

RELATION GROUPS OF THE HERMITIAN SURFACE $H(3, q^2)$ OVER A
FINITE FIELD OF CHARACTERISTIC 2.

by

Robert L. Rostermundt

B.A., University of Colorado at Boulder, 1993

A thesis submitted to the
University of Colorado at Denver
in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Applied Mathematics
2005

This thesis for the Doctor of Philosophy

degree by

Robert L. Rostermundt

has been approved

by

Stan Payne

Bill Cherowitzo

Mike Jacobson

Rich Lundgren

Eric Moorhouse

Date

Rostermundt, Robert L. (Ph.D., Applied Mathematics)

Elation Groups of the Hermitian Surface $H(3, q^2)$ Over a Finite Field of Characteristic 2.

Thesis directed by Professor Stan Payne

ABSTRACT

Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a finite generalized quadrangle (GQ) having order (s, t) . Let p be a point of \mathcal{S} . A whorl about p is a collineation of \mathcal{S} fixing all the lines through p . An elation about p is a whorl that does not fix any point not collinear with p , or is the identity. If \mathcal{S} has an elation group acting regularly on the set of points not collinear with p we say that \mathcal{S} is an elation generalized quadrangle (EGQ) with base point p . S. E. Payne posed the following question: Can there be two non-isomorphic elation groups about the same point p ? In this presentation, we show that there are exactly two (up to isomorphism) elation groups of the Hermitian surface $H(3, q^2)$ over the finite field of characteristic 2. Moreover, we investigate some possible EGQ 's that may be constructed as a coset geometry from the new elation groups, and show that the EGQ we construct are isomorphic to the Hermitian surface.

This abstract accurately represents the content of the candidate's thesis. I recommend its publication.

Signed _____
Stan Payne

DEDICATION

This is dedicated to my parents, whose constant support has helped to make this thesis a reality.

ACKNOWLEDGMENT

There are many people who have been present with me throughout this long journey and deserve thanks. I would first like to thank all the members of my committee for their time and effort. In particular, I thank my advisor Stan Payne, without whose patience I could have never reached as far as I have. I can only dream of becoming a mathematician of his stature and reputation. Furthermore, Bill Cherowitzo has been a constant source of assistance, especially during the early stages of my career as a graduate student. Here I quote Newton's letter to Hooke in 1676, in which he said, "If I have seen further than others, it is because I was standing on the shoulders of giants."

I also would like to thank Tim Penttila for selflessly suggesting this problem. Although we are separated by some distance, he has been extremely supportive throughout the process.

I also extend my appreciation to the graduate committee for appointing me a teaching assistant position. This financial support has made a great impact on my success here at UCD. Moreover, I thank the Warren Bateman Family for their generous funding of the Lynn Bateman Teaching Fellowship, and the Lynn Bateman Teaching Award, both of which I was a recipient. These were established in memory of Lynn Bateman, who had an outstanding reputation as a teaching assistant in the department.

Finally, over the past six years I have had many friends, both in and out of the math department, who have encouraged me to push on during the most difficult times. I can not name them all here, but I would like to thank a few specific individuals: Marcia Kelly, Jennifer Thurston, Steve Flink, Scott Hace, Ryan and Natalie McGrath, Christi Day, and also my family, Leo and Elizabeth and Liz Rostermundt. To all of you, I am in your debt.

Rob Rostermundt

CONTENTS

Figures	ix
1. Introduction and Review	1
1.1 Preface	1
1.2 Historical Background	2
1.3 Basic Definitions and Combinatorics	3
1.4 Elation Generalized Quadrangles	5
1.5 Introduction to q -clans	8
1.6 Some examples of q -clans	10
1.7 q -Clans and Flocks	11
1.8 4-Gonal Families from q -Clans	14
1.9 A Construction of the Hermitian Surface $H(3, q^2)$	19
1.10 Regularity in $H(3, q^2)$	20
2. Main Results	21
2.1 Forming a Sylow ₂ Subgroup in the Group of Whorls	21
2.2 Elation Groups of $H(3, q^2)$ As Subgroups of S_2	27
2.3 The Commutator Subgroup	31
2.4 The Quotient Group \mathcal{S}/\mathcal{S}'	35
2.5 Looking for Hyperplanes	36
2.6 Lower central Series	38
2.7 Building Subgroups $A(t)$ in the Exotic Elation Group E	51

2.8	The Function $\delta(t)$	53
2.9	The Function g_t	55
2.10	Property(G)	67
2.11	A Theorem of Matt Brown	80
2.12	The Final Push	81
2.13	Suggested Problems	81
	<u>Appendix</u>	
A.	Theorems	83
B.	The Hermitian Surface: A Unitary Representation	98
	<u>References</u>	103

FIGURES

Figure		
1.1	The coset geometry $\mathcal{S}^{(\infty)}$	6
1.2	Construction of F and F^* from $(S^{(p)}, G)$	8
2.1	Property(G)	68
2.2	3×3 Grid.	71
2.3	3×3 Grid.	73
2.4	Near 4×4 Grid.	75
A.1	$P2 : A_j^* \cap A_i = \{id\}$ for all $i \neq j$	87
A.2	$P3 : A_j A_i \cap A_k = \{id\}$ for all distinct i, j, k	87
A.3	$P3 : A_j A_i \cap A_k = \{id\}$ for all distinct i, j, k	88
A.4	$P4 : A_i^* A_j = G$ for all $i \neq j$	89
A.5	$P5 : A_i^* = A_i \cup \{A_i g : A_i g \cap \Omega = \emptyset\}$	91
A.6	$P5 : A_i^* = A_i \cup \{A_i g : A_i g \cap \Omega = \emptyset\}$	91

1. Introduction and Review

1.1 Preface

The goal of this thesis is to answer a question posed by S.E. Payne: Given an elation generalized quadrangle and a point p , can there be non-isomorphic elation groups having the base point p ? In this thesis we will give a proof that the Hermitian surface $H(3, q^2)$ has two non-isomorphic elation groups. Initially, Tim Penttila completed a search for the cases $q = 2$ and $q = 4$, using the Magma software package. In each case, he discovered $q^2 - 1$ new elation groups that were non-isomorphic to the known elation group. For all cases $q = 2^e$, we will construct the $q^2 - 1$ elation groups of $H(3, q^2)$. Moreover, we will show that they are non-isomorphic to the known elation group, while being pairwise isomorphic.

We start with a representation of the standard elation group due to S.E. Payne, and adjoin an involution ϕ to form a Sylow₂ subgroup (denoted S_2), having order $2q^5$, of the group of whorls about the point (∞) . We then show that the only non-elations in S_2 are contained in the coset of the commutator subgroup containing the involution ϕ . We proceed to show that the factor group S_2/S'_2 is elementary abelian; i.e., a vector space over $GF(2)$, and then using the complete set of linear functionals from S_2/S'_2 onto $GF(2)$, we construct the complete set of elation groups about (∞) . This set has size q^2 . We then show, using nilpotency class, that $q^2 - 1$ of these groups are non-isomorphic to the standard elation group. Furthermore, we show that these $q^2 - 1$ groups are pairwise isomorphic.

Next we proceed to find conditions for the existence of 4-gonal families in these new elation groups. Given these conditions, we will construct a family of EGQ and prove that these EGQ are flock- GQ . Moreover, we will be able to show that all the new GQ we have constructed are classical, and hence isomorphic to $H(3, q^2)$.

1.2 Historical Background

The notion of a finite generalized quadrangle (GQ) is a fairly recent one. J. Tits first introduced generalized polygons in 1959 [29]. Generalized polygons are the building blocks of Tits buildings, and are the precursors of more general geometries such as partial geometries, partial quadrangles, semi-partial geometries, and near polygons [30]. In actuality, generalized quadrangles have been around for some time as line systems corresponding to symplectic polarities in three-dimensional projective space over a field. But the explicit study of such geometric objects is due to Tits. Initially, progress was made in the study of what are now called classical generalized quadrangles (see [Dem68] and [FH64])- that is, those quadrangles that can be imbedded in projective space. It was in the late 1960's that other researchers began looking deeply at these geometric objects, and since then, many new examples and results have been discovered.

The focus of this thesis is the classical GQ known as $H(3, q^2)$, the Hermitian surface in three-dimensional projective space over the field $GF(q^2)$. Here we will study a certain class of collineations called elations. More specifically, we answer the question posed by S.E. Payne: Can there be two non-isomorphic

elation groups about the base point p ?

In this thesis we show that there are two elation groups of $H(3, q^2)$, up to isomorphism. We also look into the construction of elation generalized quadrangles (EGQ) arising from the newly described elation group of the Hermitian surface. Although we do not have a complete classification of these EGQ , we show that all of our constructions are isomorphic to the classical $H(3, q^2)$.

1.3 Basic Definitions and Combinatorics

We start with some basic definitions. Let \mathcal{P} and \mathcal{B} be two non-empty sets, called points and lines, with an incidence relation \mathcal{I} such there are two positive integers s and t satisfying

G1) Each point is incident with $t + 1$ lines; any two points are mutually incident with at most one line.

G2) Each line is incident with $s + 1$ points; any two lines are mutually incident with at most one point.

G3) Given a line L and a point x not incident with L there is a unique point y and a unique line M such that $x \mathcal{I} M \mathcal{I} y \mathcal{I} L$.

Such a collection $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is called a **generalized quadrangle of order** (s, t) written $GQ(s, t)$; when $s = t$ the GQ is said to have order s . The **dual** of a $GQ(s, t)$ is the $GQ(t, s)$ obtained by interchanging the roles of points and lines. Furthermore, any theorem or definition given for a GQ can be dualized by interchanging the words points and lines. It will therefore be assumed that whenever a definition or theorem is given, its dual has also been given.

Two points incident with a common line are said to be **collinear** and two lines incident with a common point are **concurrent**. If x and y are collinear we use the notation $x \sim y$. Similarly, if L and M are concurrent we denote this $L \sim M$.

If X is a set of points (respectively, lines) of \mathcal{S} , then X^\perp denotes the set of all points collinear (resp., lines concurrent) with everything in X ; X^\perp is also called the **trace** of X . If $X = \{x\}$ is a singleton set, it is common to write X^\perp as x^\perp . The **span** of X , written $X^{\perp\perp}$, is the set of all points collinear (resp., lines concurrent) with all of X^\perp . By convention $x \in x^\perp$.

Straightforward counting arguments demonstrate the following:

- $|\mathcal{P}| = (1 + s)(1 + st)$.
- $|\mathcal{B}| = (1 + t)(1 + st)$.
- For $x \in \mathcal{P}$, $|x^\perp| = 1 + s + st$.
- For $L \in \mathcal{B}$, $|L^\perp| = 1 + t + st$.
- For two non-collinear points x, y , $|\{x, y\}^\perp| = t + 1$
and $2 \leq |\{x, y\}^{\perp\perp}| \leq t + 1$.
- For two non-concurrent lines L, M , $|\{L, M\}^\perp| = s + 1$
and $2 \leq |\{L, M\}^{\perp\perp}| \leq s + 1$.

Let x, y be two noncollinear points of a $GQ(s, t)$. We say that $\{x, y\}$ is a **regular pair** provided $|\{x, y\}^{\perp\perp}| = t + 1$. If x is a point such that for every y , with $x \not\sim y$, we have $|\{x, y\}^{\perp\perp}| = t + 1$, then we say x is a **regular point**. A set

$\{x, y, z\}$ of pairwise non-collinear points is called a **triad** of points. If $\{x, y, z\}$ is a triad of points, then all points in $\{x, y, z\}^\perp$ are called **centers**.

The next important theorem is known as Higman's inequality.

Theorem 1.3.1 (D.G. Higman) [13] *Let $\mathcal{S} = (P, B, I)$ be a GQ of order (s, t) . Then $s \leq t^2$ and dually $t \leq s^2$. Furthermore, $t = s^2$ if and only if for some pair (x, y) of non-collinear points every triad (x, y, w) has exactly $s + 1$ centers if and only if every triad of points has exactly $1 + s$ centers.*

Proof: We give the proof in Theorem A.1. ■

Corollary 1.3.2 *Let $\mathcal{S} = (P, B, I)$ be a GQ of order (q^2, q) . Then every set of three pairwise non-concurrent lines has exactly $q + 1$ transversals.*

1.4 Elation Generalized Quadrangles

The focus of this thesis is a certain class of GQ called elation generalized quadrangles. Here we explain this class of quadrangles.

Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a $GQ(s, t)$, $s \geq 1$, $t \geq 1$, and let $p \in \mathcal{P}$ be a point of \mathcal{S} . A **whorl** about p is a collineation of \mathcal{S} that leaves invariant each line incident with p . If there is a group of whorls acting transitively on the points not collinear with p we say that p is a **center of transitivity**. Let θ be a whorl about p . If $\theta = id$ or if θ fixes no point of $\mathcal{P} \setminus p^\perp$, then θ is an **elation** about p . If there is a group G of elations about p acting regularly on $\mathcal{P} \setminus p^\perp$, we say \mathcal{S} is an **elation generalized quadrangle (EGQ)** with **elation group** G and **base point** p . We will often denote this quadrangle as $(\mathcal{S}^{(p)}, G)$, or simply $\mathcal{S}^{(p)}$.

We now describe a standard construction of elation generalized quadrangles. Let G be a group with order s^2t . Then let $\mathbb{F} = \{A_0, A_1, \dots, A_r\}$ be a family of $r + 1$ subgroups of G , each with order s , and let $\mathbb{F}^* = \{A_0^*, A_1^*, \dots, A_r^*\}$ be another family of $r + 1$ subgroups of G , each having order st where $A_i \leq A_i^*$ for each $0 \leq i \leq r$.

Our geometry, which we denote $\mathcal{S}^{(\infty)}$, is defined as follows. There are three types of points; (i) elements $g \in G$, (ii) cosets A_i^*g , (iii) a symbol (∞) . There are two types of lines; (i) cosets $A_i g$, (ii) symbols $[A_i]$. Incidence is as follows; the symbol (∞) is incident with the $r + 1$ lines of type (ii), the s cosets of A_i^* are the other s points on a line $[A_i]$, each point A_i^*g is incident with lines corresponding to the cosets $A_i h$ that are completely contained in the coset A_i^*g , the remaining points on a line $A_i h$ are the group elements contained in the coset $A_i h$. The diagram in figure 1.1 may be helpful.

