Isomorphisms Between Subiaco q–Clan Geometries

S. E. Payne* Tim Penttila Ivano Pinneri†

Abstract

For $q = 2^e$, $e \geq 4$, the Subiaco construction introduced in [2] provides one q–clan, one flock, and for $e \not\equiv 2 \pmod 4$, one oval in $PG(2, q)$. When $e \equiv 2 \pmod 4$, there are two inequivalent ovals. The associated generalised quadrangle of order (q^2, q) has a complete automorphism group $\mathcal{G}$ of order $2e(q^2 - 1)q^5$. For each Subiaco oval $\mathcal{O}$ there is a group of collineations of $PG(2, q)$ induced by a subgroup of $\mathcal{G}$ and stabilising $\mathcal{O}$. When $e \equiv 2 \pmod 4$, for both ovals the complete stabiliser is just that induced by a subgroup of $\mathcal{G}$.

1 Introduction

In [2] a new family of Subiaco q–clans, $q = 2^e$, were introduced. Associated with a q–clan $\mathbf{C}$ is a generalised quadrangle $GQ(\mathbf{C})$ of order (q^2, q), subquadrangles of order q and their accompanying ovals in $PG(2, q)$, a flock $\mathcal{F}(\mathbf{C})$ of a quadratic cone in $PG(3, q)$, a line spread in $PG(3, q)$, and a whole variety of related translation planes. These various geometries derived from a Subiaco q–clan are all referred to as Subiaco geometries. In the present work we concentrate on the generalised

*The first author enjoyed the warm hospitality of both the Combinatorial Computing Research Group of The University of Western Australia and C. M. O'Keefe of The University of Adelaide, as well as the financial support of the Australian Research Council. He also gratefully acknowledges the friendly atmosphere of the Department of Pure Mathematics and Computer Algebra of the Universiteit of Ghent and the support of the Belgian National Fund For Scientific Research during the evolution of this paper.

†The third author acknowledges the support of a University of Western Australia Research Scholarship.

Received by the editors May 1994

Communicated by J. Thas

quadrangles and their related ovals. For example, when q is a square the Subiaco ovals provide the only known hyperovals in $PG(2,q)$ not containing a translation oval with the exception of the hyperoval in $PG(2,64)$ with full collineation stabiliser of order 12 [12] and the hyperoval in $PG(2,256)$ [13]. Prior to the discovery of these new ovals, the only such example known was the Lunelli-Sce [6] oval in $PG(2,16)$.

In [1] and [9] a general theory was worked out for studying the collineation groups of the $GQ(\mathbf{C})$ and the induced stabilisers of the associated ovals. In [9] this theory was applied in detail only in the special case $q=2^e$ with e odd, and there only for a particular form of the Subiaco q–clan. In [1] the general theory was developed in greater depth and applied in detail to a particular Subiaco q–clan with $q=2^e$, $e \equiv 2 \pmod 4$. In the present work we obtain a great deal of information about the general case. Since this paper is a direct continuation of [9] and [1], we assume without much comment all the notation and results of those two papers.

The authors of [2] originally gave three separate constructions, one for $q=2^e$, e odd, one for $e \equiv 2 \pmod 4$, and one that worked for all e. Here we give in Section 2 one general construction and show that it yields exactly the same set of q–clans as the three original ones combined. Our emphasis is primarily on the collineation group of $GQ(\mathbf{C})$. In Section 3 we show that for each line $[A(s)]$ through the point (∞) there is a unique involution I_s of $GQ(\mathbf{C})$ fixing the line $[A(s)]$, and derive as a consequence that the stabiliser $\mathcal{G}_0$ of the points $(\underline{0},0,\underline{0})$ and (∞) is transitive on the lines through (∞). This material is used in Section 4 to show that up to isomorphism, for each $q=2^e$, there is just one Subiaco GQ of order (q^2,q), and hence just one Subiaco flock. The proof of this somewhat surprising result is used in Section 5 to completely determine the group $\mathcal{G}_0$.

In Section 6 we begin a study of the Subiaco ovals. For $e \not\equiv 2 \pmod 4$ there is, up to isomorphism, just one Subiaco oval. Clearly we know the order of the induced stabiliser of the oval, but a detailed study of its action on the oval is postponed to a later work [10]. For $e \equiv 2 \pmod 4$ there are two Subiaco ovals. Their complete stabilisers are just those induced by $\mathcal{G}_0$. They are well understood and are given in detail. When $5 \mid e$, there are some technical difficulties remaining, but even in that case our general theory gives a satisfactory understanding of the ovals and their stabilisers.

2 A Canonical Form for the Subiaco q-clan

For $q=2^e$, $e \geq 4$, $F=GF(q)$, let $\delta \in F$ be chosen so that $x^2+\delta x+1$ is irreducible over F, that is, $\mathrm{tr}\,(\delta^{-2}) = \mathrm{tr}\,(\delta^{-1}) = 1$. Then define the following functions on F:

$$\begin{aligned}
&\text{(i)} \quad f(t) = \delta^2 t^4 + \delta^3 t^3 + (\delta^2+\delta^4)t^2, \\
&\text{(ii)} \quad g(t) = (\delta^2+\delta^4)t^3 + \delta^3 t^2 + \delta^2 t, \\
&\text{(iii)} \quad k(t) = (v(t))^2 = t^4 + \delta^2 t^2 + 1, \\
&\text{(iv)} \quad F(t) = \frac{f(t)}{k(t)},
\end{aligned} \tag{1}$$

$$\text{(v)} \quad G(t) = \frac{g(t)}{k(t)}.$$

Then the **canonical Subiaco q–clan** is the set $\mathbf{C}(\delta) = \mathbf{C} = \{A_t \mid t \in F\}$, where

$$A_t = \begin{pmatrix} F(t) + (\frac{t}{\delta})^{1/2} & t^{1/2} \\ 0 & G(t) + (\frac{t}{\delta})^{1/2} \end{pmatrix}, \quad t \in F. \tag{2}$$

2.1 Theorem *The matrices A_t given in* Eq.(2) *really do form a q–clan.*

Proof: Since our proof is really that of [2] modified to avoid the restriction $\delta^2+\delta+1 \neq 0$ necessitated by the form used in [2], we merely sketch the steps with enough detail for a routine reconstruction of a complete proof.

We need to show that for t, $u \in F$, $t \neq u$, the matrix $A_t + A_u$ is anisotropic. This is equivalent to showing that

$$\begin{aligned} 1 &= \operatorname{tr}\left\{\frac{[F(t)+F(u)+((t+u)/\delta)^{1/2}][G(t)+G(u)+((t+u)/\delta)^{1/2}]}{t+u}\right\} \quad (3) \\ &= \operatorname{tr}\left\{\frac{(F(t)+F(u))(G(t)+G(u))}{t+u}\right. \\ &\qquad \left. + \frac{(F(t)+G(t)+F(u)+G(u))}{(\delta(t+u))^{1/2}} + \delta^{-1}\right\}. \end{aligned}$$

Since $\operatorname{tr}(\delta^{-1}) = 1$, and using $\operatorname{tr}(a+b) = \operatorname{tr}(a+b^2)$, this is equivalent to showing that $\operatorname{tr}(A+B+C) = 0$, where

$$\begin{aligned} &\text{(i)} \quad A = \frac{f(t)^2 + \delta f(t)g(t) + g(t)^2}{\delta(t+u)k(t)^2}, \\ &\text{(ii)} \quad B = \frac{f(u)^2 + \delta f(u)g(u) + g(u)^2}{\delta(t+u)k(u)^2}, \\ &\text{(iii)} \quad C = \frac{f(t)g(u) + f(u)g(t)}{(t+u)k(t)k(u)}. \end{aligned} \tag{4}$$

The next trick is to notice upon writing out A that $k(t)$ divides the numerator of A. So also $k(u)$ divides the numerator of B. Then the numerator of $A+B$ is symmetric in t and u, so $t+u$ may be factored out. After simplifying,

$$\begin{aligned} A+B &= \delta^3\Big((1+\delta^2)(t^3u^2+t^2u^3)+t^3+t^2u+tu^2+u^3+ \\ &\quad +(\delta+\delta^3)t^3u^3+(\delta^3+\delta^5)t^2u^2+t+u \\ &\quad +(\delta+\delta^3)(t^2+tu+u^2)\Big) \Big/ (k(t)k(u)). \end{aligned} \tag{5}$$

After expansion, factoring out $t+u$, and a little simplification,

$$\begin{aligned} C &= \Big((\delta^4+\delta^6)t^3u^3+\delta^5(t^3u^2+t^2u^3)+\delta^4(t^3u+tu^3) \\ &\quad +(\delta^6+\delta^8)t^2u^2+\delta^5(t^2u+tu^2)+(\delta^4+\delta^6)tu\Big) \Big/ (k(t)k(u)). \end{aligned} \tag{6}$$

Then in a few more steps,

$$\begin{aligned} A+B+C &= \delta^3(t+u)\Big(t^2u^2+\delta(t^2u+tu^2)+\delta^2 tu \\ &\qquad +t^2+u^2+(\delta+\delta^3)(t+u)+1\Big) \Big/ k(t)k(u) \\ &= \frac{\delta^3(t+u)(v(t)v(u)+\delta^3(t+u))}{v(t)^2v(u)^2} \\ &= X+X^2, \quad \text{where } X=\frac{\delta^3(t+u)}{v(t)v(u)}. \end{aligned}$$

So $\mathrm{tr}\,(A+B+C)=0$, as desired. □

It is, of course, of interest to see that the canonical description given in Theorem 2.1 includes the examples given in [2] and studied in [9].

2.2 Theorem (i) *If $q=2^e$ with e odd, put $\delta=1$ in* Eqs.(1) *and* (2) *and replace A_t with PA_tP, $P=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ (and write the resulting matrices in upper triangular form) to get the original construction studied in* [2].
(ii) *If $q=2^e$ with $e\equiv 2 \pmod 4$, put $\delta=\omega$ where $\omega^2+\omega+1=0$, and replace A_t with $\begin{pmatrix}\omega^2&0\\0&\omega\end{pmatrix}A_t\begin{pmatrix}\omega^2&0\\0&\omega\end{pmatrix}$ to get the construction in* [2].
(iii) *For $q=2^e$, and assuming that $\delta^2+\delta+1\neq 0$, put $a=(\delta/(1+\delta+\delta^2))^{1/2}$. Then replace A_t with $\begin{pmatrix}1&1\\a&a+1\end{pmatrix}A_t\begin{pmatrix}1&a\\1&a+1\end{pmatrix}$ to get the original general Subiaco form given in* [2]. □

3 Involutions

From now on $\mathbf{C}$ denotes a Subiaco q–clan in canonical form, and $GQ(\mathbf{C})$ is the associated generalised quadrangle of order (q^2,q) (cf. [11], [1]). The full collineation group $\mathcal{G}$ of $GQ(\mathbf{C})$ must fix the point (∞) whenever $GQ(\mathbf{C})$ is not classical, which is certainly the case when $e\geq 4$, for reasons given in [1]. Clearly to determine $\mathcal{G}$ and its actions on the lines of $GQ(\mathbf{C})$ through the point (∞) it suffices to study the subgroup $\mathcal{G}_0$ fixing the point $(\underline{0},0,\underline{0})$ (and, of course, fixing the point (∞)). Let $\mathcal{H}$ be the subgroup of $\mathcal{G}_0$ fixing the line $[A(\infty)]$, and let $\mathcal{M}$ be the subgroup of $\mathcal{H}$ fixing the line $[A(0)]$. Also, let $L=GF(2)(\delta)\subseteq F$, and put $r=[F:L]$. Since $x^2+\delta x+1$ is irreducible over F, clearly r must be odd.

3.1 Proposition $|\mathcal{M}|=r(q-1)$, *and*

$$\begin{aligned} \mathcal{M} &= \Big\{\theta(a^2,aI,\sigma)\colon(\alpha,c,\beta)\mapsto(a\alpha^\sigma,ac^\sigma,a\beta^\sigma)\mid \\ &\qquad 0\neq a\in F,\ \sigma\in\mathrm{Gal}\,(F/L)\Big\}. \end{aligned} \tag{7}$$

Proof: This is an immediate corollary of Theorem 6.4 of [1], but we prefer to use the notation $\theta(\mu, B, \sigma, \pi)$ (or just $\theta(\mu, B, \sigma)$) to denote the collineation given in Eq.(10) of [1]. □

Note: For $0 \neq \mu \in F$, $B \in GL(2, q)$, $\sigma \in \mathrm{Aut}\,(F)$, put $\Delta = \det(B)$ and define $\pi\colon F \to F\colon t \mapsto \bar{t}$ by $\bar{t} = (\mu\Delta^{-1})^2 t^\sigma + \bar{0}$ for a fixed $\bar{0} \in F$. Then

$$\theta(\mu, B, \sigma)\colon (\alpha, c, \beta) \mapsto (\alpha^\sigma B, \mu^{1/2}c^\sigma + \sqrt{\alpha^\sigma B A_{\bar{0}} B^T (\alpha^\sigma)^T}, (\mu\Delta^{-1}\beta^\sigma + \bar{0}^{1/2}\alpha^\sigma)B),$$

induces a collineation of $GQ(\mathbf{C})$ provided $A_{\bar{t}} \equiv \mu B^{-1} A_t^\sigma B^{-T} + A_{\bar{0}}$ for all $t \in F$.

