Certain Roman and flock generalized quadrangles have nonisomorphic elation groups

George Havas
ARC Centre for Complex Systems
School of Information Technology and Electrical Engineering
The University of Queensland, Queensland 4072, AUSTRALIA
Email: havas@itee.uq.edu.au

C.R. Leedham-Green
School of Mathematical Sciences, Queen Mary
University of London, E1 4NS, UNITED KINGDOM
Email: c.r.leedham-green@qmul.ac.uk

E.A. O'Brien
Department of Mathematics, University of Auckland
Private Bag 92019, Auckland, NEW ZEALAND
Email: obrien@auckland.ac.nz

Michael C. Slattery
Department of Mathematics, Statistics and Computer Science
Marquette University, P.O. Box 1881
Milwaukee WI 53201-1881, USA
Email: mikes@mscs.mu.edu

Abstract

We prove that the elation groups of a certain infinite family of Roman generalized quadrangles are not isomorphic to those of associated flock generalized quadrangles.

1 Introduction

A finite generalized quadrangle with parameters (s, t) is a point-line incidence structure $S = (P, B, I)$ in which P and B are disjoint nonempty sets of objects called *points* and *lines* respectively and for which I is a symmetric point-line incidence relation satisfying the following axioms.

- Each point is incident with $t+1$ lines, and two distinct points are incident with at most one line.
- Each line is incident with $s+1$ points, and two distinct lines are incident with at most one point.
- If p is a point and L is a line not incident with p, then there is a unique point-line pair (q, M) such that $pIMIqIL$.

It is immediate that there is a point-line duality, and the point-line dual of a generalized quadrangle is a generalized quadrangle. Comprehensive definitions and results about generalized quadrangles are given in the monograph [7] and some newer results appear in the lecture notes [6].

Let S be a finite generalized quadrangle with parameters (s, t) and let p be a point of S. An elation about the point p is a collineation of S that fixes each line through p and fixes no point not collinear with p, or is the identity collineation. If there is a group of s^2t elations acting regularly on the points of S not collinear with p then S is called an elation generalized quadrangle. Relationships between elation generalized quadrangles, 4-gonal families and particular types of quadrangles called flock generalized quadrangles are covered in [7, 8, 6].

Payne [5] introduced a new infinite family of generalized quadrangles which he called *Roman*. The basis for his construction were flock generalized quadrangles having parameters (q^2, q), where q is a prime-power. The point-line dual has parameters (q, q^2) and abelian elation group. He then considered a translation dual of the point-line dual, giving generalized quadrangles having parameters (q, q^2). Finally, he took the point-line dual of these, giving Roman generalized quadrangles with parameters (q^2, q).

Payne showed geometrically that the Roman generalized quadrangles are distinct from the flock quadrangles for $q = 3^k$ where $k \geq 3$. (For all other characteristics the translation dual is known to be isomorphic to the original.) Indeed, he claimed [5] that they were distinguished by their elation groups and:

> That this is true really does follow from our computations for $q > 9$.

In his talk at the "Finite Geometries, Groups and Computation" conference [2], Payne asked for a proof that the elation groups are not isomorphic. He also discusses this question in his lecture notes [6, Chapter 7].

Their nonisomorphism has an important impact on a major problem in geometry: namely which groups admit a 4-gonal family? The answer to this question will contribute to the characterization of the underlying groups of generalized quadrangles. We refer the interested reader to [6] for further details.

Motivated by the challenge problem posed at the Conference, we now present a proof that the elation groups are not isomorphic. Our proof is theoretical, but it was inspired by the insight gained from detailed group computations for the smallest of these groups conducted using the computer algebra systems GAP [3] and MAGMA [1]. Our approach is explained and comprehensive information about our calculations is given in [4]. Briefly, we investigated the smallest interesting case, showed that the groups could be distinguished, then generalized the result.

In Section 2 we define the elation groups and in Section 3 we prove that the elation groups are not isomorphic. We also describe (see Theorem 3.8) the automorphism group of the elation group of the flock generalized quadrangle.

2 The elation groups

Payne [5, 6] lists multiplication rules for elation groups of flock generalized quadrangles and Roman quadrangles with parameters (q^2, q). We follow his description.

Let $F = \mathrm{GF}(q)$, $q = p^k$, p an odd prime. Let $f : F^2 \times F^2 \to F$ be a symmetric, biadditive map. Further, suppose that if $(0,0) \neq \alpha \in F^2$, then $\{\beta \in F^2 : f(\alpha, \beta) = 0\}$ is an additive subgroup of F^2 with order q. For a fixed nonzero $\alpha \in F^2$, this implies that $|\{f(\alpha, \beta) : \beta \in F^2\}| = q$ also. Such an f is called a *nonsingular pairing*.