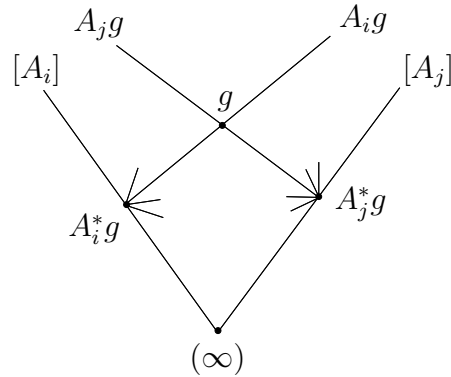


Figure 1.1: The coset geometry $\mathcal{S}^{(\infty)}$

Theorem 1.4.1 *Let G be a group of order s^2t and let $F = \{A_0, A_1, \dots, A_t\}$ be a family of $t + 1$ subgroups, each with order s , and let $F^* = \{A_0^*, A_1^*, \dots, A_t^*\}$ be another family of $t + 1$ subgroups, each having order st where $A_i \leq A_i^*$ for each $0 \leq i \leq t$. Then if we build the coset geometry $\mathcal{S}^{(\infty)}$ as prescribed above, $\mathcal{S}^{(\infty)}$ is a GQ, having order (s, t) , if and only if properties K1 and K2 hold, where*

$$K1: A_j A_i \cap A_k = \{id\} \text{ for all distinct } i, j, k.$$

$$K2: A_j^* \cap A_i = \{id\} \text{ for all } i \neq j.$$

Proof: See Theorem A.2 in Appendix A. ■

In the previous theorem, we call F a **4-gonal family** of G , and $\{G, F, F^*\}$ is called a **Kantor family**.

Let $(S^{(p)}, G)$ be an elation GQ with base point p (and group G of elations about p). Then we can obtain a 4-gonal family in the following way. To obtain the set \mathcal{F}^* we choose a point q not collinear with p and consider $\{p, q\}^\perp$. For each of the $t + 1$ points $x \in \{p, q\}^\perp$ define a subgroup A_i^* to be the stabilizer of x in G . Then define A_i to be the stabilizer in G of the line through q and x . The set $\mathcal{F} = \{A_0, A_1, \dots, A_t\}$ will be a four-gonal family for G with accompanying set $\mathcal{F}^* = \{A_0^*, A_1^*, \dots, A_t^*\}$.

Theorem 1.4.2 [28]. *Suppose that $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a GQ with order (s, t) , $s, t > 1$, with s and t powers of the same prime p . Suppose (∞) is a regular*

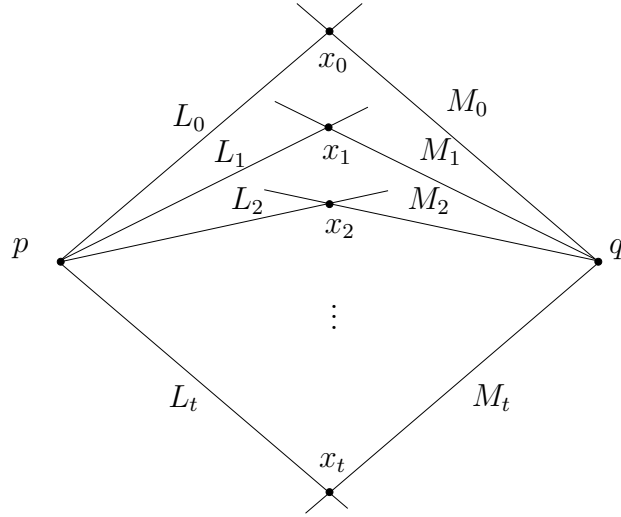


Figure 1.2: Construction of F and F^* from $(S^{(p)}, G)$

point that is a center of transitivity, and let H be the full group of whorls about (∞) . Let G be a Sylow $_p$ subgroup of H . Then we have

1. $|G| = s^2t$, or
2. $p = 2$, $|G| = 2s^2t$, and \mathcal{S} contains a proper thick $(s, t > 1)$ subGQ of order t isomorphic to $W(t)$; consequently, $s = t^2$.

1.5 Introduction to q -clans

There is a strong connection between flocks of a quadratic cone and generalized quadrangles. In fact, there is a large class of GQ known as flock generalized quadrangles. The connection between the two structures arises from particular sets of 2×2 matrices.

Definition 1.5.1 *If we let $\bar{\alpha} = (\alpha_1, \alpha_2)$, then the matrix*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

*is said to be **anisotropic** provided $Q(\bar{\alpha}) := \bar{\alpha}A\bar{\alpha}^T = 0$ if and only if $\bar{\alpha} = 0$.*

Theorem 1.5.2 *Let $a, b, c, d \in GF(q)$ where $q = 2^e$. Then the matrix*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is anisotropic if and only if $tr\left(\frac{ad}{(b+c)^2}\right) = 1$, where $tr : GF(q) \rightarrow GF(2)$ is the absolute trace function.

Put $q = 2^e$ and let $X : x \mapsto x_t$, $Y : y \mapsto y_t$, and $Z : z \mapsto z_t$ be three functions from \mathbb{F} to \mathbb{F} . Put

$$A_t = \begin{pmatrix} x_t & y_t \\ 0 & z_t \end{pmatrix}.$$

and define the set $\mathcal{C} = \{A_t : t \in \mathbb{F}\}$.

Definition 1.5.3 *The set \mathcal{C} is a **q-clan** provided all pairwise differences $A_s - A_t$ ($s, t \in \mathbb{F}, s \neq t$) are anisotropic.*

Note: The anisotropic condition on $A_t - A_s$, with $A_t, A_s \in \mathcal{C}$, is precisely that

$$tr\left(\frac{(x_t + x_s)(z_t + z_s)}{(y_t + y_s)^2}\right) = 1$$

1.6 Some examples of q -clans

Example 1.6.1 (Classical) Let $A_t = t \begin{pmatrix} 1 & 1 \\ 0 & d \end{pmatrix}$ where $\text{tr}(d) = 1$.

To see that this is a q -clan look at

$$A_t - A_s = \begin{pmatrix} t-s & t-s \\ 0 & (t-s)d \end{pmatrix}$$

and notice that $\text{tr} \left(\frac{(t-s)^2 d}{(t-s)^2} \right) = \text{tr}(d) = 1$.

Example 1.6.2 (Kantor) $A_t = \begin{pmatrix} t & t^2 \\ 0 & t^3 \end{pmatrix}$, where $t \in \mathbb{F} = GF(q)$, $q = 2^e$, and e -odd.

To see that this is a q -clan look at

$$A_t - A_s = \begin{pmatrix} t-s & t^2 - s^2 \\ 0 & t^3 - s^3 \end{pmatrix}$$

Then we have

$$\text{tr} \left(\frac{(t-s)(t^3 - s^3)}{(t^2 - s^2)^2} \right) = \text{tr}(1) + \text{tr} \left(\frac{st}{t^2 + s^2} \right)$$

The equation $x^2 + x + 1 = 0$ has no solutions in $GF(2)$ and so its roots lie in a quadratic extension of $GF(2)$. But e is odd and so $GF(4)$ is not a subfield of \mathbb{F} . Therefore $x^2 + x + 1$ is irreducible in \mathbb{F} and hence $\text{tr}(1) = 1$. Furthermore,

the polynomial $sx^2 + (s+t)x + t$ has the root $x = s/(s+t)$. It follows that $\text{tr} \left(\frac{st}{t^2 + s^2} \right) = 0$. and Kantor's example is indeed a q -clan.

Example 1.6.3 (Payne) [17] $A_t = \begin{pmatrix} t & t^3 \\ 0 & t^5 \end{pmatrix}$, where $t \in \mathbb{F} = GF(q)$, $q = 2^e$, and e odd.

Consider the difference

$$A_t - A_s = \begin{pmatrix} t - s & t^3 - s^3 \\ 0 & t^5 - s^5 \end{pmatrix}$$

Then

$$\text{tr} \left(\frac{(t-s)(t^5 - s^5)}{(t^3 - s^3)^2} \right) = \text{tr}(1) + \text{tr} \left(\frac{st(s^2 + t^2)}{(t^2 + st + s^2)^2} \right)$$

In this case $\text{tr}(1) = 1$ because e is odd. Furthermore, the polynomial $(st)x^2 + (s^2 + st + t^2)x + (s^2 + t^2) = 0$ has the root $x = 1$, and so $\text{tr} [st(s^2 + t^2)/(t^2 + st + s^2)^2] = 1$. It follows that Payne's example is a q -clan.

1.7 q -Clans and Flocks

Let $K = \{(x_0, x_1, x_2, x_3) \in PG(3, q) : x_1^2 = x_0x_2\}$. Then K is a quadratic cone in $PG(3, q)$ with vertex $(0, 0, 0, 1)$. Recall that all quadratic cones of $PG(3, q)$ are equivalent under the action of $PTL(4, q)$, hence WLOG we can choose our favorite cone.

Definition 1.7.1 *Let K be a quadratic cone with vertex V . A **flock of K** is a partition $F = \{C_t : t \in \mathbb{F}\}$ of $K \setminus \{V\}$ into q pairwise disjoint conics C_t .*

Each conic is a plane intersection $C_t = \pi_t \cap K$, where $\pi_t = [x_t, y_t, z_t, 1]^T$, and we often consider the flock to be the set of planes π_t .

Theorem 1.7.2 (J.A. Thas) [27]. *If $\mathbb{F} = GF(2^e)$, let $X : t \mapsto x_t$, $Y : t \mapsto y_t$, and $Z : t \mapsto z_t$ be three functions on \mathbb{F} . For each $t \in \mathbb{F}$, put $\pi_t = [x_t, y_t, z_t, 1]^T$, $C_t = \pi_t \cap K$, $\mathcal{F} = \{C_t : t \in \mathbb{F}\}$. Also put $A_t \equiv \begin{pmatrix} x_t & y_t \\ 0 & z_t \end{pmatrix}$ and $C = \{A_t : t \in \mathbb{F}\}$. Then C is a q -clan if and only if F is a flock.*

Proof: The set \mathbb{F} is a flock provided every two distinct conics C_t and C_s with s different from t are disjoint. If $\pi_t = [x_t, y_t, z_t, 1]^T$ and $\pi_s = [x_s, y_s, z_s, 1]^T$ are planes defining the conics C_t and C_s , we want that π_t and π_s meet at a line external to K . Therefore, the following system:

$$x_t X_0 + y_t X_1 + z_t X_2 + X_3 = 0$$

$$x_s X_0 + y_s X_1 + z_s X_2 + X_3 = 0$$

$$X_1^2 = X_0 X_2$$

can have only the trivial solution. Subtracting the second equation from the first we get

$$(x_t - x_s)X_0 + (y_t - y_s)X_1 + (z_t - z_s)X_2 = 0$$

Not all of X_0, X_1, X_2 are zero. So assume WLOG that $X_2 \neq 0$ and divide

through by X_2 to get the following equation.

$$\begin{aligned} 0 &= (x_t - x_s) \frac{X_0}{X_2} + (y_t - y_s) \frac{X_1}{X_2} + (z_t - z_s) \\ &= (x_t - x_s) \frac{X_0}{X_2} + (y_t - y_s) \frac{\sqrt{X_0 X_2}}{X_2} + (z_t - z_s) \end{aligned}$$

Letting $Y = \frac{\sqrt{X_0 X_2}}{X_2}$ we get

$$(x_t - x_s)Y^2 + (y_t - y_s)Y + (z_t - z_s) = 0.$$

Since we are in even characteristic this equation has no solutions if and only if $\frac{(x_t - x_s)(z_t - z_s)}{(y_t - y_s)^2}$ has trace equal to 1 for any $s, t \in \mathbb{F}$, $s \neq t$. This is exactly the condition that C be a q -clan. ■

Note: Two flocks are **projectively equivalent** when there exists a projective semilinear map of $PG(3, q)$ leaving the cone invariant and mapping one flock to the other.

Suppose that $\mathcal{C} = \{A_t = \begin{pmatrix} x_t & y_t \\ 0 & z_t \end{pmatrix} : t \in \mathbb{F}\}$ is a q -clan. It is easy to check that $\mathcal{C}' = \{A'_t \equiv A_t - A_0 : t \in \mathbb{F}\}$ is also a q -clan. The q -clan \mathcal{C} has an associated flock $F(\mathcal{C}) = \{\pi_t = [x_t, y_t, z_t, 1]^T : t \in \mathbb{F}\}$, and \mathcal{C}' has the associated flock $F(\mathcal{C}') = \{\pi'_t = [x_t - x_0, y_t - y_0, z_t - z_0, 1]^T : t \in \mathbb{F}\}$. Then since $T : [x, y, z, 1]^T \mapsto [x - x_0, y - y_0, z - z_0, 1]^T$ is a projective linear map on $PG(3, q)$ that leaves the cone invariant, without loss of generality we can assume that each q -clan \mathcal{C} contains the zero matrix, which by convention we will label as A_0 .

1.8 4-Gonal Families from q -Clans

Let $\mathbb{F} = GF(q)$ where $q = 2^e$. Put $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and for $\alpha, \beta \in \mathbb{F}^2 = \mathbb{F} \times \mathbb{F}$ define $\alpha \circ \beta$ by

$$\alpha \circ \beta = \alpha P \beta^T$$

Then $(\alpha, \beta) \mapsto \alpha \circ \beta$ is a non-singular, alternating, bilinear form with the property that $\alpha \circ \beta = 0$ if and only if $\{\alpha, \beta\}$ is \mathbb{F} -dependent.

