The Ghinelli-Löwe Construction of Generalized Quadrangles: An Exposition

D. Ghinelli and S. E. Payne

May 2002

1 Introduction: The Basic Construction

In 1994 the preprint [1] appeared giving a recipe for constructing finite generalized quadrangles of order (q^2, q) where $q = p^{2n}$, p a prime. A computer search located several examples with $p \equiv 3 \pmod 4$ and $n = 1$ where all the ingredients were present so that a generalized quadrangle (GQ) was actually obtained. The paper [1] was never published, largely because it was never determined whether or not the GQ were new. Recently we have been able to identify those GQ actually arising from the table in [1] as being of Kantor-Knuth type whose point-line duals are translation GQ of dimension 2 over their kernel.

In view of the fact that the GQ actually obtained are of known type, interest in the original preprint is somewhat diminished. Because it is not clear (to the present authors at least) that the general construction method is without merit, we offered a brief summary [2] of the construction and an indication of the proof that the examples actually produced are of the type indicated above. However, the present manuscript, which is intended to replace both earlier preprints [1] and [2], gives a great many more details and is available from either author. For the convenience of the reader we have reproduced in Appendix A the information in the table of [1].

We have changed the notation of [1] somewhat in order to simplify the presentation, but it should be clear even to the casual reader that the present construction is equivalent to the original.

This work is not intended to introduce the reader to the theory of generalized quadrangles (GQ), so many basic ideas and theorems are not stated

in full here. The standard reference for finite GQ is [5], and we often refer to it for needed definitions and results. We remind the reader that there is a point-line duality for GQ so that the point-line dual of a GQ with parameters (s,t) is a GQ with parameters (t,s). And any definition or result for GQ has a point-line dual version that we take as given also.

The notion of Property (G) that plays a central role in identifying the Ghinelli-Löwe GQ was introduced in [3], which was written a few years after the appearance of [5]. Property (G) has become a major focus of much of the work done on finite GQ during the past decade. The theorem of J. A. Thas in [7] that characterizes GQ of order (q^2,q) having Property (G) at some point as being exactly the flock GQ (for q odd) is one of the truly major accomplishments in the whole theory. At the appropriate place we will give a definition of Property (G).

Let $K = GF(p^n)$, p any (odd?) prime, $n \geq 1$, and $F = GF(p^{2n})$ a quadratic extension of K. Set $q = p^{2n} = |F|$. Then $\mathcal{M} = \{M_r, C_1, C_2 : r \in F\}$ is a set of $q+2$ square matrices of order 4 with elements in K for which

$$M_1 = I,\ M_r M_s = M_{rs},\quad M_r + M_s = M_{r+s},\quad \text{for all } r,s \in F. \tag{1}$$

$$M_r C_i = C_i M_r^T \quad \text{for all } r \in F, \quad i = 1,2. \tag{2}$$

$$x(M_r C_1)x^T = x(M_r C_2)x^T = 0 \text{ implies } x = 0 \quad \text{for } 0 \neq r \in F,\ x \in K^4. \tag{3}$$

For $\alpha, \beta \in K^4$ put

$$\alpha \circ \beta = \alpha C_1 \beta^T;\ \alpha \triangle \beta = \alpha C_2 \beta^T; \tag{4}$$

$$\alpha * \beta = (\alpha \circ \beta, \alpha \triangle \beta) \in K^2. \tag{5}$$

Clearly $\circ$, $\triangle$ and $*$ are maps which are linear over K and for which

$$\alpha * (\beta M_r) = \alpha M_r * \beta \quad \text{(by Eq. 2)}, \tag{6}$$

and

$$\alpha M_r * \alpha = 0 \text{ implies } \alpha = 0 \quad \text{for } 0 \neq r \in F \text{ (by Eq. 3)}. \tag{7}$$

Now put $G = \{(\alpha, \beta, u) : \alpha, \beta \in K^4, u \in K^2\}$, and define a binary operation on G by

$$(\alpha,\beta,u) \cdot (\alpha',\beta',u') = (\alpha+\alpha', \beta+\beta', u+u'+\alpha*\beta'-\beta*\alpha'). \tag{8}$$

This makes G into a group. For each $r \in F$, define the following subsets of G which are easily shown to be subgroups:

$$A_r = \left\{(\alpha, \alpha M_r, 0) : \alpha \in K^4\right\} \leq \left\{(\alpha, \alpha M_r, u) : \alpha \in K^4, u \in K^2\right\} = A_r^*. \quad (9)$$

Similarly, put

$$A_\infty = \left\{(0, \beta, 0) \in G : \beta \in K^4\right\} \leq \left\{(0, \beta, u) : \beta \in K^4, u \in K^2\right\} = A_\infty^*. \quad (10)$$

Put $\tilde{F} = F \cup \{\infty\}$, $\mathcal{J} = \{A_r : r \in \tilde{F}\}$ and $\mathcal{J}^* = \{A_r^* : r \in \tilde{F}\}$.

Theorem 1.1 *$(G, \mathcal{J}, \mathcal{J}^*)$ is a Kantor family, i.e., $\mathcal{J}$ is a 4-gonal family for G. (See [5], Chapter 8.)*

Proof: First note that $\mathcal{J}$ and $\mathcal{J}^*$ have the correct number of subgroups of the proper orders. Then the proof is made easy by the following two lemmas whose simple proofs are left to the reader.

Lemma 1.2 *For $r \in F$, the map*

$$\gamma_r : G \to G : (\alpha, \beta, u) \mapsto (\alpha, \alpha M_r + \beta, u). \quad (11)$$

is an automorphism of G that fixes A_∞ and A_∞^* pointwise and maps A_s to A_{s+r} for all $s \in F$.

Lemma 1.3 *The map*

$$\sigma : G \to G : (\alpha, \beta, u) \mapsto (\beta, \alpha, -u). \quad (12)$$

is an involutory automorphism of G interchanging A_s and $A_{s^{-1}}$ for all $s \in \tilde{F}$. (Naturally here $0^{-1} = \infty$ and $\infty^{-1} = 0$).

