) &= \frac{T((\beta t+\beta^q)^{m+k(q+1)})}{(t+T(\beta)t^{1/2}+1)^{m+k(q+1)-1}} \\
&= \frac{(t+T(\beta)t^{1/2}+1)^{2k}T((\beta t+\beta^q)^m)}{(t+T(\beta)t^{1/2}+1)^{m+k(q+1)-1}} \\
&= \frac{T((\beta t+\beta^q)^m)}{(t+T(\beta)t^{1/2}+1)^{m+k(q-1)-1}} \\
&= \frac{T((\beta t+\beta^q)^m)}{(t+T(\beta)t^{1/2}+1)^{m-1}} = h_{1,m,\beta}(t).
\end{aligned}$$

The last simplification is due to the fact that $(t+T(\beta)t^{1/2}+1)^{q-1}=1$ since $t+T(\beta)t^{1/2}+1 \in F\backslash\{0\}$. A very similar computation shows that

$$h_2(t) = h_{2,m,\beta}(t) = h_{2,m+k(q+1),\beta}(t). \qquad \square$$

It is now clear that we may restrict m to lie in $\{1,\dots,q+1\}$. However, there is a further equivalence which shows that at most half of these values lead to distinct functions.

Lemma 3.6. *For the functions f and g defined above, we have*

$$f(t) = f_{m,\beta}(t) = f_{-m,\beta}(t) \quad \textit{and} \quad g(t) = g_{m,\beta}(t) = g_{-m,\beta}(t).$$

Proof. First, observe that

$$T(\beta^{-m}) = \left(\frac{1}{\beta}\right)^m + \left(\frac{1}{\beta^q}\right)^m = \beta^{qm} + \beta^m = T(\beta^m).$$

Now,

$$\begin{aligned}
T((\beta t+\beta^q)^{-m}) &= \frac{1}{(\beta t+\beta^q)^m} + \frac{1}{(\beta^q t+\beta)^m} \\
&= \frac{(\beta^q t+\beta)^m + (\beta t+\beta^q)^m}{(\beta t+\beta^q)^m(\beta^q t+\beta)^m} = \frac{T((\beta t+\beta^q)^m)}{(t+T(\beta)t^{1/2}+1)^{2m}}.
\end{aligned}$$

Thus, we have

$$h_{1,-m,\beta}(t) = \frac{T((\beta t+\beta^q)^{-m})}{(t+T(\beta)t^{1/2}+1)^{-m-1}} = \frac{T((\beta t+\beta^q)^m)}{(t+T(\beta)t^{1/2}+1)^{2m-m-1}} = h_{1,m,\beta}(t).$$

A similar calculation shows that $h_{2,-m,\beta}(t) = h_{2,m,\beta}(t)$. $\square$

We are now in a position to be able to prove our main result.

Proof of Theorem 3.1. It is straightforward to verify that $f(0) = g(0) = 0$ and $f(1) = g(1) = 1$. As outlined in Section 2, and in the notation of the statement of Theorem 3.1, $\mathscr{C}$ is a q-clan if and only if

$$\mathrm{trace}_F\left(\frac{(f(s)+f(t))(ag(s)+ag(t))}{s+t}\right) = 1 \tag{3.5}$$

for all $s, t \in \mathrm{GF}(q)$ with $s \neq t$. (For, if (3.5) holds, then putting $s = 0$ and $t = 1$ shows that $\mathrm{trace}_F(a) = 1$.) By Lemmas 3.2 to 3.6 we need to consider $\mathrm{trace}_F((T(\gamma^m)/T(\gamma))$ for $\gamma \in N_1$ and for each $m = 1$, $q/2$, 5 and $(q-1)/3$.

If $m = 1$ then, for $\gamma \in N_1$, we have $\mathrm{trace}_F((T(\gamma^m)/T(\gamma)) = \mathrm{trace}_F(1)$. By Lemmas 3.3 and 3.4, Equation (3.5) is satisfied for all e and for all $\beta \in N_1$. In this case $f(t) = t^{1/2}$ and the q-clan is classical by [19].