On the set $G^\otimes = \mathbb{F}^2 \times \mathbb{F}^2 \times \mathbb{F} = \{(\alpha, \beta, c) : \alpha, \beta \in \mathbb{F}^2, c \in \mathbb{F}\}$ define the binary operation

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

This operation makes G^\otimes into a group of order q^5 with center $Z = \{(0, 0), (0, 0), c\}$.

This group has two important families of elementary abelian subgroups of order q^3 . For $0 \neq \gamma \in \mathbb{F}^2$, put $\mathcal{L}_\gamma = \{(\gamma \otimes \alpha, c) \in G^\otimes : \alpha \in \mathbb{F}^2, c \in \mathbb{F}\}$, and for $0 \neq \alpha \in \mathbb{F}^2$, put $\mathcal{R}_\alpha = \{(\gamma \otimes \alpha, c) \in G^\otimes : \gamma \in \mathbb{F}^2, c \in \mathbb{F}\}$.

Theorem 1.8.1 [8]. *Each \mathcal{L}_γ and each \mathcal{R}_α are elementary abelian groups of order q^3 . And for nonzero $\alpha, \gamma \in \mathbb{F}^2$, $\mathcal{L}_\gamma = \mathcal{L}_\alpha$ (resp., $\mathcal{R}_\gamma = \mathcal{R}_\alpha$) if and only if $\{\alpha, \gamma\}$ are \mathbb{F} -dependent, so we may think of the groups \mathcal{L}_γ and \mathcal{R}_α as indexed by the points of $PG(1, q)$.*

Note: We use the elements of $\tilde{\mathbb{F}} = \mathbb{F} \cup \{\infty\}$ to index the points of $PG(1, q)$ as follows: $\gamma_\infty = (0, 1)$ and $\gamma_t = (1, t)$ for $t \in \mathbb{F}$.

Let $\mathcal{C} = \{A_t \equiv \begin{pmatrix} x_t & y_t \\ 0 & z_t \end{pmatrix} : t \in \mathbb{F}\}$ be a q -clan with $A_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Also put $A_\infty = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, and $\gamma_{y_\infty} = \gamma_\infty = (0, 1)$. Then define $g(\alpha, t) = \alpha A_t \alpha^T$ for $t \in \tilde{\mathbb{F}}$ and $\alpha \in \mathbb{F}^2$. It will be useful to recognize that

$$g(\alpha + \beta, t) = (\alpha + \beta)A_t(\alpha + \beta)^T = g(\alpha, t) + g(\beta, t) + y_t(\alpha \circ \beta)$$

For each $t \in \tilde{\mathbb{F}}$ there are subgroups $A(t)$ and $A^*(t)$ of G^\otimes defined in the following way:

$$A(t) = \{(\gamma_{y_t} \otimes \alpha, g(\alpha, t)) \in G^\otimes : \alpha \in \mathbb{F}^2\} \leq A^*(t) := A(t) \cdot Z = \mathcal{L}_{\gamma_{y_t}} \leq G^\otimes.$$

It is easy to see that $A(t)$ is a subgroup when noticing that

$$(\gamma_{y_t} \otimes \alpha_1, g(\alpha_1, t)) \cdot (\gamma_{y_t} \otimes \alpha_2, g(\alpha_2, t)) = (\gamma_{y_t} \otimes (\alpha_1 + \alpha_2), g(\alpha_1 + \alpha_2, t))$$

Observe also that $A(t)$ is a subgroup of order q^2 and $A^*(t)$ is a subgroup of order q^3 . It is also helpful to see that for $t \in \mathbb{F}$, a typical element of $A(t)$ has the form

$$(\alpha, y_t \alpha, \alpha_1^2 x_t + \alpha_1 \alpha_2 y_t + \alpha_2^2 z_t), \quad \text{where } \alpha = (\alpha_1, \alpha_2) \in \mathbb{F}^2.$$

Further, an element of $A(\infty)$ looks like $(0, \alpha, 0)$.

Theorem 1.8.2 [8]. *Put $\mathcal{J}(\mathcal{C}) = \{A(t) : t \in \tilde{\mathbb{F}}\}$, $\mathcal{J}^*(\mathcal{C}) = \{A^*(t) : t \in \tilde{\mathbb{F}}\}$. Then the triple $(G^\otimes, \mathcal{J}(\mathcal{C}), \mathcal{J}^*(\mathcal{C}))$ is a Kantor family, i.e., $\mathcal{J}(\mathcal{C})$ is a 4-gonal family for G^\otimes . The associated GQ is denoted $GQ(\mathcal{C})$ and is referred to as a flock GQ.*

Proof: We know that $Y : t \mapsto y_t$ is a permutation and so for distinct $t, u \in \mathbb{F}$ we have $y_t \neq y_u$. Showing property K_2 is easy when looking at two elements from $A(t)$ and $A^*(u)$ with $u \neq t$. If

$$(\alpha, y_t \alpha, \alpha_1^2 x_t + \alpha_1 \alpha_2 y_t + \alpha_2^2 z_t) = (\hat{\alpha}, y_u \hat{\alpha}, c)$$

then $\alpha = \hat{\alpha}$ which forces both to be equal to $(0, 0)$ which then forces $c = 0$. Therefore, $A(t) \cap A^*(u) = (0, 0, 0) = \{id\}$.

Showing property K_1 is easy in one case. Look at $A(\infty)A(t) \cap A(u)$. Because $A_t - A_u$ is anisotropic we get this intersection being the identity.

What we need to show is that $A(s)A(t) \cap A(u)$ is the identity when none of s, t, u equal ∞ .

Suppose that for elements $(\gamma_{y_t} \otimes \alpha, g(\alpha, t)) \in A(t)$ and $(\gamma_{y_u} \otimes \alpha, g(\alpha, u)) \in A(u)$ we have the product

$$(\gamma_{y_t} \otimes \alpha, g(\alpha, t)) \cdot (\gamma_{y_u} \otimes \alpha, g(\alpha, u)) = (\alpha + \beta, y_t \alpha + y_u \beta, g(\alpha, t) + g(\beta, u) + y_t(\alpha \circ \beta))$$

is contained in $A(v)$. Then the following two conditions must be satisfied:

1. $y_t \alpha + y_u \beta = y_v(\alpha + \beta)$, or $(y_t + y_u)\alpha = (y_u + y_v)\beta = \gamma$ for some $\gamma \in \mathbb{F}^2$;
2. $g(\alpha, t) + g(\beta, u) + y_t(\alpha \circ \beta) = g(\alpha + \beta, v)$.

From condition 1, we get $\alpha = (y_t + y_u)^{-1}\gamma$ and $\beta = (y_u + y_v)^{-1}\gamma$. Then

using the definition of “ \circ ” we now get

$$\begin{aligned}
\alpha \circ \beta &= ((y_t + y_u)^{-1}\gamma)P((y_u + y_v)^{-1}\gamma)^T \\
&= (y_t + y_u)^{-1}(y_u + y_v)^{-1}\gamma P\gamma^T \\
&= (y_t + y_u)^{-1}(y_u + y_v)^{-1} \cdot 0 \\
&= 0
\end{aligned}$$

where the third equality holds since \circ is an alternating form. Now using condition 1, $\alpha \circ \beta = 0$, and the equation labeled $(*)$ for condition 2 we get

$$\begin{aligned}
0 &= g(\alpha, t) + g(\beta, u) + g(\alpha, v) + g(\beta, v) \\
&= (y_t + y_u)^{-2}(g(\gamma, t) + g(\gamma, v)) + (y_u + y_v)^{-2}(g(\gamma, u) + g(\gamma, v)) \\
&= \gamma B \gamma^T
\end{aligned}$$

where $B = \begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix}$ is the matrix

$$B = \begin{pmatrix} \frac{x_t + x_v}{(y_t + y_v)^2} + \frac{x_u + x_v}{(y_u + y_v)^2} & \frac{y_t + y_v}{(y_t + y_v)^2} + \frac{y_u + y_v}{(y_u + y_v)^2} \\ 0 & \frac{z_t + z_v}{(y_t + y_v)^2} + \frac{z_u + z_v}{(y_u + y_v)^2} \end{pmatrix}$$

Easy computations show that

$$\begin{aligned}
XZ &= x_t z_t (y_v + y_u)^4 + x_u z_u (y_t + y_v)^4 + x_v z_v (y_t + y_u)^4 \\
&\quad + (x_t z_u + x_u z_t) (y_v + y_t)^2 (y_v + y_u)^2 \\
&\quad + (x_t z_v + x_v z_t) (y_u + y_t)^2 (y_v + y_u)^2 \\
&\quad + (x_u z_v + x_v z_u) (y_u + y_t)^2 (y_v + y_t)^2
\end{aligned}$$

and

$$Y^2 = (y_t + y_u)^2 (y_t + y_v)^2 (y_u + y_v)^2$$

Hence

$$\begin{aligned}
tr(XZ/Y^2) &= tr \left(\frac{(x_t + x_u)(z_t + z_u)}{(y_t + y_u)^2} + \frac{(x_t + x_v)(z_t + z_v)}{(y_t + y_v)^2} + \frac{(x_u + x_v)(z_u + z_v)}{(y_u + y_v)^2} \right) \\
&= tr \left(\frac{(x_t + x_u)(z_t + z_u)}{(y_t + y_u)^2} \right) + tr \left(\frac{(x_t + x_v)(z_t + z_v)}{(y_t + y_v)^2} \right) + \\
&\quad + tr \left(\frac{(x_u + x_v)(z_u + z_v)}{(y_u + y_v)^2} \right) \\
&\equiv 1
\end{aligned}$$

since $A_t + A_u$, $A_t + A_v$, and $A_u + A_v$ are anisotropic matrices.

We have just shown that B is an anisotropic matrix and so $\gamma B \gamma^T = 0$ if and only if $\gamma = (0, 0)$. Using $\gamma = (0, 0)$, condition (i) forces $\alpha = \beta = (0, 0)$. So the only element, $(\gamma_{y_t} \otimes \alpha, g(\alpha, t)) \in A(t)$ and $(\gamma_{y_u} \otimes \alpha, g(\alpha, u)) \in A(u)$, whose product is contained in $A(v)$ is $(0, 0, 0)$, which is the identity and property $K2$ holds. Since both $K1$ and $K2$ hold, $\mathcal{J}(C)$ is a 4-gonal family for G^\otimes .

■

1.9 A Construction of the Hermitian Surface $H(3, q^2)$

Let $\mathbb{F} = GF(q)$, where $q = 2^e$, and fix a $\delta \in \mathbb{F}$ such that $tr(\delta) = 1$. For each $t \in \mathbb{F}$, put $A_t = \begin{pmatrix} t^{1/2} \cdot \delta & t^{1/2} \\ 0 & t^{1/2} \cdot \delta \end{pmatrix}$. Then,

$$\begin{aligned} tr \left[\frac{(s^{1/2}\delta - t^{1/2}\delta)(s^{1/2}\delta - t^{1/2}\delta)}{(s^{1/2} - t^{1/2})^2} \right] &= tr(\delta^2) \\ &= tr(\delta) \\ &= 1 \end{aligned}$$

and $\mathcal{C} = \{A_t : t \in \mathbb{F}\}$ is a q -clan. Put $A_\infty = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Then as in section 1.8, for each $t \in \tilde{\mathbb{F}} = \mathbb{F} \cup \infty$, define the subgroup $A(t)$ as

$$A(t) = \{(\gamma_t \otimes \alpha, g(\alpha, t)) : \alpha \in \mathbb{F}^2\}$$

Clearly, $A(t) \leq A^*(t)$ where

$$A^*(t) = \{(\gamma_t \otimes \alpha, c) : \alpha \in \mathbb{F}^2, c \in \mathbb{F}\}$$

Let $\mathcal{J}(\mathcal{C}) = \{A(t) : t \in \tilde{\mathbb{F}}\}$ and $\mathcal{J}^*(\mathcal{C}) = \{A^*(t) : t \in \tilde{\mathbb{F}}\}$.

Theorem 1.9.1 (S.E. Payne and J.A. Thas) *If $(G^\otimes, \mathcal{J}(\mathcal{C}), \mathcal{J}^*(\mathcal{C}))$ a Kantor family, as prescribed above, let $\mathcal{S} = GQ(\mathcal{C})$ be the corresponding EGQ. Then \mathcal{S} is a $GQ(q^2, q)$ isomorphic to the Hermitian surface $H(3, q^2)$.*

Proof: See Theorem A.3 in Appendix A.

■

1.10 Regularity in $H(3, q^2)$

Let $Q(5, q)$ be an elliptic quadric of $PG(5, q)$. It can be shown that $Q(5, q)$ is a GQ of order (q, q^2) .

Theorem 1.10.1 *The quadrangle $Q(5, q)$ is isomorphic to the point-line dual of $H(3, q^2)$.*

Proof: See Theorem A.4 in Appendix A. ■

Theorem 1.10.2 *Any pair of lines in $Q(5, q)$ is a regular pair.*

Proof: The 3-space defined by any pair of non-concurrent lines of $Q(5, q)$ intersects $Q(5, q)$ in an hyperbolic quadric (or regulus), and so it is clear that any pair of lines of $Q(5, q)$ is a regular pair. ■

Corollary 1.10.3 *Every point of $H(3, q^2)$ is a regular point.*

Let \mathcal{S} be $H(3, q^2)$ with elation point (∞) , as constructed by Payne. If we can find an whorl about (∞) which is not an elation and is an involution, it will follow from Theorem 1.4.2 that a $Sylow_2$ subgroup of the group of whorls about the point (∞) in $H(3, q^2)$ will have size $2q^5$.

2. Main Results

From here on we assume that $q = 2^e$ and that \mathcal{S} is the Hermitian surface $H(3, q^2)$ constructed as in Theorem 1.9.1. Suppose that W is the entire group of whorls about the point (∞) . We note that any elation group must be a 2-group, and furthermore, all Sylow 2-subgroups are conjugate in W . We aim to find a Sylow 2-subgroup of W which we call S_2 . Then contained in S_2 we are looking to find a subgroup $E \leq S_2$, of elations about (∞) , such that E is not isomorphic to the regular elation group (which we will denote \overline{G}) of \mathcal{S} . Clearly, such a group will have index $[E : S_2] = 2$, and thus be normal in S_2 .