Put $\mathcal{G} = \{\theta \in \mathrm{Aut}(G) : \theta$ preserves $\mathcal{J}$ and $\mathcal{J}^*\}$. Clearly γ_r and σ belong to $\mathcal{G}$, so we immediately have the following:

Lemma 1.4 *The group $\mathcal{G}$ is at least doubly transitive on the sets $\mathcal{J}$ and $\mathcal{J}^*$.*

To prove Theorem 1.1 we need to establish the two properties of Kantor:

$$K1. \quad A_r \cdot A_s \cap A_u = \{id\}, \quad \text{for distinct } r, s, u \in \tilde{F}. \quad (13)$$

$$K2. \quad A_r^* \cap A_s = \{id\}, \quad \text{for distinct } r, s \in \tilde{F}. \quad (14)$$

By Lemma 1.4, to prove $K1$ we may assume that $r = \infty$, $s = 0$, and $0 \neq u \in F$. Then note that

$$(0,\beta,0)\cdot(\alpha,\alpha M_0,0)=(\alpha,\beta,-\beta*\alpha)=(\gamma,\gamma M_u,0)$$

if and only if $\alpha=\gamma$, $\beta=\gamma M_u$, and $0=-\beta*\alpha=-\alpha M_u*\alpha$. This holds if and only if $\alpha=0=\beta$, which establishes $K1$.

Similarly, to prove $K2$ we may assume $r=\infty$ and $s=0$. Then if $(0,\beta,u)=(\alpha,\alpha M_0,0)$ clearly $\alpha=\beta=0\in K^4$, $u=0\in K^2$. Hence $K2$ holds. This completes the proof of Theorem 1.1 ■

From the preceding theorem it follows that there must be an elation GQ $\mathcal{S}$ with order $(q^2,q)=(p^{4n},p^{2n})$ and having the following standard incidence diagram (see Chapter 8 of [5]).

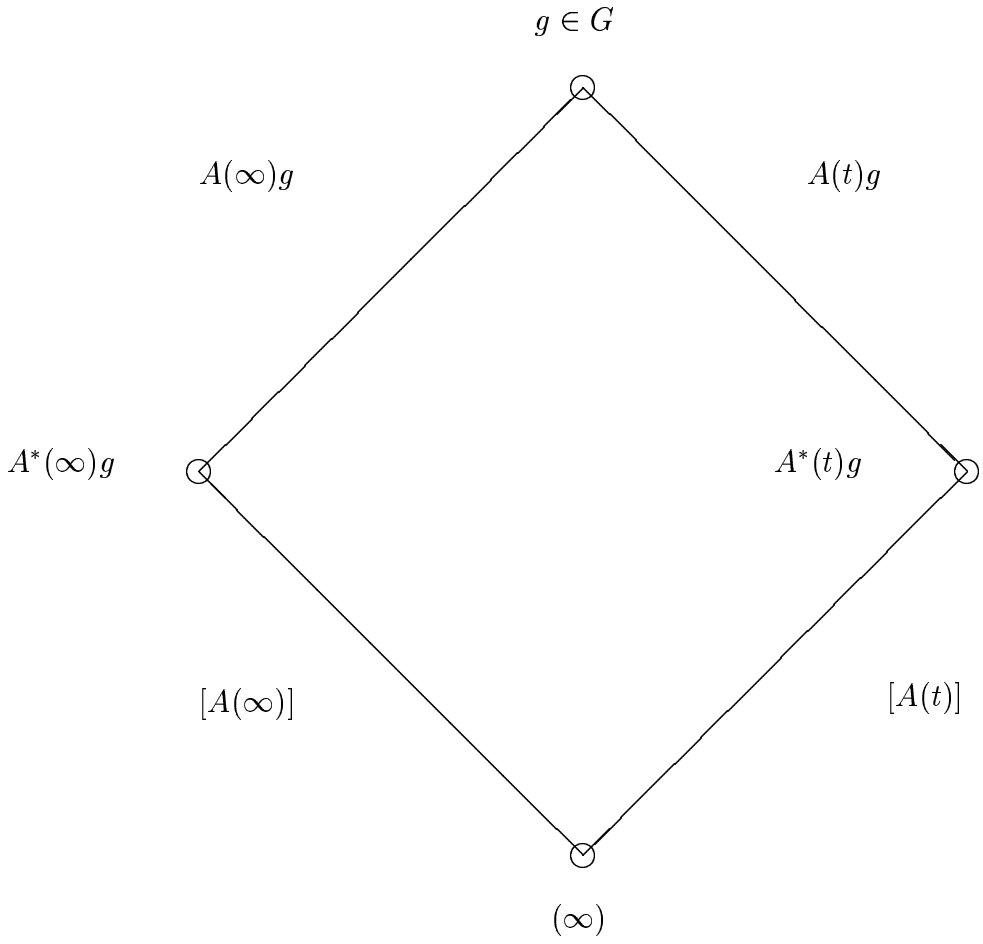

Fig. 1. Incidence Diagram for Elation Generalized Quadrangle

For convenience in later computations we compute the following.

$$(\alpha, \beta, u)^{-1} = (-\alpha, -\beta, \alpha * \beta - \beta * \alpha - u). \tag{15}$$

$$(\alpha, \beta, u)^{-1} \cdot (\gamma, \gamma M_r, v) \cdot (\alpha, \beta, u) = \tag{16}$$
$$= (\gamma, \gamma M_r, v + (\beta - \alpha M_r) * \gamma + \gamma * (\beta - \alpha M_r)).$$

Similarly,

$$(\alpha, \beta, u)^{-1} \cdot (0, \gamma, v) \cdot (\alpha, \beta, u) = (0, \gamma, v - (\gamma * \alpha + \alpha * \gamma)). \tag{17}$$

These latter two equations show that A_r^* is normal in G for all $r \in \tilde{F}$.

2 Some Collineations of $\mathcal{S}$

Define G_0 to be the group of collineations of S that fix the points (∞) and $(0,0,0)$. Clearly each $\theta \in \mathcal{G}$ induces a collineation of $\mathcal{S}$ which is also called θ and which fixes the points (∞) and $(0,0,0)$. Hence we naturally view $\mathcal{G}$ as a subgroup of G_0.