Let $G = \{(\alpha, \beta, c) : \alpha \in F^2, \beta \in F^2, c \in F\}$. Clearly G has q^5 elements. We now impose a group structure on the set G using a nonsingular pairing.

Let $f : F^2 \times F^2 \to F$ be a given nonsingular pairing. Define a binary operation $\otimes$ on G by

$$(\alpha, \beta, c) \otimes (\alpha', \beta', c') \;=\; (\alpha + \alpha', \beta + \beta', c + c' + f(\beta, \alpha')). \tag{1}$$

Now $(G, \otimes)$ is a group that we denote by G_f.

The elation group of the flock generalized quadrangle with parameters (q^2, q) is G_f where $f(\alpha, \beta) = \alpha \cdot \beta^T$ (the ordinary dot product, also denoted $\alpha \circ \beta$).

Now we specialize to $q = 3^k \geq 27$ and let n be a fixed nonsquare of F. We define $\overline{f}(\alpha, \beta)$ by

$$\overline{f}(\alpha, \beta) = \alpha \begin{pmatrix} -1 & 0 \\ 0 & n \end{pmatrix} \beta^T + \left\{ \alpha \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \beta^T \right\}^{\frac{1}{3}} + \left\{ \alpha \begin{pmatrix} 0 & 0 \\ 0 & n^{-1} \end{pmatrix} \beta^T \right\}^{\frac{1}{9}}. \tag{2}$$

Then $G_{\overline{f}}$ is the elation group of the Roman quadrangle with parameters (q^2, q).

We seek to distinguish G_f from $G_{\overline{f}}$.

3 The elation groups are not isomorphic

Let F denote the field of 3^k elements, $k \geq 3$. The following can be readily proved directly.

Lemma 3.1 *Let $g_1 = (\alpha_1, \beta_1, c_1)$ and $g_2 = (\alpha_2, \beta_2, c_2)$ be elements of G_f for a biadditive function f.*

(a) *The inverse of g_1 is $g_1^{-1} = (-\alpha_1, -\beta_1, f(\beta_1, \alpha_1) - c_1)$.*

(b) *The commutator of g_1 and g_2 is*

$$[g_1, g_2] = (0, 0, f(\beta_1, \alpha_2) - f(\beta_2, \alpha_1))$$

and, in particular, g_1 and g_2 commute if and only if $f(\beta_1, \alpha_2) = f(\beta_2, \alpha_1)$.

We establish various properties of the standard group $G = G_f$, where $f(\alpha, \beta)$ is the ordinary dot product, $\alpha \circ \beta$.

Lemma 3.2 *Let $x = (A, B, c)$, with $A, B \in F^2$ and $c \in F$, be an arbitrary element of G.*

(a) *If $A = (0, 0)$, then $C_G(x) = \{(\alpha', \beta', c') : \alpha' \in B^\perp\}$.*

(b) *If $A \neq (0, 0)$, then define a map $\gamma : F^2 \to F^2$ such that $\gamma(\alpha') \circ A = B \circ \alpha'$. In this case, $C_G(x) = \{(\alpha', \beta', c') : \beta' - \gamma(\alpha') \in A^\perp\}$.*

(c) *If x is not central in G, then $|C_G(x)| = 3^{4k}$.*

Proof: Every element of $C_G(x)$ is of the form (α', β', c') where $B \circ \alpha' = \beta' \circ A$.

(a) If $A = (0, 0)$, then this condition becomes $B \circ \alpha' = 0$ which is equivalent to $\alpha' \in B^\perp$.

(b) If $A \neq (0, 0)$, then given (α', β', c'), the definition of γ tells us that $\gamma(\alpha') \circ A = B \circ \alpha'$. Therefore the given element is in the centralizer of x if and only if we have $\gamma(\alpha') \circ A = \beta' \circ A$, or $\beta' - \gamma(\alpha') \in A^\perp$.

(c) In case (a), if $B = (0, 0)$, then there is no restriction on α' and so x is central. Otherwise, $\alpha' \in B^\perp$ implies that we have only 3^k choices for α'. With 3^{2k} choices for β' and 3^k choices for c', we deduce that $|C_G(x)| = 3^{4k}$. In case (b), for a given α' we have only 3^k choices for β', and so again $|C_G(x)| = 3^{4k}$. $\square$

Next we characterize those elements which are in the center of a centralizer.