If $m = q/2$ then, for $\gamma \in N_1$, we have $\mathrm{trace}_F((T(\gamma^m)/T(\gamma)) = \mathrm{trace}_F(1/T(\gamma)) = 1$ by Lemma 3.4. By Lemmas 3.3 and 3.4, Equation (3.5) is satisfied for all odd e and for all $\beta \in N_1$. In this case $f(t) = t^{3/4} + t^{1/2} + t^{1/4}$ and the q-clan is FTWKB by [19].

If $m = 5$ then, for $\gamma \in N_1$, we have $\mathrm{trace}_F((T(\gamma^m)/T(\gamma)) = \mathrm{trace}_F((\gamma+\gamma^q)^4 + (\gamma+\gamma^q)^2 + 1) = \mathrm{trace}_F(1)$. By Lemmas 3.3 and 3.4, then Equation (3.5) is satisfied for all e and for all $\beta \in N_1$ if $(5, q+1) = 1$. On the other hand if $(5, q+1) \neq 1$, that is e is even, then Equation (3.5) holds for only some $\beta \in N_1$. Let $\beta \in N_1$ be such that $\mathrm{trace}_F(1/T(\beta^5)) = 1$ and let $d = T(\beta)^2$; so that $T(\beta^5) = d^{1/2}(d^2+d+1)$. It follows that $d^2+d+1 \neq 0$, Equation (3.5) holds, and $\mathrm{trace}_F(1/d) = 1$ by Lemma (3.4) since $(2, q+1) = 1$. Now,

$$\begin{aligned} T((\beta t+\beta^q)^5) &= (\beta t+\beta^q)(\beta^4 t^4+\beta^{4q}) + (\beta^q t+\beta)(\beta^{4q}t^4+\beta^4) \\ &= (\beta^5+\beta^{5q})(t^5+1) + (\beta^3+\beta^{3q})(t^4+t) \\ &= d^{1/2}(d^2+d+1)(t^5+1) + d^{1/2}(d+1)(t^4+t). \end{aligned}$$

Writing $A = d^2+d+1$ gives

$$\begin{aligned} f(t) &= \frac{d^{1/2}A(t+1)}{d^{1/2}} + \frac{d^{1/2}A(t^5+1) + d^{1/2}(d+1)(t^4+t)}{d^{1/2}(t^2+dt+1)^2} + t^{1/2} \\ &= \frac{A(t+1)(t^4+d^2t^2+1) + A(t^5+1) + (d+1)(t^4+t)}{(t^2+dt+1)^2} + t^{1/2} \\ &= \frac{d^2(t^4+t) + d^2(d^2+d+1)(t^3+t^2)}{(t^2+dt+1)^2} + t^{1/2}. \end{aligned}$$

A similar calculation shows that

$$a = \frac{d^2 + d^5 + d^{1/2}}{d(d^2 + d + 1)} \quad \text{and}$$

$$g(t) = \frac{d^4t^4 + d^3(d^4 + d^2 + 1)t^3 + d^3(d^2 + 1)t}{(d^2 + d^5 + d^{1/2})(t^2 + dt + 1)^2} + \frac{d^{1/2}}{d^2 + d^5 + d^{1/2}} t^{1/2}.$$

By [6, Theorem 5], $\mathscr{C}$ is the Subiaco q-clan.

Finally, let e be even, so $3 \mid q - 1$, and let $m = \frac{q-1}{3}$. Let $v^3 = \gamma \in N_1$ and notice that $v \in N_1$ since $(3, q + 1) = 1$. Now,

$$\begin{aligned}
\frac{T(\gamma^{(q-1)/3})}{T(\gamma)} &= \frac{\gamma^{(q-1)/3} + \gamma^{q(q-1)/3}}{\gamma + \gamma^q} = \frac{v^{q-1} + v^{q(q-1)}}{v^3 + v^{3q}} \\
&= \frac{\frac{1}{v^2} + v^2}{v^3 + \frac{1}{v^3}} = \frac{\left(v + \frac{1}{v}\right)^2}{\left(v + \frac{1}{v}\right)\left(v^2 + \frac{1}{v^2} + 1\right)} \\
&= \frac{v + \frac{1}{v}}{v^2 + \frac{1}{v^2} + 1} = \frac{1}{v + \frac{1}{v} + 1} + \frac{1}{\left(v + \frac{1}{v} + 1\right)^2}.
\end{aligned}$$

Thus,

$$\operatorname{trace}_F\left(\frac{T(\gamma^{(q-1)/3})}{T(\gamma)}\right) = 0 \quad \text{for all } \gamma \in N_1.$$

By Lemmas 3.3 and 3.4, since $\left(\frac{q-1}{3}, q + 1\right) = 1$, $\mathscr{C}$ is a q-clan for all $\beta \in N_1$. $\square$

4 Automorphism groups of the Adelaide geometries

In this section we calculate the automorphism groups of the Adelaide geometries, starting with the Adelaide herd. First we recall some notation and definitions from [20].