It is easily checked that for each $r \in \tilde{F}$, A_r^* is elementary abelian and we have already seen that it is normal in G. This means that under the usual action (right multiplication by elements of G) A_r^* is the stabilizer in G of the point $A_r^* g$ for all $g \in G$ and all $r \in \tilde{F}$.

It is also clear by Lemmas 1.2 and 1.3 that $\mathcal{G}$ (viewed as a subgroup of G_0) is doubly transitive on the set of lines of $\mathcal{S}$ through the point (∞).

A *symmetry* about a point p of $\mathcal{S}$ is a collineation of $\mathcal{S}$ that fixes each point collinear with p, i.e., each point of $p^\perp$. In a GQ with parameters (s,t), the maximum order of a group of symmetries about some point p is t. If there is a group of symmetries about a point p having order t, p is said to be a center of symmetry. If every point on some line L is a center of symmetry, the group T generated by the symmetries about the points on L is an elementary abelian group of order st^2 and $\mathcal{S}$ is a *translation* GQ (TGQ) with translation group T and *translation line* L. . See Chapters 8 and 9 of [5] for an introduction to finite TGQ.

We have already noted that γ_r fixes each point of A_∞^*. These are all the point of $\mathcal{S}$ that are collinear with the point A_∞^* that are not collinear with the point (∞). Two cosets $A_\infty^*(\alpha, \beta, u)$ and $A_\infty^*(\alpha', \beta', u')$ are the same if and only if $\alpha = \alpha'$. Hence $\gamma_r : (\alpha, \beta, u) \mapsto (\alpha, \alpha M_r + B, u)$ fixes each coset of A_∞^*

as well as the point (∞). Thus γ_r is a symmetry about the point A^*_∞. This essentially completes a proof of the following theorem.

Theorem 2.1 *The set $\Gamma = \{\gamma_r : r \in F\}$ is a full group of symmetries about the point A^*_∞, i.e., the point A^*_∞ is a center of symmetry. If we identify $g \in G$ with "right multiplication by" g, then $g^{-1}\Gamma g$ is a full group of symmetries about $A^*_\infty g$. It is also true that $Z = \{(0,0,c) \in G : c \in K^2\}$ is a full group of symmetries about the point (∞). Hence each line L through (∞) is a translation axis. So the point-line dual $\hat{\mathcal{S}}$ of $\mathcal{S}$ is a TGQ, and in fact has a line each point of which is a translation point!*

Lemma 2.2 *For $0 \neq k \in K$, define*

$$\theta_k : G \to G; (\alpha, \beta, u) \mapsto (k\alpha, k\beta, k^2 u). \tag{18}$$

Then θ_k is an automorphism of G that leaves invariant each A_r (and hence each A^*_r).

In fact there are more basic collineations available.

Lemma 2.3 *For $0 \neq k \in K$, define*

(i) $\rho_k : G \to G : (\alpha, \beta, u) \mapsto (\alpha, k\beta, ku)$;

(ii) $\lambda_k : G \to G : (\alpha, \beta, u) \mapsto (k\alpha, \beta, ku)$.

Then both ρ_k and λ_k are automorphisms of G that induce collineations of $\mathcal{S}$. Clearly $\theta_k = \lambda_k \circ \rho_k$.

Note that in Lemmas 2.2 and 2.3 k is a nonzero element of K, not an arbitrary nonzero element of F.

Again for $0 \neq k \in K$ define

$$\theta_k : G \to G : (\alpha, \beta, u) \mapsto (\alpha M_{k^{-1}}, \beta M_k, u). \tag{19}$$

Then $\theta_k \in \mathrm{Aut}(G)$ and $\theta_k : A_r \mapsto A_{rk^2}$ and $\theta_k : A^*_r \mapsto A^*_{rk^2}$. The proof of this uses the fact that $\alpha M_{k^{-1}} * \beta M_k = (\alpha M_{k^{-1}} \cdot M_k) * \beta = \alpha * \beta$ by Eqs. 1 and 6.

This last fact shows that G_0 is nearly 3-transitive on the lines through (∞), but we cannot seem to find the remaining θ_k for $k \in F \setminus K$ to show triple transitivity, at least in this general a setting.

3 Property (G)

The GQ $\mathcal{S}$ has Property (G) at the point (∞) provided the following is true: For L_1 and M_1 any distinct lines through (∞), if distinct lines $L_1,\ L_2,\ L_3,\ L_4,$ $M_1,\ M_2,\ M_3,\ M_4$ satisfy the property that L_i is concurrent with M_j whenever $1 \leq i + j \leq 7$, then it is also true that L_4 is concurrent with M_4.

It turns out that all the examples given in the table of [1] do in fact have Property (G) at the point (∞), although this is rather difficult to prove. But then by a remarkable theorem of J. A. Thas in [7] it follows that $\mathcal{S}$ must be a flock quadrangle, i.e., it must arise from a q-clan. Hence by the Fundamental Theorem (and its consequences) of S. E. Payne [4] each element of the group G_0 is (induced by) an element of $\mathcal{G}$. This makes it possible to calculate the kernel of the TGQ $\hat{\mathcal{S}}$, which turns out to be the subfield K.

In this section we sketch the proof that $\mathcal{S}$ has Property (G) at the point (∞).

Without loss of generality (either because G_0 is doubly transitive on the lines through the point (∞) or because the result of [7] is really much stronger than we cited above), we may assume that L_1 is the line $[A_\infty]$ and M_1 is the line $[A_0]$. Also, we may assume that for distinct nonzero $\alpha_1,\ \alpha_2 \in K^4$ and distinct nonzero β_1 and $\beta_2 \in K^4$ that $L_2 = A_0$, $L_3 = A_0(0, \beta_1, 0)$, $L_4 = A_0(0, \beta_2, 0)$, $M_2 = A_\infty$, $M_3 = A_\infty(\alpha_1, 0, 0)$, and $M_4 = A_\infty(\alpha_2, 0, 0)$.