2.1 Forming a Sylow₂ Subgroup in the Group of Whorls

For all $(\alpha, \beta, c) \in G^\otimes$, define the map $[\alpha, \beta, c] : G^\otimes \mapsto G^\otimes$ so that $(\alpha', \beta', c')^{[\alpha, \beta, c]} = (\alpha', \beta', c') \cdot (\alpha, \beta, c) = (\alpha' + \alpha, \beta' + \beta, c' + c + \beta' \circ \alpha)$. Let $\overline{G} = \{[\alpha, \beta, c] : (\alpha, \beta, c) \in G^\otimes\}$. Then \overline{G} is the regular elation group of \mathcal{S} . Next, define the involution $\phi : G^\otimes \mapsto G^\otimes$ so that for $(\alpha, \beta, c) \in G^\otimes$ we have $(\alpha, \beta, c)^\phi = (\alpha P, \beta P, c)$. The map ϕ is a whorl of W about the point (∞) . Next, consider the following computations.

$$\begin{aligned}
(\alpha, \beta, c)^{\phi \circ [\alpha', \beta', c'] \circ \phi} &= (\alpha P, \beta P, c)^{[\alpha', \beta', c'] \circ \phi} \\
&= (\alpha P + \alpha', \beta P + \beta', c + c' + \beta P \circ (\alpha' P)^T)^{\phi} \\
&= (\alpha P + \alpha', \beta P + \beta', c + c' + \beta P \circ P^T \alpha'^T)^{\phi} \\
&= (\alpha P + \alpha', \beta P + \beta', c + c' + \beta \circ \alpha')^{\phi} \\
&= ((\alpha P + \alpha')P, (\beta P + \beta')P, c + c' + \beta \circ \alpha') \\
&= (\alpha + \alpha' P, \beta + \beta' P, c + c' + \beta \circ \alpha') \\
&= (\alpha, \beta, c)^{[\alpha' P, \beta' P, c']}
\end{aligned}$$

Note: Because $(\alpha P, \beta P, c) = (\alpha, \beta, c)^{\phi}$, we will denote $[\alpha' P, \beta' P, c']$ by $[\alpha', \beta', c']^{\phi}$.

We have shown that $\phi \circ [\alpha', \beta', c'] \circ \phi = [\alpha, \beta, c]^{\phi} \in \overline{G}$. That is, the map ϕ normalizes \overline{G} in the group of whorls about (∞) , and we can define the semi-direct product $S_2 = \overline{G} \rtimes \langle \phi \rangle$.

Remark 2.1.1 *The group S_2 is a Sylow₂ subgroup of W .*

A typical element in S_2 can be identified as $[\alpha, \beta, c] \circ \phi^i$, where $i = 0, 1$. That is, an element of S_2 should be thought of as the composition of the maps $[\alpha, \beta, c]$ and ϕ^i . We now investigate products of elements in S_2 , where multiplication of elements is simply composition of functions. We have the following possible products:

1. It is trivial to see that

$$[\alpha, \beta, c] \cdot [\alpha', \beta', c'] = [\alpha + \alpha', \beta + \beta', c + c' + \alpha' \circ \beta]$$

Therefore, it makes sense to define the following:

$$\left[(\alpha, \beta, c) \cdot (\alpha', \beta', c') \right] := [\alpha, \beta, c] \cdot [\alpha', \beta', c']$$

2. It is also easy to see that

$$[\alpha, \beta, c] \cdot [\alpha', \beta', c'] \circ \phi = \left[(\alpha, \beta, c) \cdot (\alpha', \beta', c') \right] \circ \phi$$

3. It takes a bit more work to show that

$$[\alpha, \beta, c] \circ \phi \cdot [\alpha', \beta', c'] \circ \phi = \left[(\alpha, \beta, c) \cdot (\alpha', \beta', c') \right]^\phi$$

We start with

$$(x, y, z)^{[\alpha, \beta, c] \circ \phi} = \left((x + \alpha)P, (y + \beta)P, z + c + y \circ \alpha \right)$$

Then we compute

$$\begin{aligned} & \left((x + \alpha)P, (y + \beta)P, z + c + y \circ \alpha \right)^{[\alpha', \beta', c'] \circ \phi} \\ &= \left[(x + \alpha)P + \alpha', (y + \beta)P + \beta', z + c + y \circ \alpha \right. \\ & \quad \left. + c' + (y + \beta)P \circ \alpha' \right]^\phi \\ &= \left[x + \alpha + \alpha'P, y + \beta + \beta'P, z + c + c' \right. \\ & \quad \left. + y \circ \alpha + (y + \beta)P \circ \alpha' \right] \\ &= (x, y, z) \cdot g^* \end{aligned}$$

where $g^* = (\alpha, \beta, c) \cdot (\alpha'P, \beta'P, c')$.

That is,

$$[\alpha, \beta, c] \circ \phi \cdot [\alpha', \beta', c'] \circ \phi = [(\alpha, \beta, c) \cdot (\alpha', \beta', c')^\phi]$$

4. Using the computations above we can also show the following:

$$[\alpha, \beta, c] \circ \phi \cdot [\alpha', \beta', c'] = [(\alpha, \beta, c) \cdot (\alpha', \beta', c')^\phi] \circ \phi$$

To see this we rewrite the element

$$\left((x + \alpha)P + \alpha', (y + \beta)P + \beta', z + c + y \circ \alpha + c' + (y + B)P \circ \alpha' \right)$$

in the following form.

$$\left(x + \alpha + \alpha'P, y + \beta + \beta'P, z + c + y \circ \alpha + c' + (y + B)P \circ \alpha' \right)^\phi$$

This can be done since ϕ is an involution.

Using these results we can now rewrite products of arbitrary elements of \mathcal{S} in the typical representation of elements of \mathcal{S} as follows.

$$[\alpha, \beta, c] \circ \phi^j \cdot [\alpha', \beta', c'] \circ \phi^i = [(\alpha, \beta, c) \cdot (\alpha', \beta', c')^{\phi^j}] \circ \phi^{j+i}$$

It is now easy to obtain the following theorem.

Theorem 2.1.2 Let $\mathbb{F} = GF(q)$ where $q = 2^e$. Put $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and let \bar{G} be the usual group of elations of $H(3, q^2)$ about the point (∞) . If ϕ is the involution such that $(\alpha, \beta, c)^\phi = (\alpha P, \beta P, c)$, then every non-identity element in $\mathcal{S}_2 = \bar{G} \times \langle \phi \rangle$ has order two, or four.

Proof: Choose an arbitrary element $id \neq g = \pi(\alpha, \beta, c) \circ \phi^i \in \mathcal{S}$. If i is even then

$$\begin{aligned} g^2 &= [\alpha, \beta, c] \circ \phi^i \cdot [\alpha, \beta, c] \circ \phi^i \\ &= [\alpha, \beta, c] \cdot (\alpha, \beta, c) \circ \phi^{2i} \\ &= [\bar{0}, \bar{0}, \beta P \alpha^T] \end{aligned}$$

Then $g^2 = \{id\}$ iff $\{\alpha, \beta\}$ is \mathbb{F} -dependent, and we always have $g^4 = \{id\}$. Now suppose that i is odd.

$$\begin{aligned} g^2 &= [\alpha, \beta, c] \circ \phi^i \cdot [\alpha, \beta, c] \circ \phi^i \\ &= [\alpha, \beta, c] \cdot [\alpha, \beta, c]^\phi \circ \phi^{2i} \\ &= [\alpha + \alpha P, \beta + \beta P, \beta P \alpha^T] \\ &= [\gamma, \sigma, \alpha_1 \beta_2 + \alpha_2 \beta_1] \end{aligned}$$

where $\gamma = (a, a)$, $\sigma = (b, b)$, and $a = \alpha_1 + \alpha_2 \in \mathbb{F}$ and $b = \beta_1 + \beta_2 = ca$ for some $c \in \mathbb{F}$. So $\{\gamma, \sigma\}$ is an \mathbb{F} -dependent set and we easily see that $g^4 = id$. ■

Theorem 2.1.3 *There are $q^4 - 1$ involutions in S_2 .*

Proof: Suppose that $\pi(\alpha, \beta, c) \circ \phi^i \in \mathcal{S}$ has order two. Then

$$\begin{aligned} [\alpha, \beta, c] \circ \phi^i \cdot [\alpha, \beta, c] \circ \phi^i &= [(\alpha, \beta, c) \cdot (\alpha, \beta, c)^{\phi^i}] \circ \phi^{2i} \\ &= [(\alpha, \beta, c) \cdot (\alpha, \beta, c)^{\phi^i}] \\ &= [\bar{0}, \bar{0}, 0] \end{aligned}$$

Case 1. $i = 2k$:

$$\begin{aligned} (\alpha, \beta, c) \cdot (\alpha, \beta, c)^{\phi^i} &= (\alpha, \beta, c) \cdot (\alpha, \beta, c) \\ &= (\bar{0}, \bar{0}, \beta \circ \alpha) \end{aligned}$$

which equals zero if and only if $\{\alpha, \beta\}$ is an \mathbb{F} -dependent set; i.e., $\beta = t\alpha$ for some $t \in \mathbb{F}$. So for each fixed $\alpha \neq \bar{0}$ there are q choices for each c and t . This gives us a total of $(q^2 - 1)q^2 = q^4 - q^2$ elements of order 2.

Case 2. $i = 2k + 1$:

If $\alpha = (a_1, a_2)$ and $\beta = (b_1, b_2)$, then we get

$$\begin{aligned} [\alpha, \beta, c] \cdot (\alpha, \beta, c)^{\phi} &= \left[\left((a_1, a_2), (b_1, b_2), c \right) \cdot \left((a_1, a_2)P, (b_1, b_2)P, c \right) \right] \\ &= \left[\left((a_1, a_2), (b_1, b_2), c \right) \cdot \left((a_2, a_1), (b_2, b_1), c \right) \right] \\ &= \left[(a_1 + a_2, a_1 + a_2), (b_1 + b_2, b_1 + b_2), a_1b_2 + a_2b_1 \right] \end{aligned}$$

This equals $[\bar{0}, \bar{0}, 0]$ if and only if $a_1 = a_2$ and $b_1 = b_2$. So we get $q^2 - 1$ choices for α and β , both not equal to $(0, 0)$.

Adding the two cases we get $q^4 - 1$ involutions in S_2 .

■

Corollary 2.1.4 *There are $2q^5 - q^4$ elements of order four in S_2 .*

2.2 Elation Groups of $H(3, q^2)$ As Subgroups of S_2

We first look into the group S_2 and determine which elements are not elations about (∞) .

Theorem 2.2.1 *The only elements in S_2 that fix any points not collinear with (∞) are the conjugates of ϕ .*

Proof: Suppose that Q is a point opposite (∞) that is fixed by ϕ . As S_2 is a group of whorls about (∞) and $\bar{G} \leq S_2$, the size of the orbit of Q under S_2 is exactly q^5 .

From the orbit stabilizer theorem we also know that

$$\frac{|S_2|}{|(S_2)_Q|} = \text{size of the orbit of } Q \text{ under } S_2$$

We immediately get $|(S_2)_Q| = 2$. But since $\phi \in (S_2)_Q$ we must have $(S_2)_Q = \{id, \phi\}$.

Now choose any point Q' opposite (∞) . Because \overline{G} acts regularly on points not collinear with (∞) , there is a unique $g \in \overline{G}$ such that $Q'^g = Q$. So $(Q')^{g\phi g^{-1}} = Q'$. Thus $g\phi g^{-1} \in S_{Q'}$ and using the orbit-stabilizer theorem again we get $S_{Q'} = \{id, g\phi g^{-1}\}$.

■

Corollary 2.2.2 *A subgroup $E \leq S_2$, with $|E| = q^5$, is an elation group of $H(3, q^2)$ if and only if E contains no conjugates of ϕ .*

Observation 2.2.3 *See that $g\phi g^{-1} = g\phi g^{-1}\phi^{-1}\phi = [g, \phi] \cdot \phi$. It appears that all non-elations will be in a coset of the commutator subgroup containing ϕ .*

First we determine what the conjugates of ϕ look like in the group S_2 .

Let $g = (\alpha, \beta, c) \in G^\otimes$. Its easy to show that $g^{-1} = (\alpha, \beta, c + \beta \circ \alpha)$. Then $[\alpha, \beta, c] \cdot [\alpha, \beta, c + \beta \circ \alpha] = [(\alpha, \beta, c) \cdot (\alpha, \beta, c + \beta \circ \alpha)] = [\overline{0}, \overline{0}, 0] = id \in S_2$. So conjugates of ϕ can be written as follows:

$$\begin{aligned}
[\alpha, \beta, c] \cdot \phi \cdot [\alpha, \beta, c + \beta \circ \alpha] &= [\alpha, \beta, c] \cdot [\overline{0}, \overline{0}, 0] \circ \phi \cdot [\alpha, \beta, c + \beta \circ \alpha] \\
&= [\alpha, \beta, c] \circ \phi \cdot [\alpha, \beta, c + \beta \circ \alpha] \\
&= [(\alpha, \beta, c) \cdot (\alpha P, \beta, P, c + \beta \circ \alpha)] \circ \phi \\
&= [\alpha + \alpha P, \beta + \beta P, c + c + \beta \circ \alpha + \beta \circ \alpha P] \circ \phi \\
&= [\alpha + \alpha P, \beta + \beta P, \beta \circ \alpha + \beta \circ \alpha P] \circ \phi
\end{aligned}$$

It is easy to see that $\alpha + \alpha P = (a, a)$ and $\beta + \beta P = (b, b)$ for some $a, b \in \mathbb{F}$.

Furthermore, we also have $\beta \circ \alpha + \beta \circ \alpha P = ab$, so we can simplify this last term to the following

$$\left[(a, a), (b, b), ab \right] \circ \phi$$

It follows that there are at most q^2 elements in S_2 that are not elations.

Before we determine all elation groups contained in S_2 we will need some results from the theory of groups.