Let $\mathscr{F}$ denote the collection of all functions $f : \mathrm{GF}(q) \to \mathrm{GF}(q)$ such that $f(0) = 0$. Note that each element of $\mathscr{F}$ can be expressed as a polynomial in one variable of degree at most $q - 1$ and that $\mathscr{F}$ is a vector space over $\mathrm{GF}(q)$. If $f(x) = \sum a_i x^i \in \mathscr{F}$ and $\gamma \in \operatorname{Aut} \mathrm{GF}(q)$ then we write $f^\gamma(x) = \sum a_i^\gamma x^i$ or, equivalently, $f^\gamma(x) = (f(x^{1/\gamma}))^\gamma$. We will be concerned with the group $\mathrm{P\Gamma L}(2, q)$ acting on the projective line $\mathrm{PG}(1, q)$, that is,

$$\mathrm{P\Gamma L}(2, q) = \{x \mapsto Ax^\gamma : A \in \mathrm{GL}(2, q), \gamma \in \operatorname{Aut} \mathrm{GF}(q)\}.$$

Lemma 4.1 ([20]). *For each $f \in \mathscr{F}$ and $\psi \in \mathrm{P\Gamma L}(2, q)$, where $\psi : x \mapsto Ax^\gamma$ for $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, q)$ and $\gamma \in \operatorname{Aut} \mathrm{GF}(q)$, let the image of f under ψ be the function $\psi f : \mathrm{GF}(q) \to \mathrm{GF}(q)$ 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 $\mathrm{P\Gamma L}(2,q)$ *on* $\mathscr{F}$, *which we will call the* magic action.

By the transitivity of $\mathrm{P\Gamma L}(3,q)$ on ordered quadrangles in $\mathrm{PG}(2,q)$, 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

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

where f is a (permutation) polynomial of degree at most $q-2$ satisfying $f(0)=0, f(1)=1$ and such that for each $s \in \mathrm{GF}(q)$ the function f_s where $f_s(0)=0$ and $f_s(x) = (f(x+s)+f(s))/x$, $x \neq 0$ is a permutation (see [11], but note that this and other references use the $\mathscr{D}$ notation to represent a hyperoval). Conversely, any polynomial f satisfying the above conditions gives rise to an oval $\mathscr{D}(f)$ with nucleus $(0,0,1)$. Such a polynomial is called an *o-polynomial for* $\mathrm{PG}(2,q)$.

Let $\mathscr{H}(\mathscr{C}_1) = \{\mathscr{D}(f_s) : s \in \mathrm{GF}(q) \cup \{\infty\}\}$ and $\mathscr{H}(\mathscr{C}') = \{\mathscr{D}(f_t') : t \in \mathrm{GF}(q) \cup \{\infty\}\}$ be herds. We say that $\mathscr{H}(\mathscr{C})$ and $\mathscr{H}(\mathscr{C}')$ are *isomorphic* if there exists $\psi \in \mathrm{P\Gamma L}(2,q)$ such that for all $s \in \mathrm{GF}(q) \cup \{\infty\}$ we have $\psi f_s \in \langle f_t' \rangle$ under the magic action, and where the induced map $s \mapsto t$ is a permutation of $\mathrm{GF}(q) \cup \{\infty\}$. (Where, for $f \in \mathscr{F}$, we use $\langle f \rangle$ to denote the 1-dimensional subspace of $\mathscr{F}$ containing f.) An *automorphism* of a herd $\mathscr{H}(\mathscr{C})$ is an isomorphism from $\mathscr{H}(\mathscr{C})$ to itself and the *automorphism group* $\mathrm{Aut}\,\mathscr{H}(\mathscr{C})$ of $\mathscr{H}(\mathscr{C})$ is the group of all automorphisms of $\mathscr{H}(\mathscr{C})$. In other words, the automorphism group of a herd $\mathscr{H}(\mathscr{C}) = \{\mathscr{D}(f_s) : s \in \mathrm{GF}(q) \cup \{\infty\}\}$ is the stabiliser of $\{\langle f_s \rangle : s \in \mathrm{GF}(q) \cup \{\infty\}\}$ in $\mathrm{P\Gamma L}(2,q)$, under the magic action.