Lemma 3.1 *In general the line $A_\infty(\alpha, 0, 0)$ meets the line $A_0(0, \beta, 0)$ at a point $(\alpha, \beta, (\alpha \circ \beta, \alpha \triangle \beta)) = (\alpha, \beta, (-\beta \circ \alpha, -\beta \triangle \alpha))$ if and only if*

(i) $\alpha \circ \beta + \beta \circ \alpha = 0$,

and

(ii) $\alpha \triangle \beta + \beta \triangle \alpha = 0$.

At this point a straight-forward interpretation of Lemma 3.1 as a general statement of just when $\mathcal{S}$ has Property (G) at the point (∞) yields the following result.

Lemma 3.2 *$\mathcal{S}$ has Property (G) at the point (∞) provided that whenever*
(i) $\alpha_1 \circ \beta_1 + \beta_1 \circ \alpha_1 = 0$,
(ii) $\alpha_1 \triangle \beta_1 + \beta_1 \triangle \alpha_1 = 0$,
(iii) $\alpha_1 \circ \beta_2 + \beta_2 \circ \alpha_1 = 0$,
(iv) $\alpha_1 \triangle \beta_2 + \beta_2 \triangle \alpha_1 = 0$,
(v) $\alpha_2 \circ \beta_1 + \beta_1 \circ \alpha_2 = 0$,

and
(vi) $\alpha_2 \triangle \beta_1 + \beta_1 \triangle \alpha_2 = 0$,
then also
(vii) $\alpha_2 \circ \beta_2 + \beta_2 \circ \alpha_2 = 0$,
and
(viii) $\alpha_2 \circ \beta_2 + \beta_2 \circ \alpha_2 = 0$.

In the specific examples considered by Ghinelli and Löwe two additional properties of the matrix C_1 are immediately noted: C_1 is both symmetric and invertible. **So for the remainder of this essay we assume that these two properties hold**. If we then write $\hat{C} = (C_2 + C_2^T)C_1^{-1}$ and replace β_i with $\beta_i C_1^{-1}$, we may rewrite Lemma 3.2 as the following theorem (where we finally need to assume that p is odd so that $\alpha \circ \beta + \beta \circ \alpha = 0$ if and only if $\alpha \circ \beta = 0$).

Theorem 3.3 *Property (G) fails to hold at* (∞) *if and only if there are four nonzero vectors* $\alpha_1, \alpha_2, \beta_1, \beta_2 \in K^4$ *for which*

(i) $\alpha_1 \beta_1^T = 0;\ \alpha_1 \hat{C} \beta_1^T = 0$;

(ii) $\alpha_2 \beta_1^T = 0;\ \alpha_2 \hat{C} \beta_1^T = 0$;

(iii) $\alpha_1 \beta_2^T = 0;\ \alpha_1 \hat{C} \beta_2^T = 0$;

but for which not both

(iv) $\alpha_2 \beta_2^T = 0$ *and* $\alpha_2 \hat{C} \beta_2^T = 0$ *hold.*

Clearly $\{\alpha_1, \alpha_2\}$ must be K-linearly independent.

. Then we reinterpret this in terms of the matrices C_1 and C_2. Then we notice that C_1 has determinant $1 + x^2$, which cannot be zero, since $-1 = \square \in K$.

---

4 A Quadratic Equation for $\hat{C}$

It turns out that in all the examples given in the table of [1] the matrix $\hat{C}$ satisfies a quadratic equation over K. So in this section we want to examine the consequences of such a property.

Suppose that

$$\hat{C}^2 = \lambda_1 \hat{C} + \lambda_2 I, \quad \lambda_1,\ \lambda_2 \in K. \tag{20}$$

It is also clear that in the known examples $\hat{C}$ is not a scalar matrix. So we may assume that

$$p(t) = t^2 - \lambda_1 t - \lambda_2 \quad \text{is the minimal polynomial for } \hat{C}. \tag{21}$$

First suppose that $p(t)$ factors over K. If $p(t) = (t-a)^2$ with $a \in K$, then the rational form for $\hat{C}$ is

$$\begin{pmatrix} a & 1 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

In the rational form, put $\alpha_1 = (0,1,0,0)$ and $\alpha_2 = (0,0,1,0)$. Then $\alpha_1 \hat{C} = a\alpha_1$ and $\alpha_2 \hat{C} = (0,0,a,1)$, so the important facts are that

$$A = \begin{pmatrix} \alpha_1 \\ \alpha_1 \hat{C} \\ \alpha_2 \\ \alpha_2 \hat{C} \end{pmatrix} \text{ has rank 3 and } \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \text{ has rank 2.}$$

If $p(t) = (t-a)(t-b)$ with a and b distinct elements of K, then the rational form for $\hat{C}$ is

$$\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & b \end{pmatrix}$$

In this case put $\alpha_1 = (1,0,0,0)$ and $\alpha_2 = (0,1,1,0)$. Again the same important facts as above hold. So first there is a (unique up to scalar multiple) nonzero β_1 for which

$$A{\beta_1}^T = \begin{pmatrix} \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Then since $\{\alpha_1, \alpha_2\}$ has rank 2, there is a β_2 which is not a scalar multiple of β_1 for which

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \beta_2 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

It follows that

$$\alpha_2 \hat{C} {\beta_2}^T \neq \begin{pmatrix} \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

This shows that if $p(t)$ splits over K then $\mathcal{S}$ does not have Property (G) at the point (∞).

Now suppose that $p(t)$ is irreducible over K, so $\hat{C}$ has no eigenvalues in K or eigenvectors over K. So for any nonzero vector α, $\begin{pmatrix} \alpha \\ \alpha\hat{C} \end{pmatrix}$ has rank 2. If $A = \begin{pmatrix} \alpha_1 \\ \alpha_1\hat{C} \\ \alpha_2 \\ \alpha_2\hat{C} \end{pmatrix}$ has rank 2 then$A$ and $\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$ have the same (right) nullspace. Hence any β for which $\alpha_1\beta^T = \alpha_1\hat{C}\beta^T = 0$, also satisfies $A\beta^T = 0$, implying that Property (G) holds. Also, if $\alpha_2 = u_1\alpha_1 + u_2\alpha_1\hat{C}$, then $\alpha_2\hat{C} = u_1\alpha_1\hat{C} + u_2\alpha_1(\lambda_1\hat{C} + \lambda_2 I) = (\lambda_2 u_2)\alpha_1 + (u_1 + \lambda_1 u_2)\alpha_1\hat{C}$. Hence any β for which $\alpha_1\beta^T = \alpha_1\hat{C}\beta^T = 0$ also satisfies $A\beta^T = 0$.