Theorem 2.2.4 *Given a group G , the commutator subgroup, $G' = [G, G]$, is a normal subgroup of G . Moreover, if $H \triangleleft G$, then G/H is abelian if and only if $G' \leq H$.*

Proof: For completeness we include the proof from [26].

A subgroup G' is normal in G if and only if for every $g \in G$, all conjugates ghg^{-1} remain in G' . Therefore, if $G' \leq G$, then $G' \triangleleft G$ if and only if $\gamma(G') \leq G'$ for every conjugation γ .

Let f be a homomorphism, $f : G \mapsto G$. Then $f[a, b] = [fa, fb]$. It follows that $f(G') \leq G'$. But conjugation is a homomorphism from G to G . So the commutator subgroup is a normal subgroup in G .

Next, suppose that $H \triangleleft G$. If G/H is abelian then $HaHb = HbHa$ for all $a, b \in G$. So $Hab = Hba$. So, $ab(ba)^{-1} = aba^{-1}b^{-1} = [a, b] \in H$ and $G' \leq H$. Conversely, suppose that $G' \leq H$. Then $ab(ba)^{-1} \in H$ and $Hab = Hba$ which

implies $HaHb = HbHa$. ■

We know that $[S_2 : \overline{G}] = 2$ and so $\overline{G} \triangleleft S_2$. Furthermore, the quotient group S/\overline{G} has order 2 and so must be cyclic and abelian. It follows that the commutator subgroup is contained in \overline{G} .

It turns out that all elements that are not elations will be in the coset of the commutator subgroup containing ϕ . We show this and that the quotient group S_2/S'_2 is an elementary abelian group of order $2q^2$. We will then be able to employ the following theorem.

Theorem 2.2.5 (Correspondence Theorem) *Let $K \triangleleft G$ and let $\nu : G \mapsto G/K$ be the natural map. Then $S \mapsto \nu(S) = S/K$ is a bijection from the family of all the subgroups S of G which contain K to the family of all subgroups of G/K . Moreover, if we denote S/K by S^* , then:*

1. $T \leq S$ if and only if $T^* \leq S^*$, and then $[S : T] = [S^* : T^*]$;
2. $T \triangleleft S$ if and only if $T^* \triangleleft S^*$, and then $S/T \cong S^*/T^*$.

This ensures that finding a subgroup of index 2 that does not contain the non-elation elements will be the same as finding a subgroup of S_2/S'_2 that does not contain the elements corresponding the commutator subgroup coset containing ϕ . First we form the commutator subgroup.

2.3 The Commutator Subgroup

Our main goal in this section is to show that the commutator subgroup equals the Frattini subgroup, denoted $\Phi(S_2)$, which is the intersection of all maximal subgroups. Then given this result, the quotient group S_2/S'_2 is elementary abelian and therefore a vector space over $GF(q)$.

We first need to form the inverse of a general element in \mathcal{S} . Let $g = [\alpha, \beta, c] \circ \phi$. Then if $\alpha = (a_1, a_2)$ and $\beta = (b_1, b_2)$ we get

$$\begin{aligned} g^{-1} &= \left[(a_2, a_1), (b_2, b_1), c + a_1b_2 + a_2b_1 \right] \circ \phi \\ &= \left[\alpha P, \beta P, c + \beta \circ \alpha \right] \circ \phi \end{aligned}$$

If $g = [\alpha', \beta', c']$ then

$$g'^{-1} = \left[\alpha', \beta', c' + \beta' \circ \alpha' \right]$$

We can use this information to create all commutators. Let $g = [\alpha, \beta, c] \circ \phi^i$ and $g' = [\alpha', \beta', c'] \circ \phi^j$, and suppose that $\alpha = (a_1, a_2)$, $\alpha' = (a'_1, a'_2)$, $\beta = (b_1, b_2)$, and $\beta' = (b'_1, b'_2)$. We have a number of cases. First, if i is odd and j is even then

$$[g, g'] = \left[(\bar{a}, \bar{a}), (\bar{b}, \bar{b}), b'_1(a_1 + \bar{a}) + b'_2(a_2 + \bar{a}) + \beta\alpha'^T \right]$$

where $\bar{a} = a'_1 + a'_2$ and $\bar{b} = b'_1 + b'_2$. Now see that if $\bar{a} = \bar{b} = \bar{0}$ we get

$$\begin{aligned} [g, g'] &= [\bar{0}, \bar{0}, b'_1 a_1 + b'_2 a_2 + b_1 a'_1 + b_2 a'_2] \\ &= [\bar{0}, \bar{0}, b'_1(a_1 + a_2) + a'_1(b_1 + b_2)]. \end{aligned}$$

But we can choose $b'_1, b_1, b_2, a'_1, a_1, a_2$ to obtain any element in \mathbb{F} . Therefore, all possible elements of the form $[\bar{0}, \bar{0}, c]$, which are all in the center of S_2 , are contained in the commutator subgroup. That is, if an element $[\alpha, \beta, c] \circ \phi^i$ is in S'_2 , then $[\alpha, \beta, c^*] \circ \phi^i \in S'_2$ for all $c^* \in \mathbb{F}$.

From now all our computations will neglect the third coordinate. If i is even and j is odd we get

$$[g, g'] = [(\hat{a}, \hat{a}), (\hat{b}, \hat{b}), *]$$

where $\hat{a} = a_1 + a_2$ and $\hat{b} = b_1 + b_2$.

The next case is for i and j even. Then

$$[g, g'] = [\bar{0}, \bar{0}, *]$$

The final case is for i and j both odd. We get

$$[g, g'] = [\bar{0}, \bar{0}, *]$$

All products of commutators will yield an element of the form $[(a, a), (b, b), *]$, and we can then multiply this element by an element in the center of S_2 . We have shown the following result.

Theorem 2.3.1 *The commutator subgroup S'_2 is the set of all elements of the form*

$$\left[(a, a), (b, b), c \right], \text{ where } a, b, c \in \mathbb{F}$$

Furthermore, the commutator subgroup has size q^3 .

To show that $S'_2 = \Phi(S_2)$ we need some additional group theoretic results.

Lemma 2.3.2 (Frattini Argument) *Let K be a normal subgroup of a finite group G . If P is a Sylow p -subgroup of K (for some prime p), then*

$$G = KN_G(P).$$

Proof: For completeness we include the proof from [26].

If $g \in G$, then $gPg^{-1} \leq gKg^{-1} = K$. It follows that gPg^{-1} is a Sylow p -subgroup of K , and so there exists a $k \in K$ such that $kPk^{-1} = gPg^{-1}$. Hence, $P = (k^{-1}g)P(k^{-1}g)^{-1}$, so that $k^{-1}g \in N_G(P)$. Therefore, we can factor as $g = k(k^{-1}g)$. ■

Lemma 2.3.3 *If G is a nilpotent group, then every maximal subgroup is normal in G .*

Proof: Let M be a maximal subgroup of G . Since $M \leq N_G(M)$, we get $N_G(M) = G$. ■

Theorem 2.3.4 *Let G be a finite group.*

1. $\Phi(G)$ is nilpotent.
2. If G is a p -group, then $\Phi(G) = G'G^p$ where G' is the commutator subgroup, and G^p is the subgroup of G generated by all p^{th} powers.
3. If G is a finite p -group, then $G/\Phi(G)$ is a vector space over \mathbb{Z}_p .

Proof: For completeness, we include the proof from [26].

1. Let P be a Sylow p -subgroup of $\Phi(G)$ for some p . Then since $\Phi(G) \triangleleft G$, the Frattini argument gives $G = \Phi(G)N_G(P)$. But $\Phi(G)$ consists of non-generators, and so $G = N_G(P)$. So $P \triangleleft G$ implies that $P \triangleleft \Phi(G)$. Since P was an arbitrary Sylow p -subgroup we must have $\Phi(G)$ the direct product of its Sylow p -subgroups. But all p -groups are nilpotent, and their direct product is then also nilpotent, and $\Phi(G)$ is nilpotent.

2. If M is a maximal subgroup of G , then $M \triangleleft G$ and $[G : M] = p$. Thus G/M is abelian and $G' \leq M$; moreover, G/M has exponent p , so that $x^p \in M$ for all $x \in G$. Therefore, $G'G^p \in \Phi(G)$.

3. $|G| = p^n$. Since $G'G^p = \Phi(G)$, and hence $G' \leq \Phi(G)$, the quotient group $G/\Phi(G)$ is an abelian group. If M is any maximal subgroup it must have order p^{n-1} and so $|G/M| = p$. So the coset Mx has order p and so $M = (Mx)^p = Mx^p$ and $x^p \in M$. Now consider the coset $\Phi(G)x$ where $x \in G$. From above we have

$x^p \in \Phi(G)$ for all $x \in G$. It follows that $(\Phi(G)x)^p = \Phi(G)$ and $G/\Phi(G)$ is elementary abelian. ■

Theorem 2.3.5 *The quotient group S_2/S'_2 is a vector space over $GF(2)$.*

Proof: S_2 is a 2-group, and so we show that for every $g \in \mathcal{S}$, we have $g^2 \in S'_2$. If $g \in S_2$ has order 2, then $g^2 \in S'_2$. If $g \in \mathcal{S}$ has order 4, we have already shown that $g^2 = [(a, a), (b, b), c]$ where $a, b, c \in \mathbb{F}$. It is easy to see that the subgroup generated by all squares of elements in \mathcal{S} is contained in the commutator subgroup. So by Theorem 2.3.4 we get $S'_2 = \Phi(S_2)$ and S_2/S'_2 is a vector space over \mathbb{Z}_2 . ■

2.4 The Quotient Group \mathcal{S}/\mathcal{S}'

Elements in the quotient group will be representatives of the cosets of S'_2 . We can choose the representatives of the form $[(0, a), (0, b), 0] \circ \phi^i$ which would give us $2q^2 = |S_2/S'_2|$ representatives in S_2/S'_2 . It is easy to see that each representative is in a different coset of S'_2 . Furthermore, we will denote each of these coset representatives as triples (a, b, i) where $a, b \in GF(q)$ and $i \in \mathbb{Z}_2$. Then we can define the group operation in S_2/S'_2 by

$$(a, b, i) \cdot (c, d, j) = (a + c, b + d, i + j)$$

where addition is in the appropriate field. We note that $(0, 0, 1) \in S_2/S'_2$ corresponds to the coset containing ϕ .

2.5 Looking for Hyperplanes

Let $q = 2^e$ and treat $\mathbb{F} = GF(q)$ as an e -dimensional vector space over $GF(2)$. Then for a fixed $\zeta \in GF(q)^*$, the map

$$tr_{\zeta}(x) = \sum_{i=0}^{e-1} (\zeta x)^{2^i}$$

is a linear functional; i.e., $tr_{\zeta} : GF(q) \mapsto GF(2)$. Letting ζ vary over \mathbb{F}^* gives us exactly $q - 1$ non-zero linear functionals on \mathbb{F} . Given a linear map T on a vector space V we always have $dim(V) = dim \text{ null}(T) + dim \text{ range}(T)$. But $\text{range}(tr_{\zeta})$ is a one dimensional subspace, and so $\text{null}(T)$ is a hyperplane in \mathbb{F} . So for each $\zeta \in \mathbb{F}^*$ there is a unique hyperplane in \mathbb{F} . So we have $q - 1$ distinct hyperplanes. But each hyperplane corresponds to a non-zero vector in \mathbb{F} and there are exactly $q - 1$ such vectors in $GF(q)$. Hence $\{tr_{\zeta} : \zeta \in \mathbb{F}^*\}$ gives us all linear functionals on $GF(q)$.

Now choose a triple $(a, b, i) \in S_2/S'_2$. This is a vector space over $GF(2)$. Furthermore, the map

$$\Theta_{\zeta, \sigma}(a, b, i) = tr_{\zeta}(a) + tr_{\sigma}(b) + i$$

is a linear functional from S_2/S'_2 onto $GF(q)$. The kernel is a hyperplane and it is easy to see that the vector $(0, 0, 1)$ is not in the kernel of $\Theta_{\zeta, \sigma}$. This gives us q^2 hyperplanes of S_2/S'_2 without the forbidden element $(0, 0, 1)$.

If we then define the map $\Theta_{\zeta,\sigma}^*(a, b, i) = tr_{\zeta}(a) + tr_{\sigma}(b)$ we get the other q^2 hyperplanes of S_2/S'_2 , each one containing the element $(0, 0, 1)$. We have accounted for all $2q^2$ linear functionals on S_2/S'_2 . It follows that all elation subgroups of S_2 will correspond to the q^2 hyperplanes from the kernels of the maps $\Theta_{\zeta,\sigma}$. It is worth noting that when $\zeta = \sigma = 0$ the elation group is the familiar example.

We can now give an explicit description of all elation groups in the Sylow 2-subgroup S_2 of the group of whorls of $H(3, q^2)$. The hyperplanes in S_2/S'_2 are the kernels of the maps $\Theta_{\zeta,\sigma}$. In other words, for a fixed pair, $\zeta, \sigma \in GF(q)$ (both not zero) one hyperplane is the set of all $(a, b, i) \in S_2/S'_2$ such that $\theta_{\zeta}(a) + \theta_{\sigma}(b) + i = 0$. To pull back to the original group S_2 we simply ask which coset of S'_2 contains the general element $[(a_1, a_2), (b_1, b_2), c] \circ \phi^i$. It is the coset $S'_2 \cdot [(0, a_2 + a_1), (0, b_2 + b_1), 0] \phi^i$. This is summarized in the following theorem.

Theorem 2.5.1 *Let S_2 be the above mentioned Sylow 2-subgroup of the group of whorls of $H(3, q^2)$. Fix two elements $\zeta, \sigma \in GF(q)$ and put $\Theta_{\zeta,\sigma}(a, b, i) = tr_{\zeta}(a) + tr_{\sigma}(b) + i$. Then there is an elation group $E_{\zeta,\sigma} \leq S_2$ where*

$$E_{\zeta,\sigma} = \left\{ [(a_1, a_2), (b_1, b_2), c] \circ \phi^i : \Theta_{\zeta,\sigma}(a_1 + a_2, b_1 + b_2, i) = 0 \right\}$$

For each case where at least one of ζ or σ is non-zero, we will call these corresponding $q^2 - 1$ elation groups of $H(3, q^2)$ “exotic” elation groups. When $\zeta = \sigma = 0$ we will call the group the “familiar” elation group of $H(3, q^2)$.