We recall the following theorem:

Theorem 4.2 ([20]). *Let* $q = p^e$. *The automorphism group of a classical herd and of an FTWKB herd is* $\mathrm{P\Gamma L}(2,q)$. *The automorphism group of a Payne herd for* $q \geqslant 32$ *is* $D_{2(q-1)} \rtimes C_e$. *The automorphism group of a Subiaco herd for* $q \geqslant 16$ *is* $C_{q+1} \rtimes C_{2e}$.

The main result of this section is:

Theorem 4.3. *The automorphism group of an Adelaide herd for* $q = 2^e$ *with* $e \geqslant 6$ *even and* β *of order* $q+1$ *is* $C_{q+1} \rtimes C_{2e}$ *of order* $2e(q+1)$.

Proof. The structure of the proof is similar to that of the last part of the proof of Theorem 4.2 in [20]. Let $q = 2^e$ where $e \geqslant 6$ and let $\mathscr{H}(\mathscr{C}) = \{\mathscr{D}(f_s) : s \in \mathrm{GF}(q) \cup \{\infty\}\}$ be the Adelaide herd, defined as in Section 2.3 with $f_0 = f, f_\infty = g$ and a as in Theorem 3.1. Let $\psi_1 \in \mathrm{PGL}(2,q)$ be $\psi_1 : x \mapsto Ax$ where $A = \begin{pmatrix} \mathrm{T}(\beta)^2 & 1 \\ 1 & 0 \end{pmatrix}$. Then

$$\begin{aligned}\psi_1 f(t) &= tf\left(\frac{\mathrm{T}(\beta)^2 t+1}{t}\right) + tf(\mathrm{T}(\beta)^2) \\ &= f(t) + \mathrm{T}(\beta^m)^2 ag(t) + \mathrm{T}(\beta^m)t^{1/2} \in \langle f_{\mathrm{T}(\beta^m)^2}(t)\rangle.\end{aligned}$$

Similarly,

$$\begin{aligned}\psi_1 ag(t) &= f(t) + (\mathrm{T}(\beta^m)^2+1)ag(t) + (\mathrm{T}(\beta^m)+1)t^{1/2} \\ &= f(t) + (\mathrm{T}(\beta^m)^2+1)ag(t) + (\mathrm{T}(\beta^m)+1)t^{1/2} \in \langle f_{(\mathrm{T}(\beta^m)^2+1)}(t)\rangle\end{aligned}$$

and $\psi_1 f_1(t) = (\psi_1 f(t) + \psi_1 ag(t) + t^{1/2})/a = g(t)$. Finally, for $s \in \mathrm{GF}(q)\backslash\{0,1\}$, we have

$$\begin{aligned}\psi_1 f_s(t) &= \frac{\psi_1 f(t) + s\psi_1 ag(t) + s^{1/2}t^{1/2}}{1+as+s^{1/2}} \\ &= \frac{1+s}{1+as+s^{1/2}}\left(f(t) + \left(\mathrm{T}(\beta^m)^2 + \frac{s}{1+s}\right)ag(t) + \left(\mathrm{T}(\beta^m) + \frac{s^{1/2}}{1+s^{1/2}}\right)t^{1/2}\right)\end{aligned}$$

which is in $\langle f_u(t)\rangle$ where $u = \mathrm{T}(\beta^m)^2 + s/(s+1)$.

Consider the characteristic polynomial $x^2 + T(\beta)^2 x + 1$ of A over $\mathrm{GF}(q)$. Since the roots in $\mathrm{GF}(q^2)$ are β^2 and β^{2q}, and A is a root, it follows that the order of A is the order of β^2 in $\mathrm{GF}(q^2)$, which is the order of β in $\mathrm{GF}(q^2)$, and is $q+1$ by hypothesis.