So we may consider the case where $\{\alpha_1, \alpha_1\hat{C}, \alpha_2\}$ is K-linearly independent. But to find a counterexample to Property (G) we need A to be singular. Hence there are unique scalars u_1, u_2, $u_3 \in K$ for which $\alpha_2\hat{C} = u_1\alpha_1 + u_2\alpha_1\hat{C} + u_3\alpha_2$. Then $\alpha_2(\lambda_1\hat{C} + \lambda_2 I) = u_1\alpha_1\hat{C} + u_2\alpha_1(\lambda_1\hat{C} + \lambda_2 I) + u_3\alpha_2\hat{C}$, which implies that

$$(\lambda_1 - u_3)\alpha_2\hat{C} = \lambda_2 u_2\alpha_1 + (\lambda_1 u_2 + u_1)\alpha_1\hat{C} + (-\lambda_2)\alpha_2.$$

If $\lambda_1 = u_3$, then $\lambda_2 = 0$, an impossibility when $\hat{C}$ is nonsingular. So we have

$$(\lambda_1 - u_3)\alpha_2\hat{C} = \lambda_2 u_2\alpha_1 + (\lambda_1 u_2 + u_1)\alpha_1\hat{C} - \lambda_2\alpha_2$$

and (multiply the original equation for $\alpha_2\hat{C}$ by $\lambda_1 - u_3$)

$$(\lambda_1 - u_3)\alpha_2\hat{C} = (\lambda_1 = u_3)u_1\alpha_1 + (\lambda_1 - u_3)\alpha_1\hat{C} + (\lambda_1 - u_3)u_3\alpha_2.$$

Since the coefficients on α_2 must be the same, $-\lambda_2 = (\lambda_1 - u_3)u_3$, i.e., $p(u_3) = 0$. This says $p(t)$ has roots in K contrary to our hypothesis. Hence if A is nonsingular it has rank 2 and Property (G) holds. This completes a proof of the following theorem.

Theorem 4.1 *The Ghinelli-Löwe GQ have Property (G) at the point* (∞) *if and only* $p(t) = t^2 - \lambda_1 t - \lambda_2$ *is irreducible over* K*, where* $p(t)$ *is the minimal polynomial of* $\hat{C}$*.*

5 Choosing the Matrices of $\mathcal{M}$

In [1] it was assumed that $p^n \equiv 3 \pmod 4$ so that $-1 = \square \in K$ and $F = K(\sqrt{-1})$. For $r = r_1 + r_2\sqrt{-1} \in F$, $r_1, r_2 \in K$, the specific matrices used in [1] are as follows (except that we have interchanged rows 2 and 3 as well as columns 2 and 3 of all pertinent matrices to increase the ease of computing with them):

$$m_r = \begin{pmatrix} r_1 & r_2 \\ -r_2 & r_1 \end{pmatrix} \text{ and } M_r = I_2 \otimes m_r. \tag{22}$$

Put $P_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $P_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Q = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then

$$(i) \quad P_1^2 = P_2^2 = I = -Q^2. \tag{23}$$

$$(ii) \quad P_1P_2 = Q = -P_2P_1. \tag{24}$$

$$(iii) \quad P_1Q = P_2 = -QP; QP_2 = P_1 = -P_2Q. \tag{25}$$

$$C_1 = \begin{pmatrix} P_1 - xP_2 & 0 \\ 0 & -P_1 \end{pmatrix} \tag{26}$$

$$C_2 = \begin{pmatrix} P_1 - yP_2 & -zP_2 \\ P_1 & -P_1 - P_2 \end{pmatrix} \tag{27}$$

Here x, y, z are elements of K to be chosen (by computer in [1]) so that Eq. 3 holds and with x and z never 0. For arbitrary choices of x, y and z both Eqs. 1 and 2 hold.

The next two equations show the advantage of using the block form of the matrices that we have chosen.

$$\det(aP_1 \pm bP_2) = -(a^2 + b^2) = 0 \text{ iff } a = b = 0. \tag{28}$$

$$det(aI \pm bQ) = a^2 + b^2 = 0 \text{ iff } a = b = 0. \tag{29}$$

It is now easy to compute $\det(C_1) = 1 + x^2$ which can never be 0 since -1 is a nonsquare in K. We can now compute $\hat{C} = (C_2 + C_2^T)C_1^{-1}$.

$$(1 + x^2)\hat{C} = \begin{pmatrix} 2(1 + xy)I + 2(y - x)Q & -(1 + x^2)(I + zQ) \\ (1 + xz)I + (z - x)Q & 2(1 + x^2)(I - Q) \end{pmatrix} \tag{30}$$

We now need to determine just when $\hat{C}$ satisfies a quadratic equation. To do this it is more convenient to square the matrix $(1 + x^2)\hat{C}$. This is a rather tedious operation, so we first note the following equalities.

$$(aI + bQ)(cI + dQ) = (ac - bd)I + (ad + bc)Q. \tag{31}$$

$$(aI + bQ)^2 = (a^2 - b^2)I + 2abQ. \tag{32}$$

$$\begin{pmatrix} aI + bQ & cI + dQ \\ eI + fQ & gI + hQ \end{pmatrix} \begin{pmatrix} aI + bQ & cI + dQ \\ eI + fQ & gI + hQ \end{pmatrix} = \begin{pmatrix} X & Y \\ Z & W \end{pmatrix} \tag{33}$$

where

$X = (a^2 - b^2 + ce - df)I + (2ab + cf + de)Q,$

$Y = (ac - bd + cg - dh)I + (ad + bc + ch + dg)Q,$

$Z = (ae - bf + ge - fh)I + (af + be + gf + eh)Q,$

and

$W = (ce - df + g^2 - h^2)I + (cf + de + 2gh)Q.$

For $(1+x^2)\hat{C}$ we have

$$a = 2(1+xy), \quad b = 2(y-x), \quad c = -(1+x^2), \quad d = -(1+x^2)z,$$

$$e = (1+xz), \quad f = (z-x), \quad g = 2(1+x^2), \quad h = -2(1+x^2).$$

We then compute the four blocks of $\left[(1+x^2)\hat{C}\right]^2$.