3.2 Proposition *The unique involution in $\mathcal{G}_0$ fixing $[A(1)]$ is*

$$\begin{aligned} I_1 \quad &: (\alpha, c, \beta) \mapsto (\beta P, c + \alpha \circ \beta, \alpha P) \\ &[A(t)] \mapsto [A(t^{-1})], \quad t \in \tilde{F} = F \cup \{\infty\}. \end{aligned} \tag{8}$$

Proof: Using the notation of Eqs.(1) and (2), $t^{-1}F(t) = G(t^{-1})$. This makes it easy to check directly that I_1 is a collineation mapping $[A(t)]$ to $[A(t^{-1})]$. Clearly I_1 is an involution, and uniqueness follows from Theorem 6.3 of [1] applied to $GQ(\mathbf{C}^{i_s})$. □

3.3 Proposition *There is a unique involution I_∞ in $\mathcal{H}$, that is, fixing $[A(\infty)]$.*

Proof: Put $B_\infty(= D_\infty^T$ in the notation of [1]$) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $a = d = 1+\delta+\delta^2$, $b = \delta^{3/2}$, $c = \delta^{1/2} + \delta^{5/2}$. Then a straightforward check using Theorem 5.2 and 6.3 of [1] shows that there is a unique involution in $\mathcal{H}$ given by

$$\begin{aligned} I_\infty \quad &: (\alpha, c, \beta) \mapsto (\alpha B_\infty, g_\delta(\alpha) + c, (\beta + \delta^{1/2}\alpha)B_\infty) \\ &[A(t)] \mapsto [A(t + \delta)]. \end{aligned} \tag{9}$$

Here $A_\delta = \begin{pmatrix} 1 + \delta^4 + \delta^6 & \delta^{1/2} \\ 0 & 1 + \delta^3 + \delta^7 \end{pmatrix}$, $g_\delta(\alpha) = \sqrt{\alpha A_\delta \alpha^T}$, $B_\infty A_\delta B_\infty^T = A_\delta$, and $B_\infty = B_\infty^{-1}$. □

The major goal of this section is to prove the following theorem.

3.4 Theorem *For each $s \in \tilde{F}$, there is a unique involution $I_s \in \mathcal{G}_0$ fixing the line $[A(s)]$.*

Proof: To find I_s for the generic $s \in F$, we must first compute the q–clan $\mathbf{C}^{i_s}$ obtained from $\mathbf{C}$ by using the shift-flip i_s (cf. [1]). Recall that i_s replaces A_t with $A^{i_s}_{(t+s)^{-1}} = (t + s)^{-1}(A_t + A_s)$. However, we may use Eq.(39) of [1] to obtain the new q–clan $\mathbf{C}^{i_s}$.

$$\begin{array}{ll}
a_4^{i_s} = \frac{\delta^3 s^2}{k(s)} & b_4^{i_s} = \frac{(\delta^2+\delta^4)s^2+\delta^2}{k(s)} \\
a_3^{i_s} = \frac{\delta^3 s^5+\delta^2 s^4+\delta^3 s+\delta^2+\delta^4}{k(s)^2} & b_3^{i_s} = \frac{(\delta^2+\delta^4)s^5+\delta^3 s^4+\delta^2 s+\delta^3}{k(s)^2} \\
a_2^{i_s} = \frac{\delta^3}{k(s)} & b_2^{i_s} = \frac{\delta^2+\delta^4}{k(s)} \\
a_1^{i_s} = \frac{\delta^3 s^3+\delta^2 s^2+\delta^2}{k(s)^2} & b_1^{i_s} = \frac{(\delta^2+\delta^4)s^3+\delta^3 s^2+\delta^2 s}{k(s)^2} \\
c_0^{i_s} = \frac{1}{k(s)} & c_2^{i_s} = \frac{\delta^2}{k(s)} \\
\Delta_{13}^{i_s} = \frac{\delta^5}{v(s)^5} & \Delta_{24}^{i_s} = \frac{\delta^5}{v(s)^4} \\
H = \delta^{-1/2} & K = \delta^{-1/2}.
\end{array} \tag{10}$$

The next step is the routine but onerous task of using Lemma 6.2 and Theorem 6.3 of [1] to verify that the unique involution θ_s of $GQ(\mathbf{C}^{i_s})$ fixing $[A^{i_s}(\infty)]$ really does exist and is given by $\theta_s = \theta(1, B_s, \mathrm{id}, \pi_s\colon t \mapsto t+\delta/v(s))$, where $B_s = \begin{pmatrix} a(s) & b(s) \\ c(s) & a(s) \end{pmatrix}$ is given by

$$\begin{aligned}
&\text{(i)} \quad a(s) = \frac{(s^5+1)(1+\delta+\delta^2)+(s^4+s)(1+\delta)}{v(s)^{5/2}} \\
&\text{(ii)} \quad b(s) = \frac{\delta^{3/2}s^5+\delta^{1/2}s^4+\delta^{3/2}s+\delta^{1/2}+\delta^{5/2}}{v(s)^{5/2}} \\
&\text{(iii)} \quad c(s) = \frac{(\delta^{1/2}+\delta^{5/2})s^5+\delta^{3/2}s^4+\delta^{1/2}s+\delta^{3/2}}{v(s)^{5/2}}.
\end{aligned} \tag{11}$$

Condition (i) of Theorem 6.1 of [1] implies that

$$\begin{aligned}
&\text{(i)} \quad b(s)+c(s) = \delta^{1/2}a(s) \\
&\text{(ii)} \quad (a(s))^2 + b(s)c(s) = 1.
\end{aligned} \tag{12}$$

With $\bar{0} = \delta/v(s)$, write $g_{\bar{0}}^{i_s}(\gamma) = \sqrt{\gamma A_{\bar{0}}^{i_s}\gamma^T}$. Then θ_s and i_s are computed using Eqs.(10), (17) and (18) of [1] to be

$$\begin{aligned}
&\text{(i)} \quad \theta_s\colon (\alpha,c,\beta) \mapsto (\alpha B_s, c+g_{\bar{0}}^{i_s}(\alpha B_s), (\beta+\bar{0}^{1/2}\alpha)B_s),\ t \mapsto \bar{t} = t+\bar{0}, \\
&\text{(ii)} \quad i_s\colon (\alpha,c,\beta) \mapsto (\beta+s^{1/2}\alpha, c+g_s(\alpha)+\alpha\circ\beta, \alpha),\ t \mapsto \bar{t} = (s+t)^{-1}.
\end{aligned} \tag{13}$$

The next step is to compute $I_s = i_s \circ \theta_s \circ i_s^{-1}$. A straightforward computation yields

$$\begin{aligned}
I_s\colon (\alpha,c,\beta) \mapsto & (((1+\bar{0}s)^{1/2}\alpha+\bar{0}^{1/2}\beta)B_s, \\
& c+g_s(\alpha)+\alpha\circ\beta+g_{\bar{0}}^{i_s}(\beta B_s+s^{1/2}\alpha B_s)+g_s(((1+\bar{0}s)^{1/2}\alpha+\bar{0}^{1/2}\beta)B_s) \\
& \quad +((\beta+s^{1/2}\alpha)B_s)\circ(((1+\bar{0}s)^{1/2}\alpha+\bar{0}^{1/2}\beta)B_s), \\
& (s\bar{0}^{1/2}\alpha+(1+\bar{0}s)^{1/2}\beta)B_s),\ t \mapsto \bar{t} = \frac{t(s^2+1)+\delta s^2}{\delta t+s^2+1}.
\end{aligned} \tag{14}$$

The first and third coordinates of the image of (α, c, β) under I_s are written in as simple a form as possible, but the middle coordinate can be simplified considerably.

Upon inspection of Eq.(14), it is seen that the middle term can be written in the form $c + (\alpha C\alpha^T + \alpha D\beta^T + \beta E\beta^T)^{1/2}$, where we may take C and E to be upper triangular. Using steps identical to those of the proof of 10.5.2 of [11] we find that $D = \bar{0}sP$. We could use the same approach to find information about C and E, but in the present case we can do better. From Eq.(14), $0 \mapsto \bar{0} = \delta s^2/(s^2+1)$. By considering the image of $(\alpha, 0, \underline{0}) \in A(0)$, which must be in $A(\bar{0}) = A(\frac{\delta s^2}{s^2+1})$, we see that $C \equiv (\frac{s^2+1}{s^2+\delta s+1})B_s A_{\frac{\delta s^2}{s^2+1}} B_s^T$. Similarly $\infty \mapsto \overline{\infty} = (s^2+1)/\delta$, and the fact that the image of $(\underline{0}, 0, \beta)$ must be in $A(\frac{s^2+1}{\delta})$ determines E. Specifically

$$I_s\colon (\alpha, c, \beta) \mapsto (\,-\,, c + \sqrt{\alpha C\alpha^T + \alpha D\beta^T + \beta E\beta^T},\, -\,) \qquad (15)$$

where

$$\text{(i)} \quad C \equiv \left(\frac{s^2+1}{s^2+\delta s+1}\right) B_s A_{\frac{\delta s^2}{s^2+1}} B_s^T$$

$$\text{(ii)} \quad D = \bar{0}sP = \left(\frac{\delta s^2}{s^2+\delta s+1}\right) P$$

$$\text{(iii)} \quad E \equiv \left(\frac{\delta}{s^2+\delta s+1}\right) B_s A_{\frac{s^2+1}{\delta}} B_s^T.$$

This completes the proof of Theorem 3.4. □

3.5 Corollary *$\mathcal{G}_0$ is transitive on the lines through (∞). Hence there arises only one Subiaco flock for each Subiaco q–clan.*

Proof: Since $I_s\colon [A(\infty)] \mapsto [A(\frac{s^2+1}{\delta})]$, by letting s vary over all elements of F transitivity is assured. Then by Theorem 2.5 of [1], only one flock arises. □

4 Isomorphisms between Subiaco GQ

Let δ_1, δ_2 be any two (not necessarily distinct) elements of F for which $\mathrm{tr}\,(\delta_1^{-1}) = \mathrm{tr}\,(\delta_2^{-1}) = 1$. For $i = 1, 2$, let $\mathbf{C}_i = \mathbf{C}(\delta_i)$ be the canonical Subiaco q–clan constructed using δ_i in Eqs.(1) and (2), but with the following notation: $\mathbf{C}_1 = \{A_t = \begin{pmatrix} x_t & y_t \\ 0 & z_t \end{pmatrix} \mid t \in F\}$, $x_t = F(t) + (t/\delta_1)^{1/2}$, where $F(t)$ is defined using δ_1, etc. and $\mathbf{C}_2 = \{A'_t = \begin{pmatrix} x'_t & y'_t \\ 0 & z'_t \end{pmatrix} \mid t \in F\}$, $x'_t = F'(t) + (t/\delta_2)^{1/2}$, etc. Of course $A_0 = A'_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $y_t = y'_t = t^{1/2}$ for all $t \in F$. The general goal of this section is to determine all isomorphisms $\theta\colon GQ(\delta_1) = GQ(\mathbf{C}_1) \to GQ(\delta_2) = GQ(\mathbf{C}_2)$. One major corollary will be that there is always such an isomorphism. A second major corollary, worked out in Section 5, will be a complete determination of the group $\mathcal{G}_0$.

4.1 Lemma *If* $\delta_2 = \delta_1^\sigma$ *for some* $\sigma \in \mathrm{Aut}\, F$*, then*

$$\begin{aligned} \theta(1, I, \sigma, \pi) \quad : \quad & GQ(\mathbf{C}_1) \to GQ(\mathbf{C}_2) \\ & (\alpha, c, \beta) \mapsto (\alpha^\sigma, c^\sigma, \beta^\sigma), \quad \bar{t} = t^\sigma, \end{aligned} \tag{16}$$

is an isomorphism.