Lemma 3.3 *Let x be an element of the form (A, B, c) with $A, B \in F^2$, $c \in F$. Then the center of $C_G(x)$ consists of all elements of the form (rA, rB, c'') for $r \in F$.*

Proof: First, to see that all elements of the given form are in the center of $C_G(x)$, let z be any element of the form (rA, rB, c'') for $r, c'' \in F$. Then if (α', β', c') is any element of $C_G(x)$, z will commute with it if $rB \circ \alpha' = \beta' \circ rA$. However, this is clear since membership in $C_G(x)$ implies that $B \circ \alpha' = \beta' \circ A$.

Now, to show that all central elements have such a form, let $z = (\alpha'', \beta'', c'')$ be an element of the center of $C_G(x)$. The proof will be done in two parts.

If $A = (0, 0)$, then by Lemma 3.2 (a), we must have $\alpha'' \in B^\perp$. We also want z to commute with every element of $C_G(x)$, hence we must have $\beta' \circ \alpha'' = \beta'' \circ \alpha'$ for all $\alpha' \in B^\perp, \beta' \in F^2$. In particular, if we choose β' with $\beta' \circ \alpha'' = 0$, then $0 = \beta'' \circ \alpha'$ for all $\alpha' \in B^\perp$. This implies that $\beta'' \in \langle B \rangle$, and so the right-hand side of the earlier equation is zero. Consequently, $\beta' \circ \alpha'' = 0$ for all $\beta' \in F^2$, forcing $\alpha'' = 0$. Thus every element of the center has the desired form.

On the other hand, if $A \neq (0, 0)$, then by Lemma 3.2 (b), we must have $\beta'' - \gamma(\alpha'') \in A^\perp$. Since z commutes with every element in $C_G(x)$, we must also have $\beta' \circ \alpha'' = \beta'' \circ \alpha'$ for all $\alpha', \beta' \in F^2$ where $\beta' - \gamma(\alpha') \in A^\perp$. In particular, if we take $\alpha' = 0$, then we must have $\beta' \circ \alpha'' = 0$ for all β' with $\beta' - \gamma(\alpha') \in A^\perp$. However, with $\alpha' = 0$, the defining property of γ tells us that $\gamma(\alpha') \in A^\perp$. Thus we have $\beta' \circ \alpha'' = 0$ for all β' with $\beta' \in A^\perp$ which implies that $\alpha'' \in \langle A \rangle$.

Next, if we choose $\alpha' \in B^\perp$, then the defining property of γ implies that $\gamma(\alpha') \circ A = 0$, or $\gamma(\alpha') \in A^\perp$. Therefore, since $\beta' - \gamma(\alpha') \in A^\perp$, we conclude that $\beta' \in A^\perp$. Now, since $\alpha'' \in \langle A \rangle$, we deduce that $\beta' \circ \alpha'' = 0$ and so the condition for z to be central becomes $0 = \beta'' \circ \alpha'$ for all $\alpha' \in B^\perp$. This is only possible if $\beta'' \in \langle B \rangle$.

Consequently, we can write $\alpha'' = rA$ and $\beta'' = sB$ for some $r, s \in F$. Now, for z to be central requires $\beta' \circ \alpha'' = \beta'' \circ \alpha'$ for all pairs (α', β') such that $\beta' \circ A = B \circ \alpha'$ (this being the required condition for membership in $C_G(x)$). Substituting for α'' and β'' we deduce that $r(\beta' \circ A) = s(B \circ \alpha')$. Since the second factors of each side are equal and we can choose β' so that this common value is not zero, we conclude that $r = s$, as desired. $\square$

Theorem 3.4 *For each noncentral x in $G = G_f$, the center of $C_G(x)$ has order 3^{2k}.*

Proof: Lemma 3.3 shows that we have 3^k choices for the element r and 3^k choices for c'' in picking an element of the center of $C_G(x)$, and so we have 3^{2k} elements. $\square$

Next we consider the group $\overline{G} = G_{\overline{f}}$. In order to show that $\overline{G}$ is not isomorphic to G, it will suffice to find a noncentral element in $\overline{G}$ whose centralizer does not have a center with order 3^{2k}. For this purpose, we will consider the element $\overline{x} = ((1, 0), (0, 0), 0)$.