The (1,1) block of $\left[(1+x^2)\hat{C}\right]^2$ is:

$$[4(1+xy)^2 - 4(y-x)^2 - (1+x^2(1+xz) + (1+x^2)z(z-x)]\, I +$$

$$+ [8(1+xy)(y-x) - (1+x^2)(z-x) - (1+x^2)z(1+xz)]\, Q.$$

The (1,2) block of $\left[(1+x^2)\hat{C}\right]^2$ is:

$$[-2(1+xy)(1+x^2) + 2(1+x^2)(y-x)z - 2(1+x^2)^2 - 2(1+x^2)z]\, I +$$

$$+ [-2(1+x^2)(1+xy)z - 2(1+x^2)(y-x) + 2(1+x^2)^2 - 2(1+x^2)^2 z]\, Q.$$

The (2,1) block of $\left[(1+x^2)\hat{C}\right]^2$ is:

$$[2(1+xy)(1+xz) - 2(y-x)(z-x) + 2(1+x^2)(1+xz) + 2(1+x^2)(z-x)]\, I +$$

$$+ [2(1+xy)(z-x) + 2(y-x)(1+xz) + 2(1+x^2)(z-x) - 2(1+x^2)(1+xz)]\, Q.$$

The (2,2) block of $\left[(1+x^2)\hat{C}\right]^2$ is:

$$[-(1+x^2)(1+xz) + (1+x^2)z(z-x)]\, I +$$

$$+ [-(1+x^2)(z-x) - (1+x^2)z(1+xz) - 8(1+x^2)^2]\, Q.$$

Now we want to know when there are $\lambda 1$ and $\lambda_2 \in K$ for which

$$\left[(1+x^2)\hat{C}\right]^2 = \lambda_1(1+x^2)\hat{C} + \lambda_2(1+x^2)I.$$

From the blocks (1,2) and (2,1) we get four equations in λ_1 alone.

$$\begin{aligned}
\lambda_1 &= 2(1+xy) - 2(y-x)z + 2(1+x^2) + && (34)\\
&\quad +2(1+x^2)z;\\
\lambda_1 z &= 2(1+xy)z + 2(y-x) - 2(1+x^2)(1-z); && (35)\\
\lambda_1(1+xz) &= 2(1+xy)(1+xz) + 2(1+x^2)(1+xz) + && (36)\\
&\quad -2(y-x)(z-x) + 2(1+x^2)(z-x);\\
\lambda_1(z-x) &= 2(1+xy)(z-x) + 2(y-x)(1+xz) + && (37)\\
&\quad +2(1+x^2)(z-x) - 2(1+x^2)(1+xz).
\end{aligned}$$

We now consider some linear combinations of the preceding equations.

$$\frac{(35) - z(36)}{2} = 0 = (y-x)(1+z^2) - (1+x^2)(1+z) + (1+x^2)(z-z^2). \quad (38)$$

$$\begin{aligned}
\frac{(36) - (1+xz)(36)}{2} = 0 &= (1+xz)(1+x^2+yz-xz) - (y-x)(z-x) + \quad (39)\\
&\quad -(1+x^2)(1+xz) + (1+x^2)(z-x) - (1+x^2)z(1+xz).
\end{aligned}$$

$$\frac{(37) - (z-x)(36)}{2} = 0 = (y-x)(1+z^2) - (1+x^2)(1+z^2). \quad (40)$$

Equation 38 simplifies to: $(1+z^2)(y-1-x-x^2) = 0$.

Equation 39 simplifies to: $x(z^2+1)(y-1-x-x^2) = 0$.

Equation 40 simplifies to: $(z^2+1)(y-1-x-x^2) = 0$.

Since $1+z^2 \neq 0$, we must have

$$y = 1 + x + x^2. \quad (41)$$

Note: We checked the table in [1] and found that indeed in each case $y = 1 + x + x^2$.

Now we use Eq. 36 to solve for λ_1.

$$\lambda_1 = 2(1+x^2)(x+2). \quad (42)$$

Before considering blocks (1,1) and (2,2), make the substitution $y = 1+x+x^2$, so $1+xy = 1+x+x^2+x^3 = (1+x)(1+x^2)$, and $y-x = 1+x^2$. Then both blocks yield the same information:

$$xz^2 + 2z - 5x - 4x^3 = 0, \tag{43}$$

and

$$\lambda_2 = z^2 - 2xz - 1 - 4(1+x^2)(x+2). \tag{44}$$

With a little work using Eq. 43 λ_2 can be rewritten as

$$\lambda_2 = (1+x^2)[-2zx^{-1} - 4x - 4]. \tag{45}$$

Since $\left[(1+x^2)\hat{C}\right]^2 = \lambda_1(1+x^2)\hat{C} + \lambda_2(1+x^2)I$, we now have the following theorem.

Theorem 5.1 *The matrix $\hat{C}$ satisfies a quadratic equation over K if and only if*
(i) $y = 1+x+x^2$,
and
(ii) $xz^2 + 2z - 5x - 4x^3 = 0$.

In this case we replace λ_i with $\frac{\lambda_i}{1+x^2}$, $i = 1$ and $i = 2$, so we can write

$$\hat{C}^2 = \lambda_1\hat{C} + \lambda_2 I, \tag{46}$$

with

$$\lambda_1 = 2(x+2), \tag{47}$$

$$\lambda_2 = -2(zx^{-1} + 2x + 2). \tag{48}$$

We checked all the entries in the table of [1], and indeed in every case the two conditions of Theorem 5.1 hold. Put $p(t) = t^2 - \lambda_t - \lambda_2$, so $p(t)$ is the minimal polynomial of $\hat{C}$. Then $p(t)$ is irreducible over K if and only if ${\lambda_1}^2 + 4\lambda_2 = \square \in K$. But ${\lambda_1}^2 + 4\lambda_2 = 4x^2 - 8zx^{-1} = \square$ if and only if $x^4 - 2xz = \square$. Again we checked the table in [1] and found that in every case $x^4 - 2xz = \square \in K$. This allows us to arrive at the following conclusion.