Now let $\psi_2 \in \mathrm{P\Gamma L}(2,q)$ be $\psi_2 : x \mapsto Ax^2$ where $A = \begin{pmatrix} 1 & 0 \\ \mathrm{T}(\beta)^{-2} & \mathrm{T}(\beta)^{-2}\end{pmatrix}$. Then

$$\psi_2 f(t) = \frac{1}{\mathrm{T}(\beta)}(f(\mathrm{T}(\beta)t^{1/2}+1))^2 + \frac{1}{\mathrm{T}(\beta)} = \mathrm{T}(\beta^m)ag(t) \in \langle g(t)\rangle$$

and

$$\begin{aligned}\psi_2 ag(t) &= \frac{1}{\mathrm{T}(\beta)}(ag(\mathrm{T}(\beta)t^{1/2}+1))^2 + \frac{a^2}{\mathrm{T}(\beta)} \\ &= \frac{f(t) + (\mathrm{T}(\beta^m)^2+1)ag(t) + (\mathrm{T}(\beta^m)+1)t^{1/2}}{\mathrm{T}(\beta^m)} \\ &= \frac{a(\mathrm{T}(\beta^m)^2+1) + \mathrm{T}(\beta^m))}{\mathrm{T}(\beta^m)} f_{\mathrm{T}(\beta^m)^2+1}(t) \in \langle f_{\mathrm{T}(\beta^m)^2+1}(t)\rangle.\end{aligned}$$

Finally, for $s \in \mathrm{GF}(q)\backslash\{0\}$, we have

$$\begin{aligned}
\psi_2 f_s(t) &= \frac{1}{(1+as+s^{1/2})^2}(\psi_2 f(t) + s^2\psi_2 ag(t) + st^{1/2}) \\
&= \left(\frac{s^2}{\mathrm{T}(\beta^m)} f(t) + \left(\mathrm{T}(\beta^m) + \frac{s^2(\mathrm{T}(\beta^m)^2+1)}{\mathrm{T}(\beta^m)}\right) ag(t)\right. \\
&\qquad \left. + \left(\frac{s^2(\mathrm{T}(\beta^m)+1)}{\mathrm{T}(\beta^m)} + s\right) t^{1/2}\right) \Big/ (1+as+s^{1/2})^2
\end{aligned}$$

which is in $\langle f_u(t)\rangle$ for $u = \mathrm{T}(\beta^m)^2 + 1 + \mathrm{T}(\beta^m)^2/s^2$.

Thus the element $\psi_2 \in \operatorname{Aut}\mathscr{H}(\mathscr{C})$, and has order $2e$ (see [20]). Now ψ_2 normalises $\langle\psi_1\rangle$ and $\langle\psi_1\rangle \cap \langle\psi_2\rangle$ is the identity, and we have therefore shown that the Adelaide herd admits $C_{q+1} \rtimes C_{2e}$ as automorphism group. It is straightforward to verify that the map $x \mapsto Ax$, where $A = \begin{pmatrix} \mathrm{T}(\beta)^{-2} & 0 \\ 0 & 1 \end{pmatrix}$ does not fix $\mathscr{H}(\mathscr{C})$, and the result follows by the maximality of $C_{q+1} \rtimes C_{2e}$ in $\mathrm{P\Gamma L}(2,q)$. □

We note that, with the exception of those in the last sentence, all the calculations in the proof of Theorem 4.3 are independent of the value of m. This proof is therefore a unified treatment of the groups of the Subiaco and Adelaide herds.

Corollary 4.4. *Let $q = 2^e$ where $e \geqslant 6$ is even and let $\beta \in \mathrm{GF}(q^2)$ be of order $q+1$. The automorphism group of the Adelaide generalized quadrangle over $\mathrm{GF}(q)$ arising from this β is the semidirect product of $\mathscr{G}$ (in the notation of Section 2.2) with the semidirect product of a cyclic group of order q^2-1 and a cyclic group of order $2e$. Since $|\mathscr{G}| = q^5$, this group has order $2q^5(q-1)(q-1)e$.*

Proof. See Corollary 4.1 of [20]. □

Corollary 4.5. *Let $q = 2^e$ where $e \geqslant 6$ is even and let $\beta \in \mathrm{GF}(q^2)$ be of order $q+1$. The automorphism group of the Adelaide generalized quadrangle over $\mathrm{GF}(q)$ arising from this β is transitive on the lines through (∞). Hence there is, up to isomorphism, one associated flock and one associated translation plane.*