Lemma 3.5 *The centralizer $C_{\overline{G}}(\overline{x})$ is equal to the set of elements $\{(\alpha', (b', b'^3), c') : \alpha' \in F^2, b', c' \in F\}$, and hence this subgroup has order 3^{4k}.*

Proof: Every element of $C_{\overline{G}}(\overline{x})$ is of the form (α', β', c') where $\overline{f}((0, 0), \alpha') = \overline{f}(\beta', (1, 0))$. We write $\beta' = (b'_1, b'_2)$ for the components of β'. Using the definition of $\overline{f}$, the centralizer condition becomes

$$\begin{aligned}0 &= -b_1' \cdot 1 + nb_2' \cdot 0 + (b_2' + b_1' \cdot 0)^{\frac{1}{3}} + (n^{-1}b_2' \cdot 0)^{\frac{1}{9}} \\ &= -b_1' + (b_2')^{\frac{1}{3}}\end{aligned}$$

and so, $b_2' = (b_1')^3$. Thus, for the elements of $C_{\overline{G}}(\overline{x})$, we have 3^{2k} choices for α', another 3^k choices for b_1' (and then b_2' is determined), and 3^k choices for c' giving us 3^{4k} elements in the centralizer. $\Box$

Lemma 3.6 *The center of $C_{\overline{G}}(\overline{x})$ is $\{((a'', 0), (0, 0), c'')\}$, where $a'' \in \mathrm{GF}(3)$, and so the center has order 3^{k+1}.*

Proof: Let $z = (\alpha'', \beta'', c'')$ be an element in the center of $C_{\overline{G}}(\overline{x})$ and write $\alpha'' = (a_1'', a_2'')$ and $\beta'' = (b'', (b'')^3)$ (we know β'' has this form by Lemma 3.5). Since z is central, we must have

$$\overline{f}((b', (b')^3), (a_1'', a_2'')) = \overline{f}((b'', (b'')^3), (a_1', a_2'))$$

for all $a_1', a_2', b' \in F$. Substituting into the definition of $\overline{f}$, this becomes

$$\begin{aligned}&-b'a_1'' + n(b')^3a_2'' + ((b')^3a_1'' + b'a_2'')^{\frac{1}{3}} + (n^{-1}(b')^3a_2'')^{\frac{1}{9}} \\ &\quad = -b''a_1' + n(b'')^3a_2' + ((b'')^3a_1' + b''a_2')^{\frac{1}{3}} + (n^{-1}(b'')^3a_2')^{\frac{1}{9}}\end{aligned}$$

for all $a_1', a_2', b' \in F$. In particular, if we take $b' = a_1' = 0$, we get

$$0 = n(b'')^3a_2' + (b''a_2')^{\frac{1}{3}} + (n^{-1}(b'')^3a_2')^{\frac{1}{9}}$$

for all a_2'. Now, raising to the 9th power is a field automorphism and so this equation will hold if and only if the equation obtained by taking 9th powers

$$0 = n^9(b'')^{27}(a_2')^9 + (b'')^3(a_2')^3 + n^{-1}(b'')^3a_2'$$

holds. But if $b'' \neq 0$, then this is a degree 9 polynomial in a_2' over F, and so can have at most 9 solutions. Since we assume $|F| > 9$, this contradicts the requirement that the equation hold for all $a_2' \in F$ implying that we must have $b'' = 0$.

Given that $b'' = 0$, our center condition becomes

$$-b'a_1'' + n(b')^3a_2'' + ((b')^3a_1'' + b'a_2'')^{\frac{1}{3}} + (n^{-1}(b')^3a_2'')^{\frac{1}{9}} = 0$$

for all $b' \in F$. As above, we can take the 3rd power of this equation, obtaining

$$-(a_1'')^3(b')^3 + n^3(a_2'')^3(b')^9 + a_1''(b')^3 + a_2''b' + (n^{-1}a_2'')^{\frac{1}{3}}b'$$

where we have collected the powers of b' to the end of each term. As above, if $a_2'' \neq 0$, we obtain a degree 9 polynomial in b' which is supposed to hold for all $b' \in F$. This contradiction implies that $a_2'' = 0$.

Substituting 0 for a_2'', our center condition becomes

$$-(a_1'')^3(b')^3 + a_1''(b')^3 = 0$$

for all $b' \in F$. Choosing a nonzero value of b', we must have $(a_1'')^3 = a_1''$ which implies that $a_1'' \in \mathrm{GF}(3)$. Consequently, in describing an element of the center, we have 3 choices for a_1'' and 3^k choices for c''. Hence the order of the center of $C_{\overline{G}}(\overline{x})$ is 3^{k+1}. □

Theorem 3.7 *The groups G_f and $G_{\overline{f}}$ are not isomorphic.*

Proof: Lemmas 3.5 and 3.6 imply that $\overline{x}$ is a noncentral element of $G_{\overline{f}}$ having a centralizer whose center has order 3^{k+1}. By Theorem 3.4 there are no such elements in G_f, and so the groups cannot be isomorphic. □

While this completes our primary goal of demonstrating that the two groups are non-isomorphic, we observe that it is easy from our existing analysis to determine the automorphism group of G_f.