Theorem 5.2 *The GQ given by the entries in the table of [1] all have Property (G) at the point (∞).*

6 The Kernel

If $\mathcal{S}$ is a Ghinelli-Löwe GQ with Property (G) at the point (∞) its point-line dual is a TGQ, so it has a kernel $\mathcal{K}$. Let $L_1 = [A_\infty]$ and $L_2 = A_0$. The multiplicative group $\mathcal{K}^*$ of $\mathcal{K}$ is isomorphic to

$$H = \{\theta \in \mathrm{Aut}(\mathcal{S}) : \theta \text{ fixes } L_1 \text{ and } L_2 \text{ pointwise}\}.$$

Moerover, since $\mathcal{S}$ has Property (G) at (∞), it is a flock GQ by [7]. Hence by the Fundamental Theorem of [4] each $\theta \in H$ is (induced by) an automorphism (also called θ of G.

Let $\theta \in H$. Since θ fixes L_1 pointwise, and since $A^*_\infty(\alpha,\beta,c) = A^*_\infty(\alpha',\beta',c')$ if and only if $\alpha = \alpha'$, we know that

$$\theta : (\alpha,\beta,c) \mapsto (\alpha, (\alpha,\beta,c)^{\theta_2}, (\alpha,\beta,c)^{\theta_3}), \tag{49}$$

for appropriate functions θ_2 and θ_3.

Similarly, since (α,β,c) and $\alpha',\beta',c')$ belong to the same coset of A_0^* if and only if $\beta = \beta'$, since θ fixes A_0^* and permutes the points $A_0^*(0,\beta,0)$, $0 \neq \beta$, among themselves, θ_2 is a function of β alone. Se we write $(\alpha,\beta,c)^{\theta_2} = \beta^{\theta_2}$ where $\beta^{\theta_2} = 0$ if $\beta = 0$.

$$\theta : (\alpha,\beta,c) \mapsto (\alpha, \beta^{\theta_2}, (\alpha,\beta,c)^{\theta_3}),\ 0^{\theta_2} = 0. \tag{50}$$

Since θ permutes the lines $[A_t]$, $0 \neq t \in F$, there is a permutation $t \mapsto \bar{t}$ of the elements of F with $\bar{0} = 0$ for which $\theta : A_t \mapsto A_{\bar{t}}$. This is because θ, being an automorphism of G and mapping A_i to some coset of $A_{\bar{i}}$, must map it to the coset of $A_{\bar{i}}$ containing the identity. Hence we now know that

$$\theta : (\alpha, \alpha M_t, 0) \mapsto (\alpha, \alpha M_{\bar{t}}, 0),\ \text{implying } (\alpha M_t)^{\theta_2} = \alpha M_{\bar{t}}. \tag{51}$$

For any $\beta \in K^4$, $\beta = \beta M_{t^{-1}} M_t \overset{\theta_2}{\mapsto} (\beta M_{t^{-1}}) M_{\bar{t}}$. Similarly, $\beta = \beta M_{s^{-1}} M_s \overset{\theta_2}{\mapsto} \beta M_{s^{-1}} M_{\bar{s}}$. This holds for all $\beta \in K^4$ and all $s,t \in F$. So $s^{-1}\bar{s} = t^{-1}\bar{t}$, i.e., if $s = 1$, $\bar{t} = t \cdot \bar{1}$. So $\theta_2 : \beta M_t \mapsto \beta M_{t\bar{1}}$. In particular, $\beta = \beta M_1 \mapsto \beta M_1 M_{\bar{1}} = \beta M_{\bar{1}}$.

$$\theta : (\alpha,\beta,c) \mapsto (\alpha, \beta M_{\bar{1}}, (\alpha,\beta,c)^{\theta_3}). \tag{52}$$

For the remainder of this proof write $M = M_{\bar{1}}$.

$A_\infty(\alpha,0,0)$ joins $A^*_\infty(\alpha,0,0)$ with $(\alpha,0,0)$ on A_0, both fixed points, and in general contains the points $(\alpha,\beta,-\beta*\alpha)$, for $\beta \in K^4$. So

$$\theta : (\alpha, \beta, -\beta * \alpha) \mapsto (\alpha, \beta M, -\beta * \alpha) = (\alpha, \beta M, (\alpha, \beta, -\beta * \alpha)^{\theta_3}).$$

This proves

$$-\beta M * \alpha = (\alpha, \beta, -\beta * \alpha)^{\theta_3}. \tag{53}$$

Note that $(0, 0, c') \cdot (\alpha, \beta, c) = (\alpha, \beta, c' + c)$. Write out what it means for θ to preserve the group operation in G to obtain

$$(0, 0, c')^{\theta_3} + ((\alpha, \beta, c)^{\theta_3} = (\alpha, \beta, c' + c)^{\theta_3}. \tag{54}$$

Now put $\alpha = \beta = 0$ to obtain

$$(0, 0, c')^{\theta_3} + (0, 0, c)^{\theta_3} = (0, 0, c' + c)^{\theta_3}. \tag{55}$$

Write $(0, 0, c)^{\theta_3} = c^{\theta_3}$ from now on.