Proof: Clear from Proposition 2.2 with Eq.(10) from [1], since $A_t^\sigma = A'_{t^\sigma}$. □

4.2 Lemma $GQ(\mathbf{C}_1)$ *and* $GQ(\mathbf{C}_2)$ *are isomorphic if and only if there is an isomorphism* $\theta\colon GQ(\mathbf{C}_1) \to GQ(\mathbf{C}_2)$ *of the following type (put* $\Delta = \det B$*).*

$$\begin{aligned} \text{(i)} \quad & \theta(\mu, B, \sigma, \pi)\colon GQ(\mathbf{C}_1) \to GQ(\mathbf{C}_2) \\ & (\alpha, c, \beta) \mapsto \Big(\alpha^\sigma B, \mu^{1/2} c^\sigma + \sqrt{\alpha^\sigma B A'_{\bar{0}} B^T (\alpha^\sigma)^T}, \\ & \qquad (\mu \Delta^{-1} \beta^\sigma + \bar{0}^{1/2} \alpha^\sigma) B\Big) \end{aligned} \tag{17}$$

where

$$\text{(ii)} \quad A'_{\bar{t}} \equiv \mu B^{-1} A_t^\sigma B^{-T} + A'_{\bar{0}}$$

and

$$\text{(iii)} \quad \pi\colon t \mapsto \bar{t} = (\mu/\Delta)^2 t^\sigma + \bar{0}.$$

Proof: Use Corollary 3.5 and the Fundamental Theorem with Eq.(10) of [1]. □

4.3 Lemma *For* $\delta_i \in F$ *with* $\mathrm{tr}\,(\delta_i^{-1}) = 1$, $i = 1, 2, 3$, *suppose*

$$\theta_i = \theta(\mu_i, B_i, \sigma_i, \pi_i)\colon GQ(\delta_i) \to GQ(\delta_{i+1}),$$

$i = 1, 2$, *with the notation of* Eq.(17). *Then*

$$\theta_1 \circ \theta_2 = \theta(\mu, B, \sigma, \pi)\colon GQ(\mathbf{C}_1) \to GQ(\mathbf{C}_2),$$

where

$$\begin{aligned} \text{(i)} \quad & \mu = \mu_1^{\sigma_2} \mu_2, \\ \text{(ii)} \quad & B = B_1^{\sigma_2} B_2, \\ \text{(iii)} \quad & \sigma = \sigma_1 \circ \sigma_2, \\ \text{(iv)} \quad & \pi\colon t \mapsto \bar{t} = \left(\frac{\mu_1^{\sigma_2} \mu_2}{\Delta_1^{\sigma_2} \Delta_2}\right)^2 t^{\sigma_1 \circ \sigma_2} + \left(\frac{\mu_2}{\Delta_2}\right)^2 0^{\pi_1 \circ \sigma_2} + 0^{\pi_2}. \end{aligned} \tag{18}$$

Proof: Easy exercise. □

Follow $\theta = \theta(\mu, B, \sigma, \pi)\colon GQ(\delta_1) \to GQ(\delta_2)$ with $\theta' = \theta(1, I, \sigma^{-1}, \pi'\colon t \mapsto t^{\sigma^{-1}})\colon GQ(\delta_2) \to GQ(\delta_2^{\sigma^{-1}})$. Then $\theta \circ \theta'\colon GQ(\delta_1) \to GQ(\delta_2^{\sigma^{-1}})$ is an isomorphism of the type given in Eq.(17) with $\sigma = \mathrm{id}$. So replace δ_2 with $\delta_2^{\sigma^{-1}}$ (or equally satisfactory, replace δ_1 with δ_1^σ) and from now on suppose that $\sigma = \mathrm{id}$. An isomorphism of the type $\theta(\mu, B, \sigma, \pi)\colon GQ(\mathbf{C}_1) \to GQ(\mathbf{C}_2)$ is said to be **semilinear** and to have

companion automorphism σ, and to be **linear** provided $\sigma = \mathrm{id}$. Note that the composition of linear isomorphisms is linear.

Recall that for any normalised q–clan $\mathbf{C}$ there is a group $\mathcal{N}$ of automorphisms of $GQ(\mathbf{C})$ of the type

$$\mathcal{N} = \Big\{\theta_a = \theta(a^2, aI, \mathrm{id}, \pi = \mathrm{id})\colon (\alpha, c, \beta) \mapsto (a\alpha, ac, a\beta) \mid 0 \neq a \in F\Big\}. \quad (19)$$

$\mathcal{N}$ is the **kernel** of $GQ(\mathbf{C})$, and by 2.4 of [1], for $q = 2^e$ and $\mathbf{C}$ not classical, $\mathcal{N}$ consists of all collineations of $GQ(\mathbf{C})$ fixing (∞) and $(\underline{0}, 0, \underline{0})$ linewise. If we follow θ by θ_a with $a = \Delta^{-1/2}$, then $\theta \circ \theta_a = \theta(\mu/\Delta, \Delta^{-1/2}B, \mathrm{id}, \pi)$ and $\det(\Delta^{-1/2}B) = 1$. Hence without loss of generality, from now on we may suppose that θ is a **special linear** isomorphism, that is,

$$\begin{aligned} &\theta = \theta(\mu, B, \mathrm{id}, \pi)\colon GQ(\delta_1) \to GQ(\delta_2) \qquad (20)\\ &(\alpha, c, \beta) \mapsto \Big(\alpha B, \mu^{-1/2}c + \sqrt{\alpha B A_0' B^T \alpha^T}, (\mu\beta + \bar{0}^{1/2}\alpha)B\Big)\\ &\text{where } \det B = 1, \text{ and } \pi\colon t \mapsto \bar{t} = \mu^2 t + \bar{0}, \text{ for all } t \in F.\\ &\text{We write } B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ so } B^{-1} = \begin{pmatrix} d & b \\ c & a \end{pmatrix}. \end{aligned}$$

For each $s \in \tilde{F}$, the unique involution I_s of $GQ(\delta_1)$ fixing the line $[A(s)]$ permutes the lines $[A(t)]$, $t \in \tilde{F}$, according to the Möbius transformation (cf. Eq.(14)),

$$I_s\colon t \mapsto \frac{t(s^2+1) + \delta_1 s^2}{\delta_1 t + s^2 + 1}. \quad (21)$$

Similarly, the unique involution $I'_{\bar{s}}$ of $GQ(\delta_2)$ fixing the line $[A'(\bar{s})]$ permutes the lines $[A'(\bar{t})]$, $t \in \tilde{F}$, according to

$$I'_{\bar{s}}\colon \bar{t} \mapsto \frac{\bar{t}(\bar{s}^2+1) + \delta_2 \bar{s}^2}{\delta_2 \bar{t} + \bar{s}^2 + 1},\ t \in \tilde{F}. \quad (22)$$

Moreover, $\theta^{-1} \circ I_s \circ \theta$ is clearly an involution of $GQ(\delta_2)$ fixing $\bar{s}$, that is,

$$I'_{\bar{s}} = \theta^{-1} \circ I_s \circ \theta, \quad \text{for all } s \in \tilde{F}. \quad (23)$$

Put $\bar{t} = \mu^2 t + \bar{0}$ and $\bar{s} = \mu^2 s + \bar{0}$ for all t, $s \in \tilde{F}$ into Eq.(22).

$$\begin{aligned} I'_{\bar{s}}\colon \bar{t} &\mapsto \frac{(\mu^2 t + \bar{0})(\mu^4 s^2 + \bar{0}^2 + 1) + \delta_2(\mu^4 s^2 + \bar{0}^2)}{\delta_2(\mu^2 t + \bar{0}) + (\mu^4 s^2 + \bar{0}^2) + 1} \qquad (24)\\ &= \frac{t(\mu^6 s^2 + \mu^2\bar{0}^2 + \mu^2) + \bar{0}(\mu^4 s^2 + \bar{0}^2 + 1) + \delta_2(\mu^4 s^2 + \bar{0}^2)}{t(\mu^2\delta_2) + \bar{0}^2 + \delta_2\bar{0} + \mu^4 s^2 + 1}\\ &\text{for all } s,\ t \in \tilde{F}. \end{aligned}$$

Now compute the effect of $\theta^{-1} \circ I_s \circ \theta$ on $\bar{t}$. Here

$$\bar{t} \overset{\theta^{-1}}{\mapsto} t \overset{I_s}{\mapsto} \frac{t(s^2+1)+\delta_1 s^2}{\delta_1 t + s^2 + 1} \overset{\theta}{\mapsto} \frac{\mu^2\left(t(s^2+1)+\delta_1 s^2\right)}{\delta_1 t + s^2 + 1} + \bar{0}$$
$$= \frac{t(\mu^2(s^2+1)+\bar{0}\delta_1)+\delta_1\mu^2 s^2 + \bar{0}(s^2+1)}{\delta_1 t + s^2 + 1}.$$

Using this with Eqs(23) and (24), we obtain

$$\frac{t(\mu^6 s^2 + \mu^2\bar{0}^2 + \mu^2) + \bar{0}(\bar{0}^2 + \delta_2\bar{0} + \mu^4 s^2 + 1) + \delta_2\mu^4 s^2}{t(\mu^4\delta_2) + \bar{0}^2 + \delta_2\bar{0} + \mu^4 s^2 + 1} \tag{25}$$
$$= \frac{t(\mu^2(s^2+1)+\bar{0}\delta_1)+\delta_1\mu^2 s^2 + \bar{0}(s^2+1)}{\delta_1 t + s^2 + 1}, \text{ for all } t,\ s \in \tilde{F}.$$

Put $t = 0$ in Eq.(25) and write the resulting equality as a polynomial in s. After a little simplification we obtain

$$\mu^4(\delta_2 + \delta_1\mu^2)s^4 + \left(\delta_2\mu^4 + \delta_1\mu^2(\bar{0}^2 + \delta_2\bar{0} + 1)\right) s^2 = 0. \tag{26}$$

Even if we ignore a few values of $s \in \tilde{F}$ (say $s = \infty$, $s = 0$ and $s = 1$), there are more than enough values of $s \in F$ for which Eq.(26) must hold to force the coefficients on s^4 and s^2 to be zero. Hence we obtain

$$\begin{array}{ll} \text{(i)} & \delta_2 = \mu^2\delta_1 \\ \text{(ii)} & \bar{0}^2 + \mu^2\delta_1\bar{0} + \mu^4 + 1 = 0. \end{array} \tag{27}$$

And conversely, if Eq.(27)(i) and (ii) both hold, then Eq.(25) holds. This means that Eq.(27) contains all the information to be obtained from Eq.(23) by considering only the effect of $I'_{\bar{s}}$ on $\tilde{F} \cong PG(1,q)$.

Recall Eq.(17) with the notation of Eq.(20) for our special linear θ.

$$A'_{\bar{t}} + A'_{\bar{0}} \equiv \mu \begin{pmatrix} d & b \\ c & a \end{pmatrix} \begin{pmatrix} x_t & t^{1/2} \\ 0 & z_t \end{pmatrix} \begin{pmatrix} d & c \\ b & a \end{pmatrix} \tag{28}$$
$$\equiv \mu \begin{pmatrix} d^2x_t + dbt^{1/2} + b^2 z_t & t^{1/2} \\ 0 & c^2 x_t + cat^{1/2} + a^2 z_t \end{pmatrix}.$$

Here

$$\text{(i)} \quad x_t = \frac{\delta_1^2 t^4 + \delta_1^3 t^3 + (\delta_1^2 + \delta_1^4)t^2}{t^4 + \delta_1^2 t^2 + 1} + (t/\delta_1)^{1/2}, \tag{29}$$
$$\text{(ii)} \quad z_t = \frac{(\delta_1^2 + \delta_1^4)t^3 + \delta_1^3 t^2 + \delta_1^2 t}{t^4 + \delta_1^2 t^2 + 1} + (t/\delta_1)^{1/2},$$

with analogous expressions obtained for x'_t and z'_t by replacing δ_1 with δ_2.

We want to express in detail the calculation that (for $\bar{t} = \mu^2 t + \bar{0}$)

$$x'_{\bar{t}} + x'_{\bar{0}} = \mu(d^2 x_t + dbt^{1/2} + b^2 z_t). \tag{30}$$

Use Eq.(27) and several routine steps to compute

$$\begin{aligned} x'_{\bar{t}} + x'_{\bar{0}} &= (t/\delta_1)^{1/2} + \frac{\delta_1^2\,(t^4(\mu^4 + \bar{0}^2(1+\delta_1^2)) + t^3(\mu^4\delta_1))}{t^4 + \delta_1^2 t^2 + 1} \\ &\quad + \frac{\delta_1^2\,(t^2(\mu^2\delta_1\bar{0} + 1 + \mu^4\delta_1^2 + \bar{0}^2(\delta_1^2 + \delta_1^4)) + t(\bar{0}^2\delta_1))}{t^4 + \delta_1^2 t^2 + 1}. \end{aligned} \tag{31}$$

Next compute

$$\begin{aligned} \mu(d^2 x_t + dbt^{1/2} + b^2 z_t) &= \mu(d^2 + db\delta_1^{1/2} + b^2)(t/\delta_1)^{1/2} + \\ &\frac{\mu\delta_1^2\,(t^4 d^2 + t^3(d^2\delta_1 + b^2(1+\delta_1^2)) + t^2(d^2(1+\delta_1^2) + b^2\delta_1) + tb^2)}{t^4 + \delta_1^2 t^2 + 1}. \end{aligned} \tag{32}$$

Now equate coefficients on like powers of t on both sides of Eq.(30) using Eqs.(31) and (32).

$$\begin{aligned} &\text{(i)} \quad \text{Coeff. on } t^4 \Rightarrow \mu d^2 = \mu^4 + \bar{0}^2(1+\delta_1^2) \\ &\qquad\qquad = \bar{0}(\mu^2\delta_1 + \mu^2\delta_1^3) + 1 + \delta_1^2 + \mu^4\delta_1^2. \\ &\text{(ii)} \quad \text{Coeff. on } t \Rightarrow \mu b^2 = \delta_1\bar{0} = \bar{0}(\mu^2\delta_1^2) + \delta_1 + \mu^4\delta_1. \end{aligned} \tag{33}$$

The conditions in Eq.(33) completely determine d and b as functions of $\bar{0}$. The surprising thing is that the conditions of Eq.(33) are sufficient to show (with much use of Eq.(27)(ii)) that the coefficients on t^3, t^2 and $t^{1/2}$, respectively, on both sides of Eq.(30) are equal.