We will say that the ordered pair $\{\zeta, \sigma\}$ defines the group E . We would like to simplify the notation. Fix $\zeta, \sigma \in GF(q)$, and for each pair $\alpha, \beta \in GF(q) \times GF(q)$, define the function $\widehat{\alpha + \beta} : GF(q) \times GF(q) \mapsto GF(2)$ to be $\widehat{\alpha + \beta} = tr_\zeta(\alpha) + tr_\sigma(\beta)$. If we then use the notation

$$a^{\widehat{\alpha + \beta}} = aP^{\widehat{\alpha + \beta}}$$

we can redefine the group $E_{\zeta, \sigma}$ as

$$E_{\zeta, \sigma} = \left\{ \left[\alpha, \beta, c \right]_{\zeta, \sigma} : \alpha, \beta \in GF(q) \times GF(q), c \in GF(q) \right\}$$

with the group operation

$$\left[\alpha, \beta, c \right]_{\zeta, \sigma} * \left[\alpha', \beta', c' \right]_{\zeta, \sigma} = \left[\alpha + \alpha^{\widehat{\alpha + \beta}}, \beta + \beta^{\widehat{\alpha + \beta}}, c + c' + \alpha^{\widehat{\alpha + \beta}} P \beta^T \right]_{\zeta, \sigma}$$

Next we show that these exotic elation groups are not isomorphic to the familiar elation group.

2.6 Lower central Series

Definition 2.6.1 Set $\Gamma_1(G) = G$, and $\Gamma_2(G) = [G, G]$. Inductively define $\Gamma_n = [\Gamma_{n-1}(G), G]$. The **lower central series** of a nilpotent group G is the normal series

$$G = \Gamma_1(G) \supseteq \Gamma_2(G) \supseteq \Gamma_3(G) \cdots \Gamma_n(G) = \{id\}$$

The length of the lower central series is the number of strict inclusions in the series. If the length of the series is n we say the group G has **nilpotency class n**. If two groups have different length central series then the two groups

are non-isomorphic. This follows since for any group automorphism σ we have $\sigma[a, b] = [\sigma(a), \sigma(b)]$.

Every p -group is nilpotent and has a lower central series. The group \overline{G} has class 2 since $\overline{G}' = [\overline{G}, \overline{G}] = Z(\overline{G})$ and every element in the commutator has order 2. We note that the group S_2 has nilpotency class greater than 2, since since S_2' is not abelian. We are interested in showing that each of these exotic elation groups has nilpotency class 3.

Observation 2.6.2 *Let $E = E_{\zeta, \sigma} \leq S_2$ be an exotic elation group of $H(3, q^2)$. Then*

$$E' = [E, E] = \left\{ [(a, a), (b, b), c] : c \in GF(q) \text{ and } tr_{\zeta}(a) + tr_{\sigma}(b) = 0 \right\}$$

Proof: We have already verified that $S_2' = \{ [(a, a), (b, b), c] : a, b, c \in \mathbb{F} \}$, and clearly $E' \subseteq S_2'$.

Put $g = [(a_1, a_2), (b_1, b_2), c] \circ \phi^i$ and $g' = [(a'_1, a'_2), (b'_1, b'_2), c'] \circ \phi^j$. If i and j are both odd, or both even, then $[g, g'] = [\overline{0}, \overline{0}, *]$. If i is odd and j is even, then $[g, g'] = [(a^*, a^*), (b^*, b^*), *]$ where $a^* = a'_1 + a_2$ and $b^* = b'_1 + b_2$. Since $g' \in E_{\zeta, \sigma}$ we have $tr_{\zeta}(a^*) + tr_{\sigma}(b^*) = 0$. The case with i even and j odd is the same. This completes the proof. ■

Note: It is easy to see that $|E'_{\zeta, \sigma}| = q^3/4$.

Theorem 2.6.3 *Let $E = E_{\zeta, \sigma} \leq S_2$ be an exotic elation group of $H(3, q^2)$. Then E has nilpotency class 3.*

Proof: We show this for $E = E_{1,1}$. The proof follows since $\{id\} \neq \Gamma_3(E) = [E', E] \in Z(E)$ whence $\Gamma_4(E) = \{id\}$. To show this consider $\Gamma_3(E) = \{[g, g'] : g \in E', g' \in E\}$. Let $g = [(a, a), (b, b), c]$ and $g' = [(\alpha_1, \alpha_2), (\beta_1, \beta_2), d] \circ \phi$. Then

$$\begin{aligned}
gg'g^{-1}g'^{-1} &= [(a, a), (b, b), c] \cdot [(\alpha_1, \alpha_2), (\beta_1, \beta_2), d] \circ \phi \cdot [(a, a), (b, b), c] \\
&\quad \cdot [(\alpha_2, \alpha_1), (\beta_2, \beta_1), d + \beta \circ \alpha] \circ \phi \\
&= [(a + \alpha_1, a + \alpha_2), (b + \beta_1, b + \beta_2), *] \circ \phi \\
&\quad \cdot [(a + \alpha_2, a + \alpha_1), (b + \beta_2, b + \beta_1), *] \circ \phi \\
&= [\bar{0}, \bar{0}, *] \\
&\in Z(E)
\end{aligned}$$

Similar computations show that when $g' = \pi [(\alpha_1, \alpha_2), (\beta_1, \beta_2), d]$ we still get $gg'g^{-1}g'^{-1} \in Z(E)$.

So we get the lower central series

$$E = \Gamma_1(E) \supset \Gamma_2(E) \supset \Gamma_3(E) \supset \Gamma_4(E) = \{id\}$$

The proof for all $E_{\zeta, \sigma} \neq E_{0,0}$ will follow once we show that $E_{\zeta, \sigma} \cong E_{\zeta', \sigma'}$ when at least one of ζ, σ are not equal to zero. ■

Theorem 2.6.4 *All of the $q^2 - 1$ “exotic” elation groups of $H(3, q^2)$ are pairwise isomorphic.*

Proof:

We saw in Appendix B that if $\phi = q$, then

$$W_2 = \left\{ \left(\begin{array}{cccc} 1 & \alpha & \beta & \mu \\ 0 & 1 & 0 & \bar{\beta} \\ 0 & 0 & 1 & \bar{\alpha} \\ 0 & 0 & 0 & 1 \end{array} \right) \circ \phi^i \in P\Gamma U(4, q^2) : \mu + \bar{\mu} + \alpha\bar{\beta} + \beta\bar{\alpha} = 0 \right\}$$

is a unitary representation of a Sylow₂ subgroup of the group of whorls about the point $p = (0, 0, 0, 1)$ in $H(3, q^2)$. We will use the following representation of this group.

$$W_2 = \{[\alpha, \beta, \mu] \circ \phi^i : \alpha\bar{\beta} + \beta\bar{\alpha} + \mu + \bar{\mu} = 0\}$$

with group operation

$$[\alpha, \beta, \mu] \circ \phi^i * [\alpha', \beta', \mu'] \circ \phi^j = [\alpha + \alpha'\phi^i, \beta + \beta'\phi^i, c + c'\phi^i + \alpha(\bar{\beta}')^{\phi^i} + \beta(\bar{\alpha}')^{\phi^i}] \circ \phi^{i+j}$$

Let $x = (1, a, b, c) \in P \setminus \{p^\perp\}$. Then, for any $id \neq g \in W_2$ we have

$$x^g = (1, (a + \alpha)^{q^i}, (b + \beta)^{q^i}, (c + \mu + a\bar{\beta} + b\bar{\alpha})^{q^i})$$

If $i = 0$, then $x^g \neq x$. If $i = 1$, then $x^g = x$ only if $\alpha = a + a^q$, $\beta = b + b^q$, and $\mu = 0$. That is, g is not an elation only if $\alpha, \beta \in GF(q)$, $\mu = 0$, and $i = 1$.

When we compute the commutator subgroup of W_2 we get

$$W'_2 = \{[a, b, c] : a, b, c \in GF(q)\}$$

So all non-relations in W_2 will be contained in the coset of the commutator subgroup containing ϕ .

We have $2q^2$ distinct coset representatives of W_2/W'_2 listed below (split into two sets of size q^2).

$$\{[\alpha, \beta, 0] : \alpha = (0, h), \beta = (0, k), h, k \in GF(q)\}$$

$$\{[\alpha, \beta, 0] \circ \phi : \alpha = (0, h), \beta = (0, k)h, k \in GF(q)\}$$

Since $GF(q^2) \cong GF(q) \times GF(q)$, there are no problems when considering each matrix entry to be in $GF(q) \times GF(q)$. Suppose that $\delta \in GF(q)$ with $tr(\delta) = 1$, and let i be a root of the polynomial $x^2 + x + \delta$. Then $i^q = i + 1$ is also a root of the polynomial. We can let any element in $\alpha \in GF(q) \times GF(q)$ be represented as $\alpha = a + bi$, where $a, b \in GF(q)$. It then easily follows that $tr(b) = tr(\alpha + \alpha^q)$.

Furthermore, we already know that W_2/W'_2 is a vector space over $GF(2)$. So if $\alpha = (\alpha_1, \alpha_2) \in GF(q) \times GF(q)$, and for some $\zeta \in GF(q)$ we let $T_\zeta(\alpha) = tr_\zeta(\alpha_1 + \alpha_2)$, we can define the q^2 linear functionals

$$T^* : W_2/W'_2 \mapsto GF(2) : [\alpha, \beta, 0] \circ \phi^i \mapsto T_\zeta(\alpha) + T_\sigma(\beta) + i$$

The element $[0, 0, 0] \circ \phi$ is in the kernel of T^* . It follows that

$$E_{\zeta, \sigma} = \{[\alpha, \beta, \mu] \circ \phi^{T_{\zeta}(\alpha) + T_{\sigma}(\beta)}\}$$

are q^2 elation groups of $H(3, q^2)$ about p . There are exactly q^2 elation groups about p in W_2 , and each $E_{\zeta, \sigma} \neq E_{0,0}$ must be one of the exotic elation groups about p .

As before, for a fixed $\zeta, \sigma \in GF(q)$, we will use the notation

$$a^{\frac{\zeta, \sigma}{\alpha + \beta}} = a^{\phi^{(T_{\zeta}(\alpha) + T_{\sigma}(\beta))}}$$

and redefine the group $E_{\zeta, \sigma}$ as

$$E_{\zeta, \sigma} = \{[\alpha, \beta, \mu]_{\zeta, \sigma} : \alpha\bar{\beta} + \beta\bar{\alpha} + \mu + \bar{\mu} = 0\}$$

with the following group operation.

$$[\alpha, \beta, \mu]_{\zeta, \sigma} * [\alpha', \beta', \mu']_{\zeta, \sigma} =$$

$$\left[\alpha + \alpha^{\frac{\zeta, \sigma}{\alpha + \beta}}, \beta + \beta^{\frac{\zeta, \sigma}{\alpha + \beta}}, \mu + \mu^{\frac{\zeta, \sigma}{\alpha + \beta}} + \alpha(\bar{\beta}')^{\frac{\zeta, \sigma}{\alpha + \beta}} + \beta(\bar{\alpha}')^{\frac{\zeta, \sigma}{\alpha + \beta}} \right]_{\zeta, \sigma}$$

Put $a^{\frac{1,0}{\alpha + \beta}} = a^{\widehat{\alpha}}$, $a^{\frac{0,1}{\alpha + \beta}} = a^{\widehat{\beta}}$, and $a^{\frac{1,1}{\alpha + \beta}} = a^{\widehat{\alpha + \beta}}$, and define the map Φ so that

$$\Phi : [\alpha, \beta, \mu]_{1,0} \mapsto [\alpha + \beta, \beta, \mu]_{1,1}$$

We show that Φ is a group isomorphism between $E_{1,0}$ and $E_{1,1}$, keeping in mind that Φ does not effect the required relationship on α, β, μ .

$$\begin{aligned}
& \left([\alpha, \beta, \mu]_{1,0} * [\alpha', \beta, \mu']_{1,0} \right)^\Phi \\
&= \left([\alpha + \alpha'^{\widehat{\alpha}}, \beta + \beta'^{\widehat{\alpha}}, \mu + \mu'^{\widehat{\alpha}} + \alpha(\bar{\beta}')^{\widehat{\alpha}} + \beta(\bar{\alpha}')^{\widehat{\alpha}}]_{1,0} \right)^\Phi \\
&= [\alpha + \alpha'^{\widehat{\alpha}} + \beta + \beta'^{\widehat{\alpha}}, \beta + \beta'^{\widehat{\alpha}}, \mu + \mu'^{\widehat{\alpha}} + \alpha(\bar{\beta}')^{\widehat{\alpha}} + \beta(\bar{\alpha}')^{\widehat{\alpha}}]_{1,1}
\end{aligned}$$

$$\begin{aligned}
& \left([\alpha, \beta, \mu]_{1,0} \right)^\Phi * \left([\alpha', \beta, \mu']_{1,0} \right)^\Phi \\
&= [\alpha + \beta, \beta, \mu]_{1,1} * [\alpha' + \beta', \beta', \mu']_{1,1} \\
&= [\alpha + \beta + (\alpha' + \beta')^{\widehat{\alpha'+\beta'+\beta'}}, \beta + \beta'^{\widehat{\alpha'+\beta'+\beta'}}, \mu + \mu'^{\widehat{\alpha'+\beta'+\beta'}} + \\
&\quad + (\alpha + \beta)(\bar{\beta}')^{\widehat{\alpha'+\beta'+\beta'}} + \beta(\bar{\alpha}' + \bar{\beta}')^{\widehat{\alpha'+\beta'+\beta'}}]_{1,1} \\
&= [\alpha + \alpha'^{\widehat{\alpha}} + \beta + \beta'^{\widehat{\alpha}}, \beta + \beta'^{\widehat{\alpha}}, \mu + \mu'^{\widehat{\alpha}} + \alpha(\bar{\beta}')^{\widehat{\alpha}} + \beta(\bar{\alpha}')^{\widehat{\alpha}}]_{1,1}
\end{aligned}$$