Replace c with 0 and c' with c to obtain

$$(\alpha, \beta, c)^{\theta_3} = (0, 0, c)^{\theta_3} + (\alpha, \beta, 0)^{\theta_3} = (\alpha, \beta, 0)^{\theta_3} + c^{\theta_3}. \tag{56}$$

Use this last equality with Eq. 53 to obtain $(\alpha, \beta, 0)^{\theta_3} = (\beta * \alpha)^{\theta_3} - \beta M * \alpha$, which implies

$$(\alpha, \beta, c)^{\theta_3} = (\beta * \alpha)^{\theta_3} - \beta M * \alpha + c^{\theta_3}. \tag{57}$$

At this point we have established

$$(\alpha, \beta, c)^{\theta} = (\alpha, \beta M, (\beta * \alpha)^{\theta_3} - \beta M * \alpha + c^{\theta_3}). \tag{58}$$

It is time to write out in complete generality what it means for

$$[(\alpha, \beta, c) \cdot (\alpha', \beta', c')]^{\theta} = (\alpha, \beta, c)^{\theta} \cdot (\alpha', \beta', c')^{\theta}.$$

This is a bit ungainly but completely routine. After expanding all the terms and canceling where possible, we are left with

$$(\alpha * \beta)^{\theta_3} - \alpha * \beta' M + (\beta' * \alpha)^{\theta_3} - \beta' M * \alpha = 0. \tag{59}$$

Since θ_3 is additive,

$$c^{\theta_3} = (c_1, c_2)^{\theta_3} = (c_1, 0)^{\theta_3} + (0, c_2)^{\theta_3},$$

and

$$(c+c',0)^{\theta_3} = (c,0)^{\theta_3} + (c',0)^{\theta_3}, \text{ etc.}$$

So Eq. 59 becomes

$$(\alpha\circ\beta,0)^{\theta_3} - (\alpha\circ\beta M,0) + (\beta\circ\alpha,0)^{\theta_3} - \beta M\circ\alpha = 0, \tag{60}$$

and

$$(0,\alpha\triangle\beta)^{\theta_3} - (0,\alpha\triangle\beta M) + (0,\beta\triangle\alpha)^{\theta_3} - (0,\beta M\triangle\alpha) = 0. \tag{61}$$

Consider Eq. 60. In general for the C_1 used in [1] $\alpha\circ\beta = \beta\circ\alpha$, so we have

$$2(\alpha\circ\beta,0)^{\theta_3} - 2(\alpha\circ\beta M) = 0.$$

Since $\alpha\circ\beta M = \alpha M\circ\beta$ by Eq. 6, we have

$$(\alpha\circ\beta,0)^{\theta_3} = \alpha\circ\beta M = \alpha M\circ\beta.$$

In particular

$$(\alpha C_1\beta^T,0)^{\theta_3} = \alpha M C_1\beta^T \text{ for all } \alpha,\ \beta\in K^4. \tag{62}$$

Eq. 62 is just what we need. First, if $\bar{1} = r\in K$, then $\alpha M_{\bar{1}} = \alpha M_r = r\alpha$ for all α. And it is easy to check that $\theta_r : (\alpha,\beta,c)\mapsto(\alpha,r\beta,rc)$ for $0\neq r\in K$ is in the kernel. So at least $K\subseteq\mathcal{K}$. But for $r\notin K$, the map $\theta : (\alpha,\beta,c)\mapsto(\alpha,\beta M_r,(\alpha,\beta,c)^{\theta_3})$ cannot be well defined. Here is an example. Let $r=\sqrt{-1}$, so $M_r = I\otimes Q$. C_1 is invertible, so we can choose β so that $C_1\beta^T = (1,1,0,0)^T$. Put $\alpha_1 = (1,0,0,0)$, $\alpha_2 = (0,1,0,0)$. Then $(\alpha_1 C_1\beta^T,0) = (1,0)$ and $(\alpha_2 C_1\beta^T,0) = (1,0)$. So we should have $(\alpha_1 C_1\beta^T,0)^{\theta_3} = (\alpha_2 C_1\beta^T,0)$. But

$$\alpha_1 M_{\sqrt{-1}} C_1\beta^T = (1,0,0,0)\begin{pmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&1\\0&0&-1&0\end{pmatrix}\begin{pmatrix}1\\1'\\0\\0\end{pmatrix} = 1$$

and

$$\alpha_2 M_{\sqrt{-1}} C_1 \beta^T = (0,1,0,0) \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} = -1.$$

This completes a proof of the following:

Theorem 6.1 *The kernel of (the point-line dual of) a Ghinelli-Löwe GQ arising from the table in [1] is the subfield K.*

Once we know that the point-line dual of $\mathcal{S}$ is a translation GQ with dimension 2 over its kernel, we invoke Appendix B of J. A. Thas [6] to complete a proof of the following theorem.

Theorem 6.2 *At least for the values given in the table of Ghinelli and Löwe the GQ constructed by their method is isomorphic to the Kantor-Knuth semi-field flock GQ associated with the automorphism of F given by $\sigma : x \mapsto x^q$, where $F = GF(q^2)$.*

It is not clear to us just how the conditions imposed on x, y and z led to $\hat{C}$ satisfying an irreducible quadratic polynomial. This situation deserves further study. We hope to make some progress on this point, especially as long as there is hope that the general method might yield examples not having Property (G). However, the original computer programs that produced the table of [1] were written by the junior author, and he is no longer in academia or interested in the problem.

7 Appendix A

Here we reproduce the information given in the table of [1]. Since $y = 1 + x + x^2$ in every case, we give here only the prime p, which is congruent to 3 modulo 4, and the corresponding values of x and z.

p	3	7	11	19	23	31	43	47	59	67	71	79
x	1	2	4	3	2	4	1	13	3	1	9	6
z	1	6	7	5	13	20	27	39	18	11	23	4

References

[1] D. Ghinelli and S. Löwe, Fourgonal families from nonsymmetric matrices, 1994, 9 pages.

[2] D. Ghinelli and S. E. Payne, The Ghinelli-Löwe Construction of Generalized Quadrangles, 2002, preprint.

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

[4] S. E. Payne, The fundamental theorem of q-clan geometry, *Des. Codes Cryptogr.*, 8(1–2)(1996), 181–202. Special issue dedicated to Hanfried Lenz.

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

[6] J. A. Thas, Symplectic spreads in $PG(3, q)$, inversive planes and projective planes, *Discrete Mathematics*, 174(1997), 329 – 336.

[7] J. A. Thas, Generalized quadrangles of order (s, s^2). III. *J. Combin. Theory* Ser. A 87 (1999), no. 2, 247 – 272.

Addresses of the Authors:

D. Ghinelli
Dipartimento di Matematica
Università di Roma "La Sapienza"
P.le A. Moro, 2
I-00185 ROMA (Italy)
E-mail: dina@mat.uniroma1.it

S. E. Payne
Department of Mathematics, Campus Box 170
1250 14th Street, Suite 600 (802020
P.O.Box 173364
Denver, Colorado 80217-3364