Next we want to express in detail the condition that

$$z'_{\bar{t}} + z'_{\bar{0}} = \mu(c^2 x_t + cat^{1/2} + a^2 z_t). \tag{34}$$

With routine computation using Eq.(27) we find

$$\begin{aligned} z'_{\bar{t}} + z'_{\bar{0}} &= (t/\delta_1)^{1/2} + \frac{\delta_1^2(t^4(\bar{0} + \delta_1^2\bar{0}^3) + t^3(\mu^2 + \mu^6\delta_1^2))}{t^4 + \delta_1^2 t^2 + 1} \\ &\quad + \frac{\delta_1^2(t^2(\mu^2\delta_1 + \bar{0}(1 + \mu^4\delta_1^2) + \delta_1^4\bar{0}^3 + \delta_1^2\bar{0}))}{t^4 + \delta_1^2 t^2 + 1} \\ &\quad + \frac{\delta_1^2(t(\delta_1\bar{0}(1 + \mu^4\delta_1^2) + \mu^2\delta_1^2 + \mu^2 + \mu^6\delta_1^2))}{t^4 + \delta_1^2 t^2 + 1}, \end{aligned} \tag{35}$$

and

$$\begin{aligned} \mu(c^2 x_t + cat^{1/2} + a^2 z_t) &= \mu(c^2 + ca\delta_1^{1/2} + a^2)(t/\delta_1)^{1/2} \\ &+ \frac{\mu\delta_1^2(c^2 t^4 + t^3(c^2\delta_1 + a^2(1+\delta_1^2)) + t^2(c^2(1+\delta_1^2) + a^2\delta_1) + a^2 t)}{t^4 + \delta_1^2 t^2 + 1}. \end{aligned} \tag{36}$$

Now we equate coefficients on like powers of t on both sides of Eq.(34) using Eqs.(35) and (36).

$$\begin{aligned} &\text{(i)} \quad \text{Coeff. on } t^4 \Rightarrow \mu c^2 = \bar{0}^3\delta_1^2 + \bar{0} \\ &\qquad = \bar{0}(\mu^4\delta_1^4 + \mu^4\delta_1^2 + \delta_1^2 + 1) + \mu^2\delta_1^3 + \mu^6\delta_1^3 \\ &\text{(ii)} \quad \text{Coeff. on } t \Rightarrow \mu a^2 = \bar{0}(\delta_1 + \mu^4\delta_1^3) + \mu^2 + \mu^2\delta_1^2 + \mu^6\delta_1^2. \end{aligned} \tag{37}$$

And now it is possible to use Eqs.(37) and (27) to verify that the coefficients on t^3, t^2 and $t^{1/2}$, respectively, on both sides of Eq.(34) are equal.

This means that we have effectively determined all special linear isomorphisms from $GQ(\delta_1)$ to $GQ(\delta_2)$ with the interesting corollary that there always is one.

4.4 Theorem *Let δ_1 and δ_2 be any two elements of F for which* $\text{tr}\,(\delta_1^{-1}) = \text{tr}\,(\delta_2^{-1}) = 1$. *Put $\mu^2 = \delta_2/\delta_1$. Then $(\mu^4+1)/\mu^4\delta_1^2 = \delta_1^{-2} + \delta_2^{-2}$ has trace 0. Hence*

$$\bar{0}^2 + \mu^2\delta_1\bar{0} + \mu^4 + 1 = 0 \tag{38}$$

has two solutions with $\bar{0} \in F$ (say $\bar{0}$ and $\bar{0} + \mu^2\delta_1$). Put $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where

$$\begin{aligned} &\text{(i)} \quad \mu a^2 = \bar{0}(\delta_1 + \mu^4\delta_1^3) + \mu^2\delta_1^2 + \mu^6\delta_1^2 + \mu^2, \\ &\text{(ii)} \quad \mu b^2 = \bar{0}(\mu^2\delta_1^2) + \mu^4\delta_1 + \delta_1, \\ &\text{(iii)} \quad \mu c^2 = \bar{0}(\mu^4\delta_1^4 + \mu^4\delta_1^2 + \delta_1^2 + 1) + \mu^2\delta_1^3 + \mu^6\delta_1^3, \\ &\text{(iv)} \quad \mu d^2 = \bar{0}(\mu^2\delta_1 + \mu^2\delta_1^3) + 1 + \delta_1^2 + \mu^4\delta_1^2. \end{aligned} \tag{39}$$

Then

$$\begin{aligned} \theta(\mu, B, \text{id}, \pi\colon t \mapsto \bar{t} = \mu^2 t + \bar{0})\colon GQ(\delta_1) \to GQ(\delta_2) \\ (\alpha, c, \beta) \mapsto \left(\alpha B, \mu^{1/2}c + \sqrt{\alpha B A_0' B^T \alpha^T}, (\mu\beta + \bar{0}^{1/2}\alpha)B\right) \end{aligned} \tag{40}$$

is a special linear isomorphism.

Conversely, each special linear isomorphism from $GQ(\delta_1)$ to $GQ(\delta_2)$ mapping $(\underline{0}, 0, \underline{0}) \mapsto (\underline{0}, 0, \underline{0})$, $[A(\infty)] \mapsto [A'(\infty)]$, $(\infty) \mapsto (\infty)$, must be of this form. □

Using the results of Sections 3 and 4 we can now determine all collineations of $GQ(\mathbf{C})$, for $\mathbf{C}$ a canonical Subiaco q–clan. In fact, we need only determine the stabiliser $\mathcal{H}$ of $[A(\infty)]$ in $\mathcal{G}_0$.

5 The Stabiliser $\mathcal{H}$ of $[A(\infty)]$

By the Fundamental Theorem [1] we know that any $\theta \in \mathcal{H}$ must be of the form $\theta = \theta(\mu, B, \sigma, \pi)$ given in Eq.(17). All such collineations with $\sigma = \text{id}$ are give by Lemma 6.2 of [1] (using slightly different notation), but we may also use Section 4 of the present work with $\delta_1 = \delta_2$, $\mu = 1$, along with the kernel $\mathcal{N}$.

Fix $\delta \in F$ with $\mathrm{tr}\,(\delta^{-1}) = 1$, and let $\sigma \in \mathrm{Aut}\,F$. Put $\delta_1 = \delta^\sigma$ and $\delta_2 = \delta$. In the context of Theorem 4.4, $\mu^2 = \delta_2/\delta_1 = \delta^{1-\sigma}$, so

$$\mu \;=\; \delta^{\frac{1-\sigma}{2}}. \tag{41}$$

Then Eq.(38) becomes

$$0 \;=\; \bar{0}^2 + \delta\bar{0} + \delta^{2(1-\sigma)} + 1. \tag{42}$$

One solution of Eq.(42) is

$$\bar{0} \;=\; \sum_{i=1}^{j} \delta^{1-2^i}, \quad \text{where } \sigma\colon x \mapsto x^{2^j}. \tag{43}$$

(If $\sigma = \mathrm{id}$, $j = 0$, then $\bar{0} = 0$ or $\bar{0} = \delta$).

The other solution is $\bar{0} + \delta$. For either of these two solutions for $\bar{0}$, by Theorem 4.4 there is the following isomorphism:

$$\begin{aligned} \theta \;=\; & \theta(\delta^{\frac{1-\sigma}{2}}, B, \mathrm{id}, \pi) : GQ(\delta^\sigma) \to GQ(\delta) \\ & (\alpha, c, \beta) \mapsto (\alpha B, \delta^{\frac{1-\sigma}{4}} c + \sqrt{\alpha B A_{\bar{0}} B^T \alpha^T}, (\delta^{\frac{1-\sigma}{2}} \beta + \bar{0}^{1/2}\alpha)B), \end{aligned} \tag{44}$$

where B is determined by Eqs.(39) and (41). Also $\pi\colon t \mapsto \bar{t} = \delta^{1-\sigma} t + \bar{0}$.

We also have $\theta_\sigma\colon GQ(\delta) \to GQ(\delta^\sigma)$, $(\alpha, c, \beta) \mapsto (\alpha^\sigma, c^\sigma, \beta^\sigma)$. Composition of these two collineations gives

(i) $\theta_\sigma \circ \theta\colon GQ(\delta) \to GQ(\delta)$

$$(\alpha, c, \beta) \mapsto (\alpha^\sigma B, \delta^{\frac{1-\sigma}{4}} c^\sigma + \sqrt{\alpha^\sigma B A_{\bar{0}} B^T (\alpha^\sigma)^T}, (\delta^{\frac{1-\sigma}{2}} \beta^\sigma + \bar{0}^{1/2}\alpha^\sigma)B). \tag{45}$$

(ii) $\theta_\sigma \circ \theta = \theta(\mu, B, \sigma, \pi)$ with $\pi\colon t \mapsto \delta^{1-\sigma} t^\sigma + \bar{0}$ and $\Delta = \det(B) = 1$.

If we follow $\theta_\sigma \circ \theta$ with $\theta_a \in \mathcal{N}$ (as in Eq.(19)) we obtain all elements of $\mathcal{H}$.

5.1 Theorem $|\mathcal{H}| = 2e(q-1)$. *Specifically, for each* $\sigma \in \mathrm{Aut}\,F$,

(i) *Let* $\bar{0}$ *be either solution to* $\bar{0}^2 + \delta\bar{0} + \delta^{2-2\sigma} + 1 = 0$.

(ii) *Put* $\bar{a} = \bar{0}^{1/2}\left(\delta^{\frac{3\sigma-1}{4}} + \delta^{\frac{3\sigma+3}{4}}\right) + \delta^{\frac{1-\sigma}{4}} + \delta^{\frac{3\sigma+1}{4}} + \delta^{\frac{5-\sigma}{4}}$.

(iii) *Put* $\bar{b} = \bar{0}^{1/2}\delta^{\frac{3\sigma+1}{4}} + \delta^{\frac{3-\sigma}{4}} + \delta^{\frac{3\sigma-1}{4}}$.

(iv) *Put* $\bar{c} = \bar{0}^{1/2}\left(\delta^{\frac{5\sigma+3}{4}} + \delta^{\frac{\sigma+3}{4}} + \delta^{\frac{5\sigma-1}{4}} + \delta^{\frac{\sigma-1}{4}}\right) + \delta^{\frac{5\sigma+1}{4}} + \delta^{\frac{\sigma+5}{4}}$.

(v) *Put* $\bar{d} = \bar{0}^{1/2}\left(\delta^{\frac{\sigma+1}{4}} + \delta^{\frac{5\sigma+1}{4}}\right) + \delta^{\frac{\sigma-1}{4}} + \delta^{\frac{5\sigma-1}{4}} + \delta^{\frac{\sigma+3}{4}}$.

(vi) *Put* $\bar{B} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$, *so* $\det(\bar{B}) = 1$.

(vii) *For* $0 \neq a \in F$, *put* $\mu = a^2\delta^{\frac{1-\sigma}{2}}$, $B = a\bar{B}$, $\Delta = a^2 = \det(B)$.
Then the general element of $\mathcal{H}$ *is given by*

$$\text{(i)}\quad \theta(\mu, B, \sigma, \pi)\colon (\alpha, c, \beta) \mapsto \tag{46}$$

$$(\alpha^\sigma B, \mu^{1/2}c^\sigma + \sqrt{\alpha^\sigma B A_{\bar{0}} B^T(\alpha^\sigma)^T}, (\mu\Delta^{-1}\beta^\sigma + \bar{0}^{1/2}\alpha^\sigma)B),$$

$$\pi\colon t \mapsto (\mu/\Delta)^2 t^\sigma + \bar{0}, \text{ or}$$

$$\text{(ii)}\quad \theta(a^2\delta^{\frac{1-\sigma}{2}}, B, \sigma, \pi)\colon (\alpha, c, \beta) \mapsto$$

$$(a\alpha^\sigma \bar{B}, a\delta^{\frac{1-\sigma}{4}}c^\sigma + a\sqrt{\alpha^\sigma \bar{B} A_{\bar{0}} \bar{B}^T(\alpha^\sigma)^T}, a(\delta^{\frac{1-\sigma}{2}}\beta^\sigma + \bar{0}^{1/2}\alpha^\sigma)\bar{B}),$$

$$\pi\colon t \mapsto \delta^{1-\sigma}t^\sigma + \bar{0}.$$

Note that $a = 1$, $\sigma = \mathrm{id}$, $\bar{0} = \delta$ *gives the unique involution* I_∞ *fixing* $[A(\infty)]$.

Proof: To get $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{d}$, use $\mu = \delta^{\frac{1-\sigma}{2}}$ and $\delta_1 = \delta^\sigma$, $\delta_2 = \delta$, in Theorem 4.4. □

5.2 Corollary $|\mathcal{G}_0| = 2e(q^2 - 1)$. □

Let $L = GF(2)(\delta) \subseteq F \subseteq E = GF(q^2)$. The hypothesis that $p(x) = x^2 + \delta x + 1$ be irreducible over F means that $p(x) = (x + \lambda)(x + \lambda^{-1})$ for some $\lambda \in E \setminus F$. Let ζ be a primitive element for E, so $\lambda = \zeta^j$ for some j. Then $\lambda \notin F$ if and only if $j \not\equiv 0 \pmod{q+1}$. The unique minimal polynomial for λ over F must be $x^2 + (\lambda + \lambda^q)x + \lambda^{q+1} = p(x) = x^2 + \delta x + 1$, so necessarily $\lambda^{q+1} = 1$. This is equivalent to $j \equiv 0 \pmod{q-1}$. So we may put $j = n(q-1)$, $1 \leq n \leq q$. In view of Theorem 4.4, we may choose whichever n is most convenient.