Next define the map Φ^* so that

$$\Phi^* : [\alpha, \beta, \mu]_{1,0} \longmapsto [\beta, \alpha, \mu]_{0,1}$$

We show that Φ^* is a group isomorphism between $E_{1,0}$ and $E_{0,1}$, keeping in mind that Φ^* does not affect the required relationship between α, β, μ .

$$\begin{aligned}
& \left([\alpha, \beta, \mu]_{1,0} * [\alpha', \beta, \mu']_{1,0} \right)^{\Phi^*} \\
&= \left([\alpha + \alpha'^{\widehat{\alpha}}, \beta + \beta'^{\widehat{\alpha}}, \mu + \mu'^{\widehat{\alpha}} + \alpha(\bar{\beta}')^{\widehat{\alpha}} + \beta(\bar{\alpha}')^{\widehat{\alpha}}]_{1,0} \right)^{\Phi^*} \\
&= [\beta + \beta'^{\widehat{\alpha}}, \alpha + \alpha'^{\widehat{\alpha}}, \mu + \mu'^{\widehat{\alpha}} + \alpha(\bar{\beta}')^{\widehat{\alpha}} + \beta(\bar{\alpha}')^{\widehat{\alpha}}]_{0,1}
\end{aligned}$$

$$\begin{aligned}
& \left([\alpha, \beta, \mu]_{1,0}\right)^{\Phi^*} * \left([\alpha', \beta, \mu']_{1,0}\right)^{\Phi^*} \\
&= [\beta, \alpha, \mu]_{0,1} * [\beta', \alpha', \mu]_{0,1} \\
&= [\beta + \beta'^{\widehat{\alpha}}, \alpha + \alpha'^{\widehat{\alpha}}, \mu + \mu'^{\widehat{\alpha}} + \alpha(\bar{\beta}')^{\widehat{\alpha}} + \beta(\bar{\alpha}')^{\widehat{\alpha}}]_{0,1}
\end{aligned}$$

Next, for $\delta \in GF(q)^*$ define the map Φ_δ so that

$$\Phi_\delta : [\alpha, \beta, \mu]_{1,0} \longmapsto [\delta^{-1}\alpha, \delta^{-1}\beta, \delta^{-2}\mu]_{\delta,0}$$

We show that Φ_δ is a group isomorphism between $E_{1,0}$ and $E_{\delta,0}$, keeping in mind that Φ_δ does not affect the required relationship between α, β, μ .

$$\begin{aligned}
& \left([\alpha, \beta, \mu]_{1,0} * [\alpha', \beta, \mu']_{1,0}\right)^{\Phi_\delta} \\
&= \left([\alpha + \alpha'^{\widehat{\alpha}}, \beta + \beta'^{\widehat{\alpha}}, \mu + \mu'^{\widehat{\alpha}} + \alpha(\bar{\beta}')^{\widehat{\alpha}} + \beta(\bar{\alpha}')^{\widehat{\alpha}}]_{1,0}\right)^{\Phi_\delta} \\
&= [\delta^{-1}(\alpha + \alpha'^{\widehat{\alpha}}), \delta^{-1}(\beta + \beta'^{\widehat{\alpha}}), \delta^{-2}\mu + \delta^{-2}\mu'^{\widehat{\alpha}} + \\
&\quad + \delta^{-2}\alpha(\bar{\beta}')^{\widehat{\alpha}} + \delta^{-2}\beta(\bar{\alpha}')^{\widehat{\alpha}}]_{\delta,0}
\end{aligned}$$

$$\begin{aligned}
& \left([\alpha, \beta, \mu]_{1,0}\right)^{\Phi_\delta} * \left([\alpha', \beta', \mu']_{1,0}\right)^{\Phi_\delta} \\
&= [\delta^{-1}\alpha, \delta^{-1}\beta, \delta^{-2}\mu]_{\delta,0} * [\delta^{-1}\alpha', \delta^{-1}\beta', \delta^{-2}\mu']_{\delta,0} \\
&= [\delta^{-1}(\alpha + \alpha'^{\widehat{\delta\delta^{-1}\alpha}}), \delta^{-1}(\beta + \beta'^{\widehat{\delta\delta^{-1}\alpha}}), \delta^{-2}\mu + \delta^{-2}\mu'^{\widehat{\delta\delta^{-1}\alpha}} + \\
&\quad + \delta^{-2}\alpha(\delta\bar{\beta}')^{\widehat{\delta\delta^{-1}\alpha}} + \delta^{-2}\beta(\delta\bar{\alpha}')^{\widehat{\delta\delta^{-1}\alpha}}]_{\delta,0} \\
&= [\delta^{-1}(\alpha + \alpha'^{\widehat{\alpha}}), \delta^{-1}(\beta + \beta'^{\widehat{\alpha}}), \delta^{-2}\mu + \delta^{-2}\mu'^{\widehat{\alpha}} + \\
&\quad + \delta^{-2}\alpha(\bar{\beta}')^{\widehat{\alpha}} + \delta^{-2}\beta(\bar{\alpha}')^{\widehat{\alpha}}]_{\delta,0}
\end{aligned}$$

It is easy to see that Φ_δ is also an isomorphism between $E_{0,1}$ and $E_{0,\delta}$. Next define the map $\Phi_{\zeta,\sigma}$ such that

$$\Phi_{\zeta,\sigma} : [\alpha, \beta, \mu]_{1,1} \longmapsto [\zeta^{-1}\alpha, \sigma^{-1}, \zeta^{-1}\sigma^{-1}\mu]_{\zeta,\sigma}$$

We show that $\Phi_{\zeta,\sigma}$ is a group isomorphism, keeping in mind that $\Phi_{\zeta,\sigma}$ does not affect the required relationship between α, β, μ .

$$\begin{aligned} & \left([\alpha, \beta, \mu]_{1,1} * [\alpha', \beta, \mu']_{1,1}\right)^{\Phi_{\zeta,\sigma}} \\ &= \left([\alpha + \alpha'^{\widehat{\alpha}}, \beta + \beta'^{\widehat{\alpha}}, \mu + \mu'^{\widehat{\alpha}} + \alpha(\bar{\beta}')^{\widehat{\alpha}} + \beta(\bar{\alpha}')^{\widehat{\alpha}}]_{1,1}\right)^{\Phi_{\zeta,\sigma}} \\ &= [\zeta^{-1}(\alpha + \alpha'^{\widehat{\alpha}}), \sigma^{-1}(\beta + \beta'^{\widehat{\alpha}}), \zeta^{-1}\sigma^{-1}(\mu + \mu'^{\widehat{\alpha}} + \alpha(\bar{\beta}')^{\widehat{\alpha}} + \beta(\bar{\alpha}')^{\widehat{\alpha}})]_{\zeta,\sigma} \\ & \\ & \left([\alpha, \beta, \mu]_{1,1}\right)^{\Phi_{\zeta,\sigma}} * \left([\alpha', \beta', \mu']_{1,1}\right)^{\Phi_{\zeta,\sigma}} \\ &= [\zeta^{-1}\alpha, \sigma^{-1}\beta, \zeta^{-1}\sigma^{-1}\mu]_{\zeta,\sigma} * [\zeta^{-1}\alpha', \sigma^{-1}\beta', \zeta^{-1}\sigma^{-1}\mu']_{\zeta,\sigma} \\ &= [\zeta^{-1}(\alpha + \alpha'^{\zeta\zeta^{-1}\widehat{\alpha+\sigma\sigma^{-1}\beta}}), \sigma^{-1}(\beta + \beta'^{\zeta\zeta^{-1}\widehat{\alpha+\sigma\sigma^{-1}\beta}}), \zeta^{-1}\sigma^{-1}\mu + \\ & \quad + \sigma^{-1}\zeta^{-1}\mu'^{\zeta\zeta^{-1}\widehat{\alpha+\sigma\sigma^{-1}\beta}} + \zeta^{-1}\sigma^{-1}\alpha(\bar{\beta}')^{\zeta\zeta^{-1}\widehat{\alpha+\sigma\sigma^{-1}\beta}} + \zeta^{-1}\sigma^{-1}\beta(\bar{\alpha}')^{\zeta\zeta^{-1}\widehat{\alpha+\sigma\sigma^{-1}\beta}}]_{\zeta,\sigma} \\ &= [\zeta^{-1}(\alpha + \alpha'^{\widehat{\alpha}}), \sigma^{-1}(\beta + \beta'^{\widehat{\alpha}}), \zeta^{-1}\sigma^{-1}(\mu + \mu'^{\widehat{\alpha}} + \alpha(\bar{\beta}')^{\widehat{\alpha}} + \beta(\bar{\alpha}')^{\widehat{\alpha}})]_{\zeta,\sigma} \end{aligned}$$

The isomorphisms $\Phi, \Phi^*, \Phi_\delta, \Phi_{\zeta,\sigma}$ show that all $q^2 - 1$ exotic elation groups are isomorphic. That is, there are exactly two elation groups of $H(3, q^2)$, up to isomorphism. ■

Although we have shown isomorphism, to satisfy curiosity, we mention some other isomorphisms between these exotic elation groups in the original represen-

tation of the exotic elation groups.

Theorem 2.6.5 *Let s, t be distinct non-zero elements of $GF(q)$. Then if $t = s\delta \in GF(q)$, the two elation groups $E_{t\zeta, \zeta}$ and $E_{s\zeta, s^{-1}t\zeta}$ are isomorphic under the map*

$$\Delta : [\alpha, \beta, c] \circ \phi^i \mapsto [\delta\alpha, \delta^{-1}\beta, c] \circ \phi^i$$

This gives us $q - 1$ orbits of size $q - 1$.

Proof: Suppose that $t = s\delta \in GF(q)^*$ and consider the map:

$$\Delta : [\alpha, \beta, c] \circ \phi^i \mapsto [\delta\alpha, \delta^{-1}\beta, c] \circ \phi^i$$

Then Δ is a group isomorphism of S_2 .

Recall that

$$\begin{aligned} & E_{t\zeta, \zeta} \\ &= \left\{ \left[(a_1, a_2), (b_1, b_2), c \right] \circ \phi^i : \Theta_{t\zeta, \zeta}(a_1 + a_2, b_1 + b_2, i) = 0 \right\} \\ &= \left\{ \left[(a_1, a_2), (b_1, b_2), c \right] \circ \phi^i : \Theta_{\delta(s\zeta), \delta^{-1}(\zeta)}(a_1 + a_2, b_1 + b_2, i) = 0 \right\} \\ &= \left\{ \left[(a_1, a_2), (b_1, b_2), c \right] \circ \phi^i : \Theta_{(s\zeta), (s^{-1}t\zeta)}(\delta[a_1 + a_2], \delta^{-1}[b_1 + b_2], i) = 0 \right\} \end{aligned}$$

We now apply Δ to an elation group $E_{t\zeta, \zeta}$.

$$\begin{aligned}
& \Delta [E_{t\zeta, \zeta}] \\
&= \left\{ \left[\delta(a_1, a_2), \delta^{-1}(b_1, b_2), c \right] \circ \phi^i : \Theta_{t\zeta, \zeta}(a_1 + a_2, b_1 + b_2, i) = 0 \right\} \\
&= \left\{ \left[\delta(a_1, a_2), \delta^{-1}(b_1, b_2), c \right] \circ \phi^i : \Theta_{s\zeta, s^{-1}t\zeta}(\delta[a_1 + a_2], \delta^{-1}[b_1 + b_2], i) = 0 \right\} \\
&= \left\{ \left[(x_1, x_2), (y_1, y_2), c \right] \circ \phi^i : \Theta_{s\zeta, (s^{-1}t)\zeta}(x_1 + x_2, y_1 + y_2, i) = 0 \right\} \\
&= E_{s\zeta, s^{-1}t\zeta}
\end{aligned}$$

Hence $E_{t\zeta, \zeta} \cong E_{s\zeta, (s^{-1}t)\zeta}$.

Next suppose that $E_{s\zeta, s^{-1}t\zeta} = E_{t\beta, \beta}$ for any $t \in GF(q)$ and $\beta, \zeta \in GF(q)$. Then $s = t\beta\zeta^{-1}$, and

$$\begin{aligned}
s^{-1}t\zeta &= (t\beta\zeta^{-1})^{-1}t\zeta \\
&= t^{-1}\beta^{-1}\zeta t\zeta \\
&= \beta^{-1}\zeta^2
\end{aligned}$$

But this equals β if and only if $\zeta = \beta$. That is, under the map Δ , $E_{t\zeta,\zeta}$ is not the image of $E_{t\beta,\beta}$ for any $t \in GF(q)^*$ when $\beta \neq \zeta$. This gives us $q - 1$ orbits for each $t \in GF(q)^*$, each orbit containing $q - 1$ groups for each $\delta \in GF(q)^*$. ■

Theorem 2.6.6 *Let ζ, σ be distinct non-zero elements of $GF(q)$. Then if $\zeta = \sigma\delta \in GF(q)$, $E_{\zeta,0} \cong E_{\sigma,0}$ and $E_{0,\zeta} \cong E_{0,\sigma}$ under the map*

$$\Delta : [\alpha, \beta, c] \circ \phi^i \mapsto [\delta\alpha, \delta^{-1}\beta, c] \circ \phi^i$$

This gives us 2 orbits of size $q - 1$.