Corollary 4.6. *Let $q = 2^e$ where $e \geqslant 6$ is even and let $\beta \in \mathrm{GF}(q^2)$ be of order $q+1$. The automorphism group of the Adelaide herd over $\mathrm{GF}(q)$ arising from this β is transitive on the ovals of the herd. Hence an Adelaide oval in $\mathrm{PG}(2,q)$ is stabilised by a cyclic group of order $2e$.*

Let $q = 2^e$ where $e \geqslant 6$ is even and let $\beta \in \mathrm{GF}(q^2)$ be of order $q+1$. Suppose that $e/2$ is odd. Then the Adelaide generalized quadrangle is new, as follows. By comparing the orders of the respective automorphism groups, it is immediate that if the Adelaide generalized quadrangle is not new then it is a Subiaco generalized quadrangle. The automorphism group of the Subiaco generalized quadrangle for this q is also transitive on the lines through (∞) (see [30]), however, in this case the automorphism group of the Subiaco generalized quadrangle is not transitive on the ovals of the herd (see [22]) and this suffices to show that the groups are different. We remark that since in $\mathrm{PG}(2,4^4)$ the Adelaide oval is known not to be a Subiaco oval [37], the Adelaide generalized quadrangle in $\mathrm{PG}(2,4^4)$ is new.

In a sequel to this paper, we will show that for $m \not\equiv \pm 1 \pmod{q+1}$, $\mathscr{H}(\mathscr{C}_{m,\beta})$ is isomorphic to $\mathscr{H}(\mathscr{C}_{m',\beta})$ if and only if $m \equiv \pm m' \pmod{q+1}$ and hence the Adelaide generalized quadrangles are new, for $e \geqslant 6$ even. It is then immediate that the Adelaide flocks and Adelaide planes are also new.

Let $q = 2^e$ where $e \geqslant 6$ is even and let $\beta \in \mathrm{GF}(q^2)$ be of order $q+1$. We remark that in $\mathrm{PG}(2,q)$ an Adelaide oval over $\mathrm{GF}(q)$ arising from this β is either new or is a Subiaco oval, as follows. First, every previously known hyperoval in $\mathrm{PG}(2,q)$ where $q \geqslant 6$ is even is either a translation hyperoval or a Subiaco hyperoval. The main theorem of [19] shows that an Adelaide oval is not a translation hyperoval, for otherwise an Adelaide herd would be either classical or an FTWKB herd; contrary to the calculation of the respective groups. Since a non-translation oval contained in a translation hyperoval has a group of order $(q-1)e$, its homography group has odd order $q-1$. Since an Adelaide oval has an induced homography group of order 2, these two ovals are different.

5 Open problems

There are several open questions and problems arising immediately from this work, as follows.

1. Is the group described in Corollary 4.6 the full stabiliser of an Adelaide oval? The answer is known to be in the affirmative for $e = 6$ and 8 [37].
2. Are the Adelaide ovals new for all q, that is, do not belong to any previously known family? The answer is known to be in the affirmative for $e = 6$ and 8 [37].
3. For a given $q = 2^e$ with $e \geqslant 6$ even, are all Adelaide generalized quadrangles isomorphic (that is, those for different β)?
4. Do the Adelaide class of geometries and the regular cyclic class of geometries discovered by Penttila [34] form a single family?
5. Classify cyclic generalized quadrangles in characteristic 2, that is, classify herds which are stabilised by a cyclic group of order $q+1$. The known examples are the classical, FTWKB, Subiaco and Adelaide generalized quadrangles.

References

[1] L. Bader, G. Lunardon, S. E. Payne, On q-clan geometry, $q = 2^e$. *Bull. Belg. Math. Soc. Simon Stevin* **1** (1994), 301–328. MR 97b:51004 Zbl 0803.51006

[2] L. Bader, G. Lunardon, J. A. Thas, Derivation of flocks of quadratic cones. *Forum Math.* **2** (1990), 163–174. MR 91k:51012 Zbl 0692.51006

[3] D. Betten, 4-dimensionale Translationsebenen mit 8-dimensionaler Kollineationsgruppe. *Geometriae Dedicata* **2** (1973), 327–339. MR 49 #3652 Zbl 0272.50028