Consider the following pair of involutions.

$$\text{(i)}\quad I_0 = \theta\left(1, B_0, \mathrm{id}, \pi\colon t \mapsto t/(\delta t + 1)\right), \tag{47}$$

$$\text{with } B_0 = \begin{pmatrix} 1 + \delta + \delta^2 & \delta^{1/2} + \delta^{5/2} \\ \delta^{3/2} & 1 + \delta + \delta^2 \end{pmatrix}.$$

$$\text{(ii)}\quad I_\delta = \theta\left(1, B_\delta, \mathrm{id}, \pi\colon t \mapsto (t(\delta^2+1) + \delta^3)/(\delta t + \delta^2 + 1)\right),$$

$$\text{with } B_\delta = \begin{pmatrix} 1 + \delta^4 + \delta^6 + \delta^7 & \delta^{1/2} + \delta^{9/2} + \delta^{13/2} \\ \delta^{15/2} & 1 + \delta^4 + \delta^6 + \delta^7 \end{pmatrix}.$$

First consider the action of $I_0 \circ I_\delta$ on the lines $[A(t)]$, $t \in \tilde{F}$. For $t \in F$, let t correspond to $(t, 1) \in PG(1, q)$ and ∞ correspond to $(1, 0)$. So $t \mapsto (at + b)/(ct + d)$ is represented in matrix form by $\gamma \mapsto \gamma \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ for $\gamma \in PG(1, q)$. So I_0 and I_δ, respectively, are represented by $\begin{pmatrix} 1 & \delta \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} \delta^2 + 1 & \delta \\ \delta^3 & \delta^2 + 1 \end{pmatrix}$, respectively. Then $I_0 \circ I_\delta$ is represented by $\begin{pmatrix} 1 + \delta^2 + \delta^4 & \delta^3 \\ \delta^3 & 1 + \delta^2 \end{pmatrix}$ with trace δ^4 and det $= 1$. Hence $I_0 \circ I_\delta$ has eigenvalues λ^4 and λ^{-4} on $\tilde{F}$. Then $(\lambda^4)^j \in F$ if and only if $\lambda^j \in F$.

If $n = 1$, that is, $\lambda = \zeta^{q-1}$, then $\lambda^{4j} \in F$ if and only if $j \equiv 0 \pmod{q+1}$ if and only if $(I_0 \circ I_\delta)^j = \text{id}$ on $\tilde{F}$, so that $I_0 \circ I_\delta$ permutes the lines $[A(t)]$ in a cycle of length $q+1$.

Now consider the action of $I_0 \circ I_\delta$ on the subquadrangles, that is, on the subgroups G_α. $I_0 \circ I_\delta \colon G_\alpha \mapsto G_{\alpha B_0 B_\delta}$. First compute

$$\text{(i)} \quad B_0 \circ B_\delta = \begin{pmatrix} 1+\delta+\delta^2+\delta^4+\delta^5+\delta^8+\delta^9+\delta^{10} & \delta^{3/2}+\delta^{11/2}+\delta^{19/2} \\ \delta^{3/2}+\delta^{11/2}+\delta^{19/2} & 1+\delta+\delta^4+\delta^5+\delta^6+\delta^8+\delta^9 \end{pmatrix}, \tag{48}$$

and in general

$$\text{(ii)} \quad (B_0 \circ B_\delta)^j = \frac{1}{\delta^{1/2}} \begin{pmatrix} [10j + \frac{1}{2}] & [10j] \\ [10j] & [10j - \frac{1}{2}] \end{pmatrix}, \text{ where } [a] = \lambda^a + \lambda^{-a}.$$

(**Note**: The formula in Eq.(48)(ii) is obtained by diagonalising $B_0 \circ B_\delta$ over E.)

Since $\det(B_0 \circ B_\delta) = 1$ and $\operatorname{tr}(B_0 \circ B_\delta) = \delta^2 + \delta^6 + \delta^{10} = \lambda^{10} + \lambda^{-10} = [10]$, it follows that $B_0 \circ B_\delta$ has eigenvalues λ^{10} and λ^{-10}, with (left) eigenvectors $(\lambda^{1/2}, 1)$ and $(1, \lambda^{1/2})$, respectively. Since $I_0 \circ I_\delta \colon G_\alpha \to G_{\alpha B_0 \circ B_\delta}$, we see that $(B_0 \circ B_\delta)^j$ leaves invariant some G_α if and only if $(\lambda^{10})^j \in F$. So if $\lambda = \zeta^{q-1}$, $(\lambda^{10})^j \in F$ if and only if $5j \equiv 0 \pmod{q+1}$. This complete a proof of the following.

5.3 Theorem *Let $\delta = \lambda + \lambda^{-1}$, where $\lambda = \zeta^{q-1}$, ζ a primitive element for $E = GF(q^2)$. Then*

(i) *$I_0 \circ I_\delta$ permutes the lines through (∞) in a cycle of length $q+1$.*

(ii) *If $e \not\equiv 2 \pmod 4$ (that is, $q+1 \not\equiv 0 \pmod 5$), then $I_0 \circ I_\delta$ permutes the G_α in a cycle of length $q+1$.*

(iii) *If $e \equiv 2 \pmod 4$, $I_0 \circ I_\delta$ permutes the G_α in five cycles of length $(q+1)/5$.* □

5.4 Corollary *If $q = 2^e$ with $e \not\equiv 2 \pmod 4$, there is a unique Subiaco oval. It has stabiliser of order $2e$ inherited from $\mathcal{G}_0$.*

Proof: Uniqueness follows from Theorem 4.4 and Theorem 5.3(ii). Since $|\mathcal{G}_0| = 2e(q^2-1)$, $\mathcal{G}_0$ is transitive on all $q+1$ G_α, and the kernel $\mathcal{N}$ induces the identity map on the plane of the oval $\mathcal{O}_\alpha$, the corollary is proved. □

In a later paper [10] the action of the induced stabiliser of $\mathcal{O}_\alpha$ will be considered in greater depth in the case that $e \not\equiv 2 \pmod 4$. For the remainder of this work we concentrate on the case $e \equiv 2 \pmod 4$.

6 Subiaco Ovals with $q + 1 \equiv 0 \pmod 5$

Let $e \equiv 2 \pmod 4$, $\delta = \omega \in F$ with $\omega^2 + \omega + 1 = 0$. So $L = GF(2)(\delta) = GF(4)$, and $r = [F : L]$ implies that $e = 2r$ with r odd. Recall the following involutions from Eqs.(8) and (9).

$$\text{(i)} \quad I_\infty \colon (\alpha, c, \beta) \mapsto (\alpha P, g_\omega(\alpha) + c, (\beta + \omega^2\alpha)P), \tag{49}$$

$$\text{(ii)} \quad I_1 \colon (\alpha, c, \beta) \mapsto (\beta P, c + \alpha \circ \beta, \alpha P),$$

with the immediate consequences

(iii) $I_\infty \circ I_1\colon (\alpha, c, \beta) \mapsto (\beta + \omega^2\alpha, c + g_\omega(\alpha) + \alpha\circ\beta, \alpha)$,

(iv) $I_\infty \circ I_1\colon (a\alpha, c, b\alpha) \mapsto ((b + \omega^2 a)\alpha, c + a g_\omega(\alpha), a\alpha)$.

It is clear from Eq.(49)(iv) that $I_\infty \circ I_1$ leaves invariant each G_α, $\alpha \in PG(1,q)$. It is also easy to check that $I_\infty \circ I_1$ is a collineation of order 5. And clearly Gal (F/L) provides a group of order r stabilising each G_α, and the kernel provides an additional factor of order $q-1$. This provides the following.

6.1 Lemma *$\langle I_\infty \circ I_1, \mathrm{Gal}\,(F/L), \mathcal{N}\rangle$ is a group of order $5r(q-1)$ stabilising G_α for each $\alpha \in PG(1,4)$. Hence the orbit containing G_α has length at most $4(q+1)/5$.* □

6.2 Lemma *The stabiliser in $\mathcal{G}_0$ of $G_{(1,1)}$ is $\bigcup\{\mathcal{H}I_s \mid s \in \tilde{L}\}$ of order $(q-1)10e$, so the $\mathcal{G}_0$-orbit Ω_1 containing $G_{(1,1)}$ has length $(q+1)/5$.*

Proof: If $A_t = \begin{pmatrix} x_t & t^{1/2} \\ 0 & z_t \end{pmatrix}$ gives the Subiaco q–clan $\mathbf{C}$ in canonical form, then $A'_t = \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix} A_t \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix} = \begin{pmatrix} \omega x_t & t^{1/2} \\ 0 & \omega^2 z_t \end{pmatrix}$ gives the original q–clan $\mathbf{C}'$ studied in [1] (cf. Theorem 2.2 of the present work.)

The associated isomorphism of generalised quadrangles is given by

$$\theta \;=\; \theta(1, B, \mathrm{id}, \pi = \mathrm{id})\colon GQ(\mathbf{C}) \to GQ(\mathbf{C}') \qquad (50)$$

$$(\alpha, c, \beta) \mapsto (\alpha B, c, \beta B),\ B = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}.$$

Since $\theta\colon G_{(1,1)} \mapsto G_{(1,1)}$, φ is a collineation of $GQ(\mathbf{C}')$ leaving invariant $G_{(1,\omega)}$ if and only if $\theta \circ \varphi \circ \theta^{-1}$ is a collineation of $GQ(\mathbf{C})$ leaving invariant $G_{(1,1)}$. Clearly, $\theta\colon [A(\infty)] \mapsto [A'(\infty)]$. In [1] it is shown that the stabiliser $\mathcal{H}'$ of $[A'(\infty)]$ leaves invariant G'_α with $\alpha = (1,\omega)$, so in the present situation $\mathcal{H}$ must leave $G_{(1,1)}$ invariant. (We checked that this does indeed hold, but the details in the canonical case seem rather more tedious than those in [1].) But now, as in [1], it is easy to check that the full stabiliser of $G_{(1,1)}$ is $\bigcup\{\mathcal{H}I_s \mid s \in \tilde{L}\}$. □

6.3 Lemma *$\mathcal{G}_0$ has exactly $q+1$ involutions, each fixing a unique G_α.*

Proof: We know that for each $s \in \tilde{F}$ there is a unique involution I_s fixing $[A(s)]$. Since $q+1$ is odd, any involution would have to fix some line $[A(s)]$. Hence $\mathcal{G}_0$ has just the involutions I_s. By considering the associated matrix B_s, we immediately find the following:

(i) I_∞ fixes only $G_{(1,1)}$. (51)

(ii) For $s \in F$, I_s fixes a unique G_α.

(a) I_s fixes $G_{(0,1)} \iff c(s) = 0 \iff s^5 + s^4 + \omega^2 s + 1 = 0$, (see Eq.(67)(iii) of [1]).

(b) I_s fixes only $G_{(c(s), a(s)+1)} \iff c(s) \neq 0$.

□

6.4 Theorem *$\mathcal{G}_0$ has two orbits on the G_α, the short orbit Ω_1 of length $(q+1)/5$ and containing $G_{(1,1)}$ and a long orbit Ω_2 of length $4(q+1)/5$.*

Proof: Since $\mathcal{G}_0$ acts on Ω_1 and $|\Omega_1| = (q+1)/5$ is odd, each of the $q+1$ involutions $I_s \in \mathcal{G}_0$ must fix some $G_\alpha \in \Omega_1$. Hence by Lemma 6.3 no I_s can fix any G_β not in Ω_1. Suppose Ω_2 is any $\mathcal{G}_0$-orbit on the G_α's other than Ω_1. The stabiliser of any $G_\beta \in \Omega_2$ must have odd order, implying that 4, the highest power of 2 dividing $|\mathcal{G}_0|$, must divide $|\Omega_2|$. By Theorems 4.4 and 5.3, $|\Omega_2| = k(q+1)/5$, with $1 \le k \le 4$. Since $(q+1)/5$ is odd, it must be that $k = 4$. □

6.5 Corollary *$\langle I_\infty \circ I_1, \mathrm{Gal}\,(F/L), \mathcal{N}\rangle$ is the full subgroup of $\mathcal{G}_0$ stabilising each G_α in Ω_2 with $\alpha \in PG(1,4)$.* □

Note: Theorem 6.4 improves Theorem 7.6 of [1].