Clearly the automorphism group of G_f maps into $\mathrm{GL}(4k, 3) \times \mathrm{GL}(k, 3)$, where the two factors correspond to the action of the automorphism group on the Frattini factor $V = G_f/\Phi(G_f)$ and its center respectively. Let Γ denote the image of the automorphism group in this direct product, and let Γ_i denote the the images of the projections of Γ into these two factors.

Now Γ_1 must preserve the set of images in V of the centers of the centralizers of the noncentral elements of G_f. By Lemma 3.3 this set consists of the 1-dimensional F-subspaces of V, where F acts naturally on V. It follows that $\Gamma_1 \leq \Gamma\mathrm{L}(4, q)$ by the fundamental theorem of projective geometry (recall that $q = 3^k$).

Consider now the subgroup Γ^* of Γ consisting of those elements that map into $\mathrm{GL}(4, q)$ rather than $\Gamma\mathrm{L}(4, q)$, and the associated subgroups Γ_1^* and Γ_2^*. By considering $[x, y]$ and $[\alpha x, y]$ for some $\alpha \in F$ it is easy to see that Γ_2^* acts on the center of G_f by scalars in F. Now the formula for a commutator in G_f shows that Γ_1^* acts on V by elements of a generalized symplectic group; that is to say, the group $\mathrm{GSp}(4, q)$ that preserves the symplectic form defined by commutation (where this is regarded as an F-bilinear form from $\wedge^2 V$ to F) up to scalar multiplication, the image in Γ_2^* of an element of Γ^* being multiplication by the corresponding scalar. Conversely, if $h \in \mathrm{GSp}(4, q)$ and γ is the corresponding scalar, then h and γ define an element of $\mathrm{GSp}(4, q) \times F^\times \leq \mathrm{GL}(4k, 3) \times \mathrm{GL}(k, 3)$ that lifts to an automorphism θ of G_f, since θ will preserve commutation, and G_f is of exponent 3. Clearly the automorphism group of F acts naturally on G_f, the same automorphism necessarily acting on the Frattini factor of G_f and on its center.

Hence we obtain the following result, where $\Gamma\mathrm{Sp}(4, q)$ denotes $\mathrm{GSp}(4, q)$ extended by the automorphism group of F.

Theorem 3.8 *There is an exact sequence $0 \to A \to Aut(G_f) \to \Gamma\mathrm{Sp}(4, q) \to 1$, where A is an elementary abelian 3-group of rank $4k^2$ consisting of those automorphisms that centralize the Frattini factor of G_f.*

While we have not analyzed the automorphism group of $G_{\overline{f}}$, we expect that this approach provides an alternative proof that the two groups are nonisomorphic.

Acknowledgements

We thank S.E. Payne for helpful discussions about the geometrical background to the problem. The first author was partially supported by the Australian Research Council and the third by the Marsden Fund of New Zealand via grant UOA 124.

References

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: the user language, *J. Symbolic Comput.* **24** (1997), 235–265.
See also `http://magma.maths.usyd.edu.au/magma/`

[2] Finite Geometries, Groups and Computation Conference, Pingree Park, Colorado State University, 4–9 September 2004; `http://www.math.colostate.edu/~hulpke/pingree/`

[3] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version* 4.4, 2004; `http://www.gap-system.org/`

[4] G. Havas, C.R. Leedham-Green, E.A. O'Brien and M.C. Slattery, Computing with elation groups, (submitted).

[5] S.E. Payne, An essay on skew translation generalized quadrangles, *Geom. Dedicata* **32** (1989), 93–118.

[6] S.E. Payne, *Ten Lectures in Perth (Elation Generalized Quadrangles, Etc.)*, Research Report 2004/11, School of Mathematics and Statistics, The University of Western Australia, 2004; `http://www.maths.uwa.edu.au/research/reports/2004/rr11.pdf`

[7] S.E. Payne and J.A. Thas, *Finite Generalized Quadrangles*. Pitman, 1984.

[8] S.E. Payne and K. Thas, Notes on elation generalized quadrangles, *European J. Combin.* **24** (2003), 969–981.