[4] W. Cherowitzo, Hyperovals in Desarguesian planes of even order. In: *Combinatorics '86 (Trento, 1986)*, 87–94, North-Holland 1988. MR 89c:51011 Zbl 0651.51009

[5] W. Cherowitzo, α-flocks and hyperovals. *Geom. Dedicata* **72** (1998), 221–246. MR 99m:51011 Zbl 0930.51007

[6] W. Cherowitzo, T. Penttila, I. Pinneri, G. F. Royle, Flocks and ovals. *Geom. Dedicata* **60** (1996), 17–37. MR 97c:51006 Zbl 0855.51008

[7] F. De Clerck, C. Herssens, Flocks of the quadratic cone in $\mathrm{PG}(3,q)$ for q small. The CaGe Reports **8** (1992), Computer Algebra Group, The University of Ghent, Belgium.

[8] J. C. Fisher, J. A. Thas, Flocks in $\mathrm{PG}(3,q)$. *Math. Z.* **169** (1979), 1–11. MR 81a:05023 Zbl 0406.51004

[9] M. J. Ganley, On likeable translation planes of even order. *Arch. Math. (Basel)* **41** (1983), 478–480. MR 85f:51011a Zbl 0534.51005

[10] J. W. P. Hirschfeld, *Finite projective spaces of three dimensions*. Oxford Univ. Press 1985. MR 87j:51013 Zbl 0574.51001

[11] J. W. P. Hirschfeld, *Projective geometries over finite fields*. Oxford Univ. Press 1998. MR 99b:51006 Zbl 0899.51002

[12] J. W. P. Hirschfeld, J. A. Thas, *General Galois geometries*. Oxford Univ. Press 1991. MR 96m:51007 Zbl 0789.51001

[13] N. L. Johnson, Semifield flocks of quadratic cones. *Simon Stevin* **61** (1987), 313–326. MR 89g:51009 Zbl 0645.51005

[14] W. M. Kantor, Generalized quadrangles associated with $G_2(q)$. *J. Combin. Theory Ser. A* **29** (1980), 212–219. MR 82b:51007 Zbl 0465.51007

[15] W. M. Kantor, Some generalized quadrangles with parameters q^2, q. *Math. Z.* **192** (1986), 45–50. MR 87f:51016 Zbl 0592.51003

[16] N. Knarr, A geometric construction of generalized quadrangles from polar spaces of rank three. *Results Math.* **21** (1992), 332–344. MR 93b:51009 Zbl 0765.51006

[17] M. Law, T. Penttila, BLT-sets over small fields II. Preprint 2000.

[18] M. Law, T. Penttila, Some flocks in characteristic 3. *J. Combin. Theory Ser. A* **94** (2001), 387–392. MR 2002i:51005 Zbl 01618730

[19] C. M. O'Keefe, T. Penttila, Characterisations of flock quadrangles. *Geom. Dedicata* **82** (2000), 171–191. MR 2001h:51009 Zbl 0969.51007

[20] C. M. O'Keefe, T. Penttila, Automorphism groups of generalized quadrangles via an unusual action of $\mathrm{P\Gamma L}(2,2^h)$. *European J. Combin.* **23** (2002), 213–232. MR 1 881 553 Zbl pre01740611

[21] C. M. O'Keefe, J. A. Thas, Collineations of Subiaco and Cherowitzo hyperovals. *Bull. Belg. Math. Soc. Simon Stevin* **3** (1996), 177–192. MR 97d:51011 Zbl 0854.51006

[22] S. E. Payne, The Subiaco notebook: An introduction to q-clan geometry. Unpublished notes. The .ps file is available on S. E. Payne's homepage http://www-math.cudenver.edu/~spayne.