For a given α, the oval $\mathcal{O}_\alpha$ obtained directly from G_α is

$$\mathcal{O}_\alpha = \{(1, g_t(\alpha), t^{1/2}) \in PG(2,q) \mid t \in F\} \cup \{(0,0,1)\}. \tag{52}$$

The semilinear map $T\colon (x,y,z) \mapsto (x^2, z^2, y^2)$ on $PG(2,q)$ replaces $\mathcal{O}_\alpha$ with

$$\mathcal{O}_\alpha^{(2)} = \{(1, t, h_\alpha(t)) \mid t \in F\} \cup \{(0,1,0)\}, \text{ with } h_\alpha(t) = \alpha A_t \alpha^T. \tag{53}$$

There are just two ovals we consider here.

$$\text{(i)} \quad \text{For } \alpha = (1,1),\ h_\alpha(t) = \frac{\omega^2(t^4+t)}{t^4+\omega^2t^2+1} + t^{1/2}, \tag{54}$$

$$\text{(ii)} \quad \text{For } \alpha = (0,1),\ h_\alpha(t) = \frac{t^3+t^2+\omega^2 t}{t^4+\omega^2t^2+1} + \omega t^{1/2}.$$

For $\alpha = (1,1)$, $\mathcal{O}_\alpha$ belongs to the short $\mathcal{G}_0$-orbit Ω_1 with length $(q+1)/5$. For $\alpha = (0,1)$, if $5 \not| r$, $\mathcal{O}_\alpha$ belongs to the long $\mathcal{G}_0$-orbit Ω_2. But if $5 \mid r$, it follows from computations in [1] that $\mathcal{O}_\alpha$ also belongs to the short orbit Ω_1.

Remark: In [10] it will be shown that when $\delta = \lambda + \lambda^{-1}$, $\lambda = \zeta^{q-1}$, ζ is a primitive element of $E = GF(q^2)$, then $(1, \delta^{1/2})$ is in the long orbit. But we postpone any further discussion of this example.

Direct computation with the formulae for $h_\alpha(t)$ in Eq.(54) provides the following information.

$$\text{(i)} \quad \text{If } \alpha = (1,1),\ h_\alpha(t) = t^2, \text{ for } t \in GF(4). \tag{55}$$

$$\text{(ii)} \quad \text{If } \alpha = (0,1),\ h_\alpha(t) = \omega^2 t^2, \text{ for } t \in GF(4).$$

We want to use Eq.(55) to write out explicitly the stabiliser of $\mathcal{O}_\alpha^{(2)}$ induced by $\mathcal{G}_0$. By Theorem 6.5, when $\alpha = (0,1)$ no $\theta \in \mathcal{G}_0$ stabilising G_α has companion automorphism $\sigma = 2$. So we first put $\alpha = (1,1)$ and apply both Eq.(46)(ii) and Lemma 6.2. Since elements of the kernel $\mathcal{N}$ induce the identity map on the $PG(2,q)$ containing $\mathcal{O}_{(1,1)}^{(2)}$, in Eq.(46)(ii) we may put $a = 1$, so $\bar{B} = B$ and $\Delta = 1$, and $\delta = \omega$.

Then for $\alpha = (1,1)$, $\alpha^\sigma \bar{B} \equiv \alpha$, so we obtain the following induced automorphisms of $G_{(1,1)}$.

$$\theta(\omega^{\sigma-1}, \bar{B}, \sigma, \pi)\colon (a\alpha, c, b\alpha) \mapsto \qquad (56)$$
$$(a^\sigma\alpha, \omega^{1-\sigma}c^\sigma + a^\sigma\sqrt{\alpha A_{\bar{0}}\alpha^T}, (\omega^{\sigma-1}b^\sigma + \bar{0}^{1/2}a^\sigma)\alpha).$$

So the induced map on $PG(2,q)$ preserving $\mathcal{O}^{(2)}_{(1,1)}$ is

$$\theta(\omega^{\sigma-1}, \bar{B}, \sigma, \pi)\colon (x,y,z) \mapsto (x^\sigma, \omega^{1-\sigma}z^\sigma + \bar{0}x^\sigma, \omega^{\sigma-1}z^\sigma + \bar{0}^2x^\sigma). \qquad (57)$$

Here for $\sigma \in \mathrm{Aut}\,F$, $\bar{0}$ is either solution of $\bar{0}^2 + \delta\bar{0} + \delta^{2-2\sigma} + 1 = 0$. Hence $\omega^\sigma = \omega$ implies $\bar{0} \in \{0, \omega\}$ and $\omega^\sigma = \omega^2$ implies $\bar{0} \in \{1, \omega^2\}$. So in any case $\bar{0}^4 = \bar{0}$. Put $\sigma = 2$ and $\bar{0} = 1$ to get the specific map

$$\psi\colon (x,y,z) \mapsto (x^2, \omega^2y^2 + x^2, \omega z^2 + x^2). \qquad (58)$$

Note: The involution $\varphi\colon (x,y,z) \mapsto (y,x,z)$ leaves invariant $\mathcal{O}^{(2)}_\alpha$ for $\alpha = (1,1)$, but not for $\alpha = (0,1)$. From Eq.(49)(iv),

$$\text{On the oval } \mathcal{O}^{(2)}_\alpha,\ I_\infty \circ I_1\colon (x,y,z) \mapsto (\omega x + y, x, z + x(\alpha A_\omega \alpha^T)). \qquad (59)$$

Then also using Eq.(55), we obtain,

On the oval $\mathcal{O}^{(2)}_{(1,1)}$ we have the following induced stabilising collineations, (60)

(i) $I_\infty \circ I_1\colon (x,y,z) \mapsto (\omega x + y, x, z + \omega^2 x)$

(ii) $I_\infty\colon (x,y,z) \mapsto (x, y + \omega x, z + \omega^2 x)$

$$\text{On the oval } \mathcal{O}^{(2)}_{(0,1)},\ I_\infty \circ I_1\colon (x,y,z) \mapsto (\omega x + y, x, z + \omega x). \qquad (61)$$

For $\alpha = (1,1)$, it is routine to verify that $h_\alpha(t+\omega) = h_\alpha(t) + \omega^2$, which can be used to give a direct verification that the collineation of Eq.(60)(ii) does stabilise $\mathcal{O}^{(2)}_{(1,1)}$. For $\alpha = (0,1)$, it is also routine to verify that $h_\alpha((t+\omega)^{-1}) = (h_\alpha(t) + \omega)(t+\omega)^{-1}$. This can be used to show directly that the map in Eq.(61) also stabilises $\mathcal{O}^{(2)}_{(0,1)}$.

We have essentially completed a proof of the following theorem:

6.6 Theorem *For $e \equiv 2 \pmod 4$, $\delta = \omega$ and $\alpha = (1,1)$, the complete group induced by $\mathcal{G}_0$ on $PG(2,q)$ and stabilising*

$$\mathcal{O}^{(2)}_{(1,1)} = \left\{(1, t, \frac{\omega^2(t^4+t)}{t^4 + \omega^2t^2 + 1} + t^{1/2}) \mid t \in F\right\} \cup \{(0,1,0)\},$$

has order $10e$ and is generated by the following three collineations:

(i) $\varphi\colon (x,y,z) \mapsto (y,x,z)$,

(ii) $\theta\colon (x, y, z) \mapsto (x, y + \omega x, z + \omega^2 x)$, *and*

(iii) $\psi\colon (x, y, z) \mapsto (x^2, x^2 + \omega^2 y^2, x^2 + \omega z^2)$. □

Note: $\theta \circ \varphi\colon (x, y, z) \mapsto (y + \omega x, x, z + \omega^2 x)$ has order 5.

6.7 Theorem *For $e \equiv 2 \pmod 4$, $5 \not| e$, $\delta = \omega$, and $\alpha = (0, 1)$, the complete group induced by $\mathcal{G}_0$ on $PG(2, q)$ and stabilising*

$$\mathcal{O}^{(2)}_{(0,1)} = \left\{(1, t, \frac{t^3 + t^2 + \omega^2 t}{t^4 + \omega^2 t^2 + 1} + \omega t^{1/2}) \mid t \in F\right\} \cup \{(0, 1, 0)\},$$

has order $5e/2$ and is generated by the following collineations:

(i) $\theta_\sigma\colon (x, y, z) \mapsto (x^\sigma, y^\sigma, z^\sigma)$, $\sigma \in \mathrm{Aut}\, F$ *with* $\omega^\sigma = \omega$,

(ii) $\theta \circ \varphi\colon (x, y, z) \mapsto (y + \omega x, x, z + \omega x)$. □

For $e \equiv 10 \pmod{20}$, $\mathcal{O}^{(2)}_{(0,1)}$ belongs to the short orbit Ω_1. So $\alpha = (1, \delta^{1/2})$ is used in [10] to compute the corresponding stabiliser of order $5e/2$.

What remains to be shown here is that in all cases with $e \equiv 2 \pmod 4$, the group stabilising $\mathcal{O}^{(2)}_\alpha$ and induced by $\mathcal{G}_0$ is the complete subgroup of $P\Gamma L(2, q)$ stabilising $\mathcal{O}^{(2)}_\alpha$.

From the proof of Theorem 6.4 we know that α (that is, G_α) is in the long orbit Ω_2 precisely if it is fixed by no involution I_s. So we may use Eq.(11) to recognize members of Ω_2. Moreover, each oval $\mathcal{O}^{(2)}_\alpha$ may be associated with an irreducible algebraic curve in $PG(2, q)$ of degree 10. Then a little algebraic geometry (viz., Bezout's theorem) and some classical group theory finish off the proof as follows.

We want to reindex the $\alpha \in PG(1, q)$ by $c \in \tilde{F}$ in the following way. For $c \in \tilde{F}$, put $\alpha_c = \left(\frac{\omega^2 + \omega c}{1 + c^{1/2} + \omega c}, \frac{\omega c}{1 + c^{1/2} + \omega c}\right)$. Clearly $1 + c^{1/2} + \omega c \neq 0$ for all $c \in F$. Then $\alpha_c = (1, 1)$ if and only if $c = \infty$, and for c, $d \in F$, $\alpha_c \equiv \alpha_d$ if and only if $c = d$. For $c = \omega$, $\alpha_c = (0, \omega^2) \equiv (0, 1)$. For $c \in \tilde{F} \setminus \{\infty, \omega\}$, $\alpha_c \equiv (1, c/(c + \omega))$. Index the ovals $\mathcal{O}^{(2)}_\alpha$ for $\alpha \in PG(1, q)$ so that $\mathcal{O}_c = \mathcal{O}^{(2)}_{\alpha_c}$, $c \in \tilde{F}$. Hence we have the following:

$$\begin{aligned} \mathcal{O}_\infty &= \{(1, t, f_\infty(t)) \mid t \in F\} \cup \{(0, 1, 0)\}, \text{ where} \\ & f_\infty(t) = \tfrac{\omega^2 t^4 + \omega^2 t}{t^4 + \omega^2 t^2 + 1} + t^{1/2}. \end{aligned} \tag{62}$$

Then for $c \in F$, using Eqs.(1), (2) and (53) we obtain

$$\begin{aligned} \mathcal{O}_c &= \{(1, t, f_c(t)) \mid t \in F\} \cup \{(0, 1, 0)\} \quad \text{where} \\ f_c(t) &= \left(\tfrac{\omega^2 + \omega c}{1 + c^{1/2} + \omega c}\right)^2 \left(\tfrac{\omega^2 t^4 + t^3 + t^2}{t^4 + \omega^2 t^2 + 1} + \omega t^{1/2}\right) \\ &\quad + \left(\tfrac{(\omega^2 + \omega c)\omega c}{1 + c + \omega^2 c^2}\right) t^{1/2} + \tfrac{\omega^2 c^2}{1 + c + \omega^2 c^2} \left(\tfrac{t^3 + t^2 + \omega^2 t}{t^4 + \omega^2 t^2 + 1} + \omega t^{1/2}\right) \\ &= \tfrac{1}{1 + c + \omega^2 c^2} \left(\tfrac{(1 + \omega c^2) t^4 + \omega t^3 + \omega t^2 + \omega c^2 t}{t^4 + \omega^2 t^2 + 1} + (\omega^2 + c + \omega^2 c^2) t^{1/2}\right). \end{aligned} \tag{63}$$

The choice of α_c may seem unnecessarily complicated, but it has the following interesting consequences.

6.8 Lemma *Let* $g \in PGL(3,q)$ *be defined by*

$$g\colon (x,y,z) \mapsto (y, x+\omega y, \omega^2 y + z).$$

Then g *is a collineation of order 5 stabilising* $\mathcal{O}_c$ *for every* $c \in \tilde{F}$.

Proof: Using Eq.(49) we see that $I_1 \circ I_\infty\colon (\alpha, c, \beta) \mapsto (\beta, c+\alpha\circ\beta+g_\omega(\beta P), \alpha+\omega^2\beta)$, and in particular, $I_1 \circ I_\infty\colon (a\alpha, c, b\alpha) \mapsto (b\alpha, c+g_\omega(b\alpha P), (a+\omega^2 b)\alpha)$. Hence $I_1 \circ I_\infty$ is a collineation of order 5 leaving G_α invariant for each $\alpha \in PG(1,q)$. Use the semilinear map $T\colon (x,y,z) \mapsto (x^2, y^2, z^2)$ mapping $\mathcal{O}_\alpha$ to $\mathcal{O}_\alpha^{(2)}$ to transfer the action of $I_1 \circ I_\infty$ to the map

$$g_\alpha\colon (x,y,z) \mapsto (y, x+\omega y, z + y\alpha(PA_\omega P^T)\alpha^T)$$

which stabilises $\mathcal{O}_\alpha$. Note that $PA_\omega P^T \equiv A_\omega = \begin{pmatrix} \omega & \omega^2 \\ 0 & \omega \end{pmatrix}$. For $\alpha = (1,1)$, $\alpha A_\omega \alpha^T = \omega^2$. Now put $\alpha = \alpha_c$ and compute

$$\alpha A_\omega \alpha^T = \left(\frac{\omega+\omega^2c^2}{1+c+\omega^2c^2}\right)\omega + \left(\frac{(\omega^2+\omega c)\omega c}{1+c+\omega^2c^2}\right)\omega^2 + \left(\frac{\omega^2c^2}{1+c+\omega^2c^2}\right)\omega = \omega^2.$$

Hence for every $c \in \tilde{F}$, g_{α_c} is the map g of the Lemma. □

6.9 Lemma

(i) $\mathcal{O}_\infty$ *is always in the short orbit* Ω_1.

(ii) *For* $c \in F$, $\mathcal{O}_c \in \Omega_2$ *if and only if*

$$p_c(x) = x^5 + (\omega^2c^2+\omega^2)x^4 + (\omega^2c^2+1)x + 1 = 0,$$

has no root in F.

(iii) *There is a* $c \in F \setminus GF(4)$ *for which both* $p_c(x) = 0$ *and*

$$p_{(\omega^2c^2+\omega^2)}(x) = x^5 + (c^4+\omega)x^4 + c^4x + 1 = 0,$$

have no root in F.

Proof: We have already seen that (i) holds. For $c = \omega$, $p_\omega(x) = x^5 + x^4 + \omega^2 x + 1$, which by [1] is irreducible if and only if $\mathcal{O}_{(0,1)} \in \Omega_2$ if and only if 5 does not divide e. For $\omega \neq c \in F$, $\alpha_c \equiv (1, c/(c+\omega))$. So put $d = c/(c+\omega)$. Then

$$\begin{aligned}
\mathcal{O}_c \in \Omega_2 \quad &\Longleftrightarrow \quad \alpha_c \in \Omega_2 \\
&\Longleftrightarrow \quad (1,d) \in \Omega_2 \\
&\Longleftrightarrow \quad (1,d) \text{ is fixed by no involution } I_s, \\
&\Longleftrightarrow \quad (1,d)B_s \not\equiv (1,d) \text{ for all } s \in F, \\
&\qquad \text{where } B_s = \begin{pmatrix} a(s) & b(s) \\ c(s) & a(s) \end{pmatrix} \text{ from Eq.(11),}
\end{aligned}$$

$$\begin{aligned}
&\iff b(s) + da(s) \neq d(a(s) + dc(s)) \text{ for all } s \in F, \\
&\iff b(s) \neq d^2 c(s) \text{ for all } s \in F, \\
&\iff d^2 \neq \frac{b(s)}{c(s)} = \frac{s^5 + \omega^2 s^4 + s + 1}{s^5 + s^4 + \omega^2 s + 1} \text{ for all } s \in F, \\
&\iff s^5(1 + d^2) + s^4(d^2 + \omega^2) + s(1 + d^2\omega^2) + d^2 + 1 = 0 \\
&\qquad \text{has no solution } s \in F, \\
&\iff s^5 + \left(\frac{d^2 + \omega^2}{1 + d^2}\right) s^4 + \left(\frac{1 + d^2\omega^2}{1 + d^2}\right) s + 1 = 0 \\
&\qquad \text{has no solution } s \in F, \\
&\iff p_c(s) \neq 0 \text{ for all } s \in F, \\
&\qquad \text{where } c = \frac{d\omega}{1 + d}, \text{ that is, } d = \frac{c}{c + \omega}.
\end{aligned}$$

This completes the proof of (ii).

Hence $p_c(x) = 0$ has no root in F for $4(q + 1)/5$ values of $c \in F$. Moreover, $c \mapsto \omega^2 c^2 + \omega^2$ is a bijection on F, so $p_{(\omega^2 c^2 + \omega^2)}(x) = 0$ has no root in F also for $4(q + 1)/5$ values of c. This implies that both $p_c(x) = 0$ and $p_{(\omega^2 c^2 + \omega^2)}(x) = 0$ have no root for at least $(3q + 2)/5$ values of c, from which (iii) follows. □

Define the conic $\mathcal{O}\colon xy = z^2$, that is,

$$\mathcal{O} = \{(1, t, t^{1/2}) \mid t \in F\} \cup \{(0, 1, 0)\}.$$

6.10 Lemma

(i) *$\mathcal{O}_\infty \cap \mathcal{O} = PG(2, 4) \cap \mathcal{O}$,*

(ii) *For c satisfying condition (iii) of Lemma 6.9, $\mathcal{O}_c \in \Omega_2$ and $\mathcal{O}_c \cap \mathcal{O} = PG(2, 4) \cap \mathcal{O}$.*

Proof: For (i), $(\mathcal{O}_\infty \setminus \{(0, 1, 0)\}) \cap \mathcal{O} = \{(1, t, f_\infty(t)) \mid f_\infty(t) = t^{1/2}\}$. Clearly $f_\infty(t) = t^{1/2}$ if and only if $t \in GF(4)$. Similarly, if c satisfies condition (iii) of Lemma 6.9, then $\mathcal{O}_c \in \Omega_2$ and $(\mathcal{O}_c \setminus \{(0, 1, 0)\}) \cap \mathcal{O} = \{(1, t, f_c(t)) \mid f_c(t) = t^{1/2}\}$. Using Eq.(63) we may compute that $f_c(t) = t^{1/2}$ if and only if $\omega^2 t(t^3 + 1)(t^5 + (c^4 + \omega)t^4 + c^4 t + 1) = 0$, proving (ii). □

For each $c \in \tilde{F}$ we may define the hyperoval $\mathcal{H}_c = \mathcal{O}_c \cup \{(0, 0, 1)\}$, and with a natural abuse of language refer to $\mathcal{H}_c$ belonging to Ω_1 or Ω_2. For example, $\mathcal{H}_\infty \in \Omega_1$. And for $c = c_0$ satisfying condition (iii) of Lemma 6.9, $\mathcal{H}_{c_0} \in \Omega_2$. From now on fix $c = c_0$ to be such an element.

By the results in [12] the hyperovals $\mathcal{H}_\infty$ and $\mathcal{H}_{c_0}$ are inequivalent for $q = 64$ and have full collineation stabilisers of order 60 and 15, respectively. So from now on we assume that $q \geq 1024$.

Using the ideas of [8] we shall show that $\mathcal{H}_\infty$ and $\mathcal{H}_{c_0}$ are the pointsets of two absolutely irreducible degree ten algebraic curves in $PG(2, q)$.

6.11 Lemma *For both $c = \infty$ and $c = c_0$, $\mathcal{H}_c$ is the pointset of an absolutely irreducible degree ten algebraic curve $\mathcal{C}$ in $PG(2, q)$ having $(0, 0, 1)$ as its only singular point. The multiplicity of $(0, 0, 1)$ for $\mathcal{C}$ is 8, and in $PG(2, q^2)$ there are two* *tangent lines for $\mathcal{C}$ at $(0,0,1)$. The tangent lines are $Q = [\eta,1,0]^T\colon \eta x + y = 0$ and $\bar{Q} = [\eta^q,1,0]^T\colon \eta^q x + y = 0$, where $\eta \in GF(q^2)\setminus GF(q)$ satisfies $\eta^{q+1} = 1$ and $\eta^q + \eta = \omega$.*

Proof: For $c \in \{\infty, c_0\}$, write $d = c/(c+\omega)$, so $d \in \{1, c_0/(c_0+\omega)\}$. In particular, we are avoiding the case $c = \omega$ with $d = \infty$. Put $m_c = \left(\frac{\omega^2+\omega c}{1+c^{1/2}+\omega c}\right)^2$. So $m_c \neq 0$, $m_\infty = 1$, and $\alpha_c = (m_c)^{1/2}(1,d)$. Then $\mathcal{H}_c = \{(1,t,f_c(t)) \mid t \in F\} \cup \{(0,1,0),(0,0,1)\}$ is projectively equivalent to $\bar{\mathcal{H}}_c = \{(1,t,f_c(t)/m_c) \mid t \in F\} \cup \{(0,1,0),(0,0,1)\}$. Here

$$\begin{aligned}\frac{f_c(t)}{m_c} = f(t,d) &= \left(\frac{\omega^2t^4+t^3+t^2}{t^4+\omega^2t^2+1} + \omega t^{1/2}\right) + dt^{1/2} + d^2\left(\frac{t^3+t^2+\omega^2 t}{t^4+\omega^2t^2+1} + \omega t^{1/2}\right)\\ &= \frac{\omega^2t^4+(1+d^2)(t^3+t^2)+\omega^2d^2t}{t^4+\omega^2t^2+1} + (\omega + d + \omega d^2)t^{1/2}.\end{aligned}$$

Define $g_c \in PGL(3,q^2)$ by $g_c\colon (x,y,z) \mapsto (x,y,m_c z)$. So $g_c\colon \bar{\mathcal{H}}_c \mapsto \mathcal{H}_c$, and g_c fixes the two points $(0,1,0)$ and $(0,0,1)$. We show that $\bar{\mathcal{H}}_c$ satisfies the conclusions of the Lemma. Since g_c also fixes the lines Q, $\bar{Q}$, it will follow that $\mathcal{H}_c$ satisfies the same conclusions.

The point $(1,t,f(t,d)) \equiv (1,y,z)$ satisfies

$$z = \frac{\omega^2y^4+(1+d^2)(y^3+y^2)+d^2\omega^2y}{y^4+\omega^2y^2+1} + (\omega+d+\omega d^2)y^{1/2}.$$

Multiply through by $y^4+\omega^2y^2+1$, square both sides, and then make the resulting equation homogeneous in x, y, z to get the algebraic curve $\mathcal{C}_d\colon h_d(x,y,z) = 0$, where

$$\begin{aligned}h_d(x,y,z) &= (z^2 + (\omega^2+d^2+\omega^2d^4)xy)(y^2+\omega xy+x^2)^4\\ &\quad + \omega x^2y^8 + \omega d^4x^8y^2 + (1+d^4)(x^4y^6+x^6y^4).\end{aligned} \tag{64}$$

By construction, for all $t \in F$, $(1,t,f(t,d)) \in \mathcal{C}_d$. But in fact it is routine to check that the pointset of $\mathcal{C}_d$ is exactly the hyperoval $\bar{\mathcal{H}}_c$ (always $d = c/(c+\omega)$). So $|\mathcal{C}_d| = q+2$, and we want to prove that $h_d(x,y,z)$ is absolutely irreducible.

First compute $\frac{\partial h_d}{\partial x} = (\omega^2+d^2+\omega^2d^4)y(y^2+\omega xy+x^2)^4$, $\frac{\partial h_d}{\partial y} = (\omega^2+d^2+\omega^2d^4)x(y^2+\omega xy+x^2)^4$, and $\frac{\partial h_d}{\partial z} = 0$. Since $\omega^2+x+\omega^2x^2$ is irreducible over $GF(4)$, and hence over F, $\omega^2+d^2+\omega^2d^4 \neq 0$ for all $d \in F$. It follows readily that the only singular point of $\mathcal{C}_d$ is $(0,0,1)$ with multiplicity 8 and $(0,0,1)$ has two tangents Q, $\bar{Q}$ in the quadratic extension of F, where the product of Q and $\bar{Q}$ is $y^2+\omega xy+x^2 = 0$. If one of Q, $\bar{Q}$ is a component of $\mathcal{C}_d$, so is the other, and in this case $y^2+\omega xy+x^2$ must divide $h_d(x,y,z)$. We now show that this is not the case. Put $y^2 = \omega xy + x^2$, and hence $y^4 = x^3(y+\omega x)$, $y^6 = x^5y$, $y^8 = \omega x^8 + \omega yx^7$ into $h_d(x,y,z)$. After a little simplification, $h_d(x,y,z) = x^9(\omega^2(1+d^4)y + x)$, which is not the zero polynomial. This proves that neither tangent to $\mathcal{C}_d$ at $(0,0,1)$ is a component of $\mathcal{C}_d$.

Now suppose that $\mathcal{C}_d$ has components $C_1,\ldots,C_l$, $l > 1$, with $\deg C_i = k_i$, and suppose $(0,0,1)$ has multiplicity t_i for C_i. So $\sum k_i = 10$ and $\sum t_i = 8$. If some

$t_i = k_i$, then $t_i = k_i = 1$ and C_i is a line. But in this case C_i must be tangent to C_i at $(0,0,1)$, so C_i is tangent to $\mathcal{C}_d$ at $(0,0,1)$, contradicting the previous paragraph. So the only possibility is that there are exactly two components C_1 and C_2 with $t_1 = k_1 - 1$ and $t_2 = k_2 - 1$.

First suppose C_1 and C_2 are defined over F, and $(0,0,1)$ is a $(k_i - 1)$-tuple point for C_i, $i = 1$, 2. Any tangent to C_i at $(0,0,1)$ is tangent to $\mathcal{C}_d$ and not defined over F. So any line (over F) through $(0,0,1)$ meets C_i in a second point, which implies $|C_i| \geq q+2$. Since any point of $C_1 \cap C_2$ is a singular point for $\mathcal{C}_d$ clearly $|C_1 \cup C_2| \geq 2(q+2) - 1 > q+2 = |\mathcal{C}_d|$, an impossibility.