[23] S. E. Payne, Generalized quadrangles as group coset geometries. In: *Proceedings of the Eleventh Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1980), Vol. II*, volume 29, 717–734. MR 83h:51024 Zbl 0453.05015

[24] S. E. Payne, A new infinite family of generalized quadrangles. In: *Proceedings of the sixteenth Southeastern international conference on combinatorics, graph theory and computing (Boca Raton, Fla., 1985)*, volume 49, 115–128. MR 88h:51010 Zbl 0632.51011

[25] S. E. Payne, An essay on skew translation generalized quadrangles. *Geom. Dedicata* **32** (1989), 93–118. MR 91f:51010 Zbl 0706.51006

[26] S. E. Payne, Collineations of the generalized quadrangles associated with q-clans. In: *Combinatorics '90 (Gaeta, 1990)*, 449–461, North-Holland 1992. MR 94e:51010 Zbl 0767.51003

[27] S. E. Payne, Collineations of the Subiaco generalized quadrangles. *Bull. Belg. Math. Soc. Simon Stevin* **1** (1994), 427–438. MR 95k:51013 Zbl 0803.51007
[28] S. E. Payne, A tensor product action on q-clan generalized quadrangles with $q = 2^e$. *Linear Algebra Appl.* **226/228** (1995), 115–137. MR 96g:51014 Zbl 0841.51003
[29] S. E. Payne, The fundamental theorem of q-clan geometry. *Des. Codes Cryptogr.* **8** (1996), 181–202. MR 97f:51013 Zbl 0874.51001
[30] S. E. Payne, T. Penttila, I. Pinneri, Isomorphisms between Subiaco q-clan geometries. *Bull. Belg. Math. Soc. Simon Stevin* **2** (1995), 197–222. MR 96g:51013 Zbl 0842.51004
[31] S. E. Payne, T. Penttila, G. F. Royle, Building a cyclic q-clan. In: *Mostly finite geometries (Iowa City, IA, 1996)*, 365–378, Dekker 1997. MR 98j:51010 Zbl 0887.51003
[32] S. E. Payne, L. A. Rogers, Local group actions on generalized quadrangles. *Simon Stevin* **64** (1990), 249–284. MR 93a:51002 Zbl 0735.51007
[33] S. E. Payne, J. A. Thas, *Finite generalized quadrangles*. Pitman 1984. MR 86a:51029 Zbl 0551.05027
[34] T. Penttila, Regular cyclic BLT-sets. *Rend. Circ. Mat. Palermo (2) Suppl.* no. **53** (1998), 167–172. MR 99i:51008 Zbl 0911.51005
[35] T. Penttila, I. Pinneri, Hyperovals. *Australas. J. Combin.* **19** (1999), 101–114. MR 2001d:51010 Zbl 0939.51018
[36] T. Penttila, G. F. Royle, Classification of hyperovals in $PG(2, 32)$. *J. Geom.* **50** (1994), 151–158. MR 95f:51005 Zbl 0805.51005
[37] T. Penttila, G. F. Royle, On hyperovals in small projective planes. *J. Geom.* **54** (1995), 91–104. MR 96j:51013 Zbl 0840.51003
[38] T. Penttila, G. F. Royle, BLT-sets over small fields. *Australas. J. Combin.* **17** (1998), 295–307. MR 99g:05043 Zbl 0911.51004
[39] T. Penttila, L. Storme, Monomial flocks and herds containing a monomial oval. *J. Combin. Theory Ser. A* **83** (1998), 21–41. MR 99e:51008 Zbl 0923.51004
[40] J. A. Thas, Generalized quadrangles and flocks of cones. *European J. Combin.* **8** (1987), 441–452. MR 89d:51016 Zbl 0646.51019
[41] J. A. Thas, Generalized quadrangles of order (s, s^2). I. *J. Combin. Theory Ser. A* **67** (1994), 140–160. MR 95h:51009 Zbl 0808.51010
[42] J. A. Thas, Generalized quadrangles of order (s, s^2). II. *J. Combin. Theory Ser. A* **79** (1997), 223–254. MR 99e:51004 Zbl 0887.51004
[43] J. A. Thas, Generalized quadrangles of order (s, s^2). III. *J. Combin. Theory Ser. A* **87** (1999), 247–272. MR 2000g:51005 Zbl 0949.51003
[44] M. Walker, A class of translation planes. *Geometriae Dedicata* **5** (1976), 135–146. MR 54 #8442 Zbl 0356.50022

Received 4 June, 2001; revised 16 November, 2001

W. E. Cherowitzo, Department of Mathematics, University of Colorado at Denver, Campus Box 170, P.O. Box 173364, Denver, CO 80217-3364, USA
Email: wcherowi@carbon.cudenver.edu

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

T. Penttila, Department of Mathematics and Statistics, The University of Western Australia, 6907 Australia
Email: penttila@maths.uwa.edu.au