So we may suppose C_1 and C_2 are not defined over $F = GF(q)$, but over some $GF(q^r)$, $r > 1$. Let $\mathrm{id} \neq \sigma \in \mathrm{Gal}\,(GF(q^r)/GF(q))$. Then $C_1^\sigma = C_2$, so $\deg C_1 = \deg C_2 = 5$. By Lemma 10.1.1 of [3], $|C_i| \leq 5^2$, so $|\mathcal{C}_d| \leq 49$. Since $q > 64$ we have a contradiction. □

Acknowledgment: We thank our friend and colleague J. A. Thas for explaining to us how the preceding proof should go.

For the remainder of this section write $\mathcal{H}_1 = \mathcal{H}_\infty$ and $\mathcal{H}_2 = \mathcal{H}_{c_0}$. Then for $i = 1$, 2, let $G_i = P\Gamma L(3,q)_{\mathcal{H}_i}$ be the full collineation stabiliser of the hyperoval $\mathcal{H}_i$.

Let $g \in P\Gamma L(3,q)$ have a companion automorphism $\sigma \in \mathrm{Aut}\,(F)$. Let $h \in F[x,y,z]$ be a homogeneous polynomial. The **image**, h^g, of h under g is defined by:

$$h^g = g \circ h \circ \sigma^{-1},$$

and for $d = 1 \in F$, write $h_1 = h_d(x,y,z)$ (since $g_\infty = \mathrm{id}$), and for $d = c_0/(c_0+\omega)$, let h_2 be the image of $h_d(x,y,z)$ under $g_{c_0}^{-1}$. Then we have $\mathcal{H}_i = \{(x,y,z) \in PG(2,q) \mid h_i(x,y,z) = 0\}$, $i = 1$, 2.

6.12 Lemma

$$G_i = \{g \in P\Gamma L(3,q) \mid h_i^g = \lambda h_i, \lambda \in GF(q) \setminus \{0\}\}, \text{ for } i = 1,\ 2.$$

Proof:

($\supseteq$) Let $g \in P\Gamma L(3,q)$ with $h_i^g = \lambda h_i$, $\lambda \in GF(q) \setminus \{0\}$ for $i = 1$, 2. Then g fixes the set of points (x,y,z) such that $h_i(x,y,z) = 0$. But these are just the points of the hyperoval $\mathcal{H}_i$ for $i = 1$, 2.

($\subseteq$) Let $g \in G_i$ and suppose $h_i^g \neq h_i$. If $\mathcal{C}_i$: $h_i(x,y,z) = 0$, $i = 1$, 2, then the pointsets of $\mathcal{C}_i$ and ${\mathcal{C}_i}^g$ coincide. By Bezout's Theorem, it follows that the number of points of $\mathcal{C}_i \cap \mathcal{C}_i^g$, counted according to multiplicity, is at most 100. This is contrary to our hypothesis that $q \geq 1024$. □

Since $(0,0,1)$ is the unique singular point of $\mathcal{C}_i$, $i = 1$, 2, G_i must fix $(0,0,1)$ and the set $\{Q, \bar{Q}\}$ of tangents. Also, since $(0,0,1)$ is on $\mathcal{H}_i$, no nontrivial element of G_i can have $(0,0,1)$ as its centre, $i = 1$, 2. Hence G_1 and G_2 fix $(0,0,1)$ but not linewise, and so act faithfully on the quotient space $PG(2,q)/(0,0,1)$.

We are now ready to prove the final theorem of this section.

6.13 Theorem *The hyperovals $\mathcal{H}_1$ and $\mathcal{H}_2$ in $PG(2,q)$, $q = 2^e$, are inequivalent for $e \equiv 2 \pmod 4$. The full collineation stabiliser of $\mathcal{H}_1$ in $P\Gamma L(3,q)$ is isomorphic to $C_5 \rtimes C_{2e}$, and the full collineation stabiliser of $\mathcal{H}_2$ in $P\Gamma L(3,q)$ is isomorphic to $C_5 \rtimes C_{e/2}$.*

Proof: Let $h \in PGL(2,q)$ with $|h| = q+1$. Then $\langle h \rangle$ is a Singer cycle of $PG(1,q)$, so $\langle h \rangle = C_{q+1}$ acts regularly on $PG(1,q)$. Since h is induced by an invertible 2×2 matrix over F with (conjugate) eigenvalues in $GF(q^2) \setminus GF(q)$, we have $\langle h \rangle$ fixing a conjugate pair of points, say $\{P, \bar{P}\}$. As $N_{P\Gamma L(2,q)}(\langle h \rangle)$ permutes the fixed points of $\langle h \rangle$, $N_{P\Gamma L(2,q)}(\langle h \rangle)$ stabilises the conjugate pair $\{P, \bar{P}\}$. Hence $N_{P\Gamma L(2,q)}(\langle h \rangle) \leq P\Gamma L(2,q)_{\{P,\bar{P}\}}$. And since $P\Gamma L(2,q)$ acts transitively on conjugate pairs of points, then replacing h by a conjugate if necessary,

$$N_{P\Gamma L(2,q)}(\langle h \rangle) \leq P\Gamma L(2,q)_{\{Q,\bar{Q}\}},$$

where $\{Q, \bar{Q}\}$ is the pair of conjugate tangent lines (which are conjugate points in the quotient space) to the hyperovals at $(0,0,1)$ in $PG(2,q)$. By [5] and [4, Theorem II.7.3], we have

$$N_{P\Gamma L(2,q)}(\langle h \rangle) = C_{q+1} \rtimes C_{2e}.$$

But the order of $P\Gamma L(2,q)_{\{Q,\bar{Q}\}}$ is $2(q+1)e$, so by comparing orders

$$C_{q+1} \rtimes C_{2e} = P\Gamma L(2,q)_{\{Q,\bar{Q}\}}.$$

Hence both G_1 and G_2 are subgroups of $C_{q+1} \rtimes C_{2e}$. From this, for the g from Lemma 6.8, we have that $\langle g \rangle$ is normal in $PGL(2,q)_{\{Q,\bar{Q}\}}$, since $\langle g \rangle$ is characteristic in $\langle h \rangle$, which is normal in $PGL(2,q)_{\{Q,\bar{Q}\}}$. Since $q^2 + q + 1 \equiv 1 \pmod 5$, g has a unique fixed line, namely $x + y + \omega^2 z = 0$. Since G_1 and G_2 normalise $\langle g \rangle$, they fix $x + y + \omega^2 z = 0$.

Let $H_i = G_i \cap C_{q+1}$, for $i = 1, 2$. We have H_1 and H_2 fixing both tangent lines Q and $\bar{Q}$, so fixing their product $x^2 + \omega xy + y^2 = 0$. They also fix the line $x + y + \omega^2 z = 0$, so fix $x^2 + y^2 + \omega z^2 = 0$. Let $\mathcal{P}$ be the pencil generated by these two. The group induced on the set of conics of $\mathcal{P}$ by the stabiliser in $PGL(3,q)$ of $\mathcal{P}$ is cyclic of order $q-1$. Since $(q+1, q-1) = 1$ each H_i fixes every conic in $\mathcal{P}$. So for $i = 1, 2$, H_i fixes the conic $\mathcal{O}\colon xy = z^2$, so it fixes $\mathcal{H}_i \cap \mathcal{O} = \mathcal{O} \cap PG(2,4)$, by Lemma 6.10.

Now H_i acts semiregularly on $PG(2,q) \setminus \{(0,0,1)\}$ for $i = 1, 2$. All points (except the fixed point) have orbits of length $|H_i|$. But since H_i fixes $\mathcal{O} \cap PG(2,4)$ and acts semiregularly on $\mathcal{O}$, we have $|H_i|$ dividing $|\mathcal{O} \cap PG(2,4)| = 5$. Hence $|H_i| = 1$ or 5. But $\langle g \rangle \leq H_i$, so $H_i = \langle g \rangle$ for $i = 1, 2$. Hence G_1 and G_2 are subgroups of $\langle g \rangle \rtimes C_{2e}$.

From Theorem 6.6 we have the induced group of $\mathcal{H}_1$ having order $10e$ so we have $G_1 = \langle g \rangle \rtimes C_{2e}$.

As $q + 1 \equiv 0 \pmod 5$ with $q = 2^e$, then $e = 2r$ where r is odd, so $e/2$ is odd. We now show that $G_2 \leq \langle g \rangle \rtimes C_{e/2}$. The subgroup $C_5 \rtimes C_4$ contains all the involutions of $\langle g \rangle \rtimes C_{2e}$ (five in total) since $e/2$ is odd. These five involutions are conjugate under $\langle g \rangle$. If G_2 contains an involution then it will contain the involution φ from Theorem 6.6. Since

$$\varphi\colon \{(1, t, f_2(t)) \mid t \in F\} \mapsto$$
$$\{(t, 1, f_2(t)) \mid t \in F\} = \{(1, u, uf_2(u^{-1})) \mid u \in F\},$$

it follows that if G_2 contains an involution, then $f_2(t) = tf_2(t^{-1})$ for all $t \in F$, but this is not so. Hence 2 does not divide $|G_2|$. That is, $G_2 \leq \langle g \rangle \rtimes C_{e/2}$.

From Theorem 6.7 we have the induced group of $\mathcal{H}_2$ has order $5e/2$. Hence $G_2 = \langle g \rangle \rtimes C_{e/2}$.

This completes the proof of the theorem. □

Remark: In the case of $\mathcal{H}_1$ the statement of Theorem 6.6 can be sharpened slightly. Not only does $\theta \circ \varphi$ have order 5, but $\varphi \circ \psi \neq \psi \circ \varphi$ while $\theta \circ \psi = \psi \circ \theta$. Moreover, ψ has order $2e$ and $\psi^e = \theta$. So

$$\langle \varphi, \theta, \psi \rangle = \langle \theta \circ \varphi \rangle \rtimes \langle \psi \rangle \cong C_5 \rtimes C_{2e}.$$

For $e \not\equiv 2 \pmod 4$ and $q \geq 32$, it is also true that the stabiliser of order $2e$ of the Subiaco oval induced by the collineation group of the GQ is the complete oval stabiliser (cf. [8]).

7 Remarks on the Subiaco hyperovals

For $q = 16$ the Subiaco hyperoval is a Lunelli-Sce hyperoval. For $q = 32$, the Subiaco hyperoval is a Payne hyperoval. For $q = 64$, they are the hyperovals discovered by Penttila and Pinneri [12], with groups of orders 15 and 60. For $q = 128$, 256, they are the hyperovals which were also discovered by Penttila and Royle [13].

By the results on the stabilisers of the Subiaco hyperovals, the only known infinite family of hyperovals which could intersect with the family of Subiaco hyperovals is the family of Payne hyperovals, for q not square (see [12] for stabilisers of the known hyperovals and [8] for the stabiliser of the Subiaco hyperovals). In this case, with $q = 2^e$, and e odd, both the Payne and the Subiaco hyperoval in $PG(2, q)$ have a stabiliser in $P\Gamma L(3, q)$ that is cyclic of order $2e$, so they could conceivably be equivalent. However, the Subiaco hyperoval is an absolutely irreducible curve of degree 10 and the Payne hyperoval is associated with an absolutely irreducible curve of degree 6 [14]. By Bezout's theorem, for $q \geq 128$, it follows that the Subiaco hyperoval is not a Payne hyperoval. Of course, for $q = 32$, it is a Payne hyperoval.

References

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

[2] W. Cherowitzo, T. Penttila, I. Pinneri, and G. Royle, Flocks and ovals, Geom. Ded., To appear (1995).

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

[4] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.

[5] W.M. Kantor, *Classical groups from a non-classical viewpoint*, Mathematical Institute (Oxford Lectures 1978), Oxford, 1979.

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

[7] C.M. O'Keefe and T. Penttila, Symmetries of arcs, *J.C.T (A)*, To appear (1991).

[8] C.M. O'Keefe and J.A. Thas, Collineations of some hyperovals, In preparation (1994).

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

[10] S.E. Payne, A tensor product action on q–clan geometries with $q = 2^e$, *Linear algebra and its applications,* To appear.

[11] S.E. Payne and J.A. Thas, *Finite generalized quadrangles*, Pitman, 1984.

[12] T. Penttila and I. Pinneri, Irregular hyperovals in $PG(2, 64)$, *J. of Geometry*, **51** (1994), 89–100.

[13] T. Penttila and G.F. Royle, Hyperovals in projective planes of small order, *J. of Geometry*, To appear (1994).

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

Addresses of the authors:
Stanley E. Payne, Department of Mathematics, CU-Denver Campus Box 170, PO Box 173364, Denver Colorado 80217-3364 USA.
e-mail: spayne@carbon.cudenver.edu
Tim Penttila, Department of Mathematics, University of Western Australia, Nedlands 6009, Western Australia, Australia.
e-mail: penttila@maths.uwa.edu.au
Ivano Pinneri, Department of Mathematics, University of Western Australia, Nedlands 6009, Western Australia, Australia.
e-mail: ivano@maths.uwa.edu.au