Proof: Recall the following group isomorphism:

$$\Delta : [\alpha, \beta, c] \circ \phi^i \mapsto [\delta\alpha, \delta^{-1}\beta, c] \circ \phi^i$$

Then since $\zeta = \sigma\delta$ for some $\delta \in GF(q)$ we get

$$\begin{aligned} E_{0,\zeta} &= \left\{ [(a_1, a_2), (b_1, b_2), c] \circ \phi^i : \Theta_{0,\zeta}(a_1 + a_2, b_1 + b_2, i) = 0 \right\} \\ &= \left\{ [(a_1, a_2), (b_1, b_2), c] \circ \phi^i : \Theta_{0,\delta^{-1}\sigma}(a_1 + a_2, b_1 + b_2, i) = 0 \right\} \\ &= \left\{ [(a_1, a_2), (b_1, b_2), c] \circ \phi^i : \Theta_{0,\sigma}(\delta(a_1 + a_2), \delta^{-1}(b_1 + b_2), i) = 0 \right\} \end{aligned}$$

Using the same argument as in the previous theorem we get

$$\begin{aligned} \Delta [E_{0,\zeta}] &= \left\{ [\delta(a_1, a_2), \delta^{-1}(b_1, b_2), c] \circ \phi^i : \Theta_{0,\zeta}(\delta(a_1 + a_2), \delta^{-1}(b_1 + b_2), i) = 0 \right\} \\ &= \left\{ [(x_1, x_2), (y_1, y_2), c] \circ \phi^i : \Theta_{0,\sigma}(x_1 + x_2, y_1 + y_2, i) = 0 \right\} \\ &= E_{0,\sigma} \end{aligned}$$

Since for all $\zeta, \sigma \in GF(q)^*$ there is some δ such that $\zeta = \sigma\delta$, we must have $E_{0,\zeta} \cong E_{0,\sigma}$ for all non-zero $\zeta, \sigma \in GF(q)$. Similar computations show that $E_{\zeta,0} \cong E_{\sigma,0}$ for all non-zero $\zeta, \sigma \in GF(q)$. ■

We have partitioned the $q^2 - 1$ exotic elation groups into $q + 1$ orbits of size $q - 1$. We will list the orbits as $[E_{t_1\zeta,\zeta}], \dots, [E_{t_{q-1}\zeta,\zeta}], [E_{1,0}], [E_{0,1}]$, where t_i ranges over $GF(q)^*$. Next, consider the map

$$\overline{\Delta} : [\alpha, \beta, c] \circ \phi^i \mapsto [\delta\alpha, \delta\beta, \delta^2c] \circ \phi^i$$

Now consider the following elation group where $\zeta = \beta \cdot \delta$.

$$\begin{aligned} E_{t\zeta,\zeta} &= \left\{ \left[(a_1, a_2), (b_1, b_2), c \right] \circ \phi^i : \Theta_{t\zeta,\zeta}(a_1 + a_2, b_1 + b_2, i) = 0 \right\} \\ &= \left\{ \left[(a_1, a_2), (b_1, b_2), c \right] \circ \phi^i : \Theta_{t\delta\beta,\delta\beta}(a_1 + a_2, b_1 + b_2, i) = 0 \right\} \\ &= \left\{ \left[(a_1, a_2), (b_1, b_2), c \right] \circ \phi^i : \Theta_{t\beta,\beta}(\delta(a_1 + a_2), \delta(b_1 + b_2), i) = 0 \right\} \\ &\quad \Downarrow \\ \overline{\Delta} [E_{t^{1/2}\zeta,\zeta}] &= \left\{ \left[\delta(a_1, a_2), \delta(b_1, b_2), \delta c \right] \circ \phi^i : \Theta_{t\beta,\beta}(\delta(a_1 + a_2), \delta(b_1 + b_2), i) = 0 \right\} \\ &= E_{t\beta,\beta} \end{aligned}$$

and $E_{t\zeta,\zeta} \cong E_{t\beta,\beta}$ for all $\zeta, \beta \in GF(q)$. So $\overline{\Delta}$ provides an isomorphism between the $q - 1$ Δ -orbits $[E_{t_1\zeta,\zeta}], \dots, [E_{t_{q-1}\zeta,\zeta}]$.

We mention one other known group isomorphism. Consider the map Δ^σ where $\sigma = 2^s$. Then

$$\Delta^\sigma : [\alpha, \beta, c] \circ \phi^i \mapsto [\alpha^\sigma, \beta^\sigma, c^\sigma] \circ \phi^i$$

is also a group isomorphism for any automorphism σ . To see the image of such a map, let $q = 2^e$ and consider the following, where $\langle \alpha \rangle = GF(q)^*$ and $a, c \in GF(q)$.

$$\begin{aligned} tr(c \cdot \Delta^\sigma(a)) &= tr(c \cdot a^\sigma) \\ &= tr(\alpha^i \cdot (\alpha^j)^{2^s}) \\ &= \sum_{n=0}^{e-1} [\alpha^i \cdot (\alpha^j)^{2^s}]^{2^n} \\ &= \sum_{n=0}^{e-1} [\alpha^{i \cdot 2^{-s}} \cdot (\alpha^j)]^{2^{n+s}} \\ &= \sum_{n=0}^{e-1} [\alpha^{i \cdot 2^{-s}} \cdot (\alpha^j)]^{2^n} \\ &= tr(c^{2^{-s}} \cdot a) \end{aligned}$$

where the second to last equality follows since raising to the 2^s power is an isomorphism and does not change the value of the absolute trace function.

2.7 Building Subgroups $A(t)$ in the Exotic Elation Group E

Let $q = 2^e$ and denote $\alpha \in GF(q^2)$ by (a_1, a_2) where $a_i \in GF(q)$. Using the absolute trace function $tr : GF(q) \mapsto GF(2)$ we define the map $T : GF(q) \times GF(q) \mapsto GF(2)$ by

$$T(\alpha) = \text{tr}(a_1) + \text{tr}(a_2)$$

Similar to when we worked with the unitary representation of these groups, we put $a^{\widehat{\alpha}} = aP^{T(\alpha)}$. We now define the elation group $E_{1,0}$ as follows

$$E_{1,0} = \left\{ [\alpha, \beta, c] : \alpha, \beta \in GF(q) \times GF(q), c \in GF(q) \right\}.$$

with group product

$$[\alpha, \beta, c] * [\alpha', \beta', c'] = [\alpha + \alpha'^{\widehat{\alpha}}, \beta + \beta'^{\widehat{\alpha}}, c + c' + (\alpha')^{\widehat{\alpha}}P\beta'^T].$$

For the remainder of this paper we will assume that $E = E_{1,0}$. We also note that in some computations we will revert back to the old notation, using $aP^{T(\alpha)}$ instead of $a^{\widehat{\alpha}}$.

For each $t \in GF(q)$, let $\delta(t)$ be a function from $GF(q) \times GF(q)$ into $GF(q) \times GF(q)$, and let g_t be a map from $GF(q) \times GF(q)$ into $GF(q)$. For each $t \in GF(q)$ we also have a subset $A(t)$ of order q^2 such that

$$A(t) = \left\{ [\alpha, \alpha^{\delta(t)}, g_t(\alpha)] \right\}$$

What are the necessary and sufficient conditions on $\delta(t)$ and g_t so that $A(t)$ is a group?

2.8 The Function $\delta(t)$

Consider the product

$$\begin{aligned} g \cdot g' &= \left[\alpha, \alpha^{\delta(t)}, g_t(\alpha) \right] \cdot \left[\alpha', \alpha'^{\delta(t)}, g_t(\alpha') \right] \\ &= \left[\alpha + (\alpha')^{\widehat{\alpha}}, \alpha^{\delta(t)} + (\alpha'^{\delta(t)})^{\widehat{\alpha}}, g_t(\alpha) + g_t(\alpha') + (\alpha^{\delta(t)})^{\widehat{\alpha}} P \alpha'^T \right] \end{aligned}$$

Hence $\alpha^{\delta(t)} + (\alpha'^{\delta(t)})^{\widehat{\alpha}} = (\alpha + (\alpha')^{\widehat{\alpha}})^{\delta(t)}$.

We show that $\delta(t)$ is an additive function.

First let $\alpha = 0$. Then $0^{\delta(t)} + \alpha'^{\delta(t)} = \alpha'^{\delta(t)}$ and $0^{\delta(t)} = 0$. Now if $T(\alpha) = 0$, we get $\alpha^{\delta(t)} + \alpha'^{\delta(t)} = (\alpha + \alpha')^{\delta(t)}$, which holds regardless of the value of $T(\alpha')$.

We next show that $\alpha^{\delta(t)} P = (\alpha P)^{\delta(t)}$ for all $\alpha \in GF(q) \times GF(q)$. We first suppose that $T(\alpha) = 1$. Then $\alpha^{\delta(t)} + \alpha'^{\delta(t)} P = (\alpha + \alpha' P)^{\delta(t)}$, and if we put $\alpha' = \alpha P$, then

$$\alpha^{\delta(t)} + (\alpha P)^{\delta(t)} P = (\alpha + \alpha P P)^{\delta(t)} = 0 \implies \alpha^{\delta(t)} P = (\alpha P)^{\delta(t)}$$

Next, we show that $\beta^{\delta(t)} P = (\beta P)^{\delta(t)}$ when $T(\beta) = 0$. If we have some β such that $T(\beta) = 0$ we know that we can choose two elements $\alpha = (\alpha_1, 0)$ and $\alpha' = (\alpha'_1, 0)$ such that $T(\alpha) = T(\alpha') = 1$ and $\alpha + \alpha' P = \beta$. Letting $\beta = \alpha + \alpha' P$ it is clear that that $\delta(t)$ satisfies $(\alpha P + \alpha')^{\delta(t)} = [(\alpha + \alpha' P) P]^{\delta(t)}$.

From above we know $\delta(t)$ satisfies $\alpha^{\delta(t)} + \alpha' \delta(t) P = (\alpha + \alpha' P)^{\delta(t)}$. Using the fact that $T(\alpha') = T(\alpha' P) = 1$ we get

$$\begin{aligned}
\alpha^{\delta(t)} + \alpha' \delta(t) P &= (\alpha + \alpha' P)^{\delta(t)} \\
\alpha^{\delta(t)} + \alpha' P \delta(t) &= (\alpha + \alpha' P)^{\delta(t)} \\
(\alpha^{\delta(t)} + \alpha' P \delta(t)) P &= (\alpha + \alpha' P)^{\delta(t)} P \\
\alpha^{\delta(t)} P + \alpha' P \delta(t) P &= (\alpha + \alpha' P)^{\delta(t)} P \\
\alpha P^{\delta(t)} + \alpha' P P \delta(t) &= (\alpha + \alpha' P)^{\delta(t)} P \\
\alpha P^{\delta(t)} + \alpha' \delta(t) &= (\alpha + \alpha' P)^{\delta(t)} P \\
(\alpha P + \alpha')^{\delta(t)} &= (\alpha + \alpha' P)^{\delta(t)} P \\
\beta P^{\delta(t)} &= \beta^{\delta(t)} P
\end{aligned}$$

So when $T(\beta) = 0$ we get $\beta^{\delta(t)} P = \beta P^{\delta(t)}$. This completes the argument that $\alpha' \delta(t) P = \alpha' P \delta(t)$ for all $\alpha \in GF(q) \times GF(q)$. Now recall that when $T(\alpha) = 1$, $\delta(t)$ must satisfy $\alpha^{\delta(t)} + \alpha' \delta(t) P = (\alpha + \alpha' P)^{\delta(t)}$. Using the above computations we see that when $T(\alpha) = 1$ we get $\alpha^{\delta(t)} + \alpha' P \delta(t) = (\alpha + \alpha' P)^{\delta(t)}$. It follows that $\delta(t)$ is an additive function on all of $GF(q) \times GF(q)$. Fortunately, there is an easy classification of additive functions from $GF(q)$ into $GF(q)$.

Theorem 2.8.1 *If $f : GF(q) \mapsto GF(q)$ is an additive function, then*

$$f(x) = a_0 x + a_1 x^p + a_2 x^{p^2} + \cdots + a_{e-1} x^{p^{e-1}}$$

where $a_i \in GF(q)$.

Proof: See Theorem A.6 in Appendix A. ■

Suppose that $\delta(t)$ is the additive function that is used in the definition of the subgroup $A(t)$. Given the above theorem, for all $\alpha \in GF(q) \times GF(q)$ we must have

$$\begin{aligned}
[\alpha^{\delta(t)}]P &= \left(a_0\alpha + a_1\alpha^p + a_2\alpha^{p^2} + \cdots + a_{2e-1}\alpha^{p^{2e-1}} \right) P \\
&= (a_0\alpha)P + (a_1\alpha^p)P + (a_2\alpha^{p^2})P + \cdots + (a_{2e-1}\alpha^{p^{2e-1}})P \\
&= a_0(\alpha P) + a_1(\alpha P)^p + a_2(\alpha P)^{p^2} + \cdots + a_{2e-1}(\alpha P)^{p^{2e-1}} \\
&= (\alpha P)^{\delta(t)}
\end{aligned}$$

Unfortunately, we do not have a complete answer about which additive functions will suffice. However, we do have the following conjecture about $\delta(t)$.

Conjecture 2.8.2 *Let $\delta(t) : GF(q^2) \mapsto GF(q^2)$. Then let*

$$A(t) = \left\{ \left[\alpha, \alpha^{\delta(t)}, g_t(\alpha) \right] : \alpha \in GF(q) \times GF(q), c \in GF(q) \right\}$$

be a subset of $E_{1,0}$. A necessary condition that $A(t)$ be a subgroup is that $\delta(t)$ be additive function of the form

$$x^{\delta(t)} = ax$$

for some $a \in GF(q)$.

2.9 The Function g_t

We need to determine properties of g_t so that $A(t)$ is a subgroup. Multiplying two elements in $A(t)$ we easily get the following condition on g_t .

$$g_t(\alpha) + g_t(\alpha') + g_t(\alpha + (a')^{\widehat{\alpha}}) = (a')^{\widehat{\alpha}} P(\alpha^{\delta(t)})^T \quad (2.1)$$

$$g_t(\alpha) + g_t(\alpha') + g_t(a^{\widehat{\alpha}'} + \alpha') = a^{\widehat{\alpha}'} P(\alpha'^{\delta(t)})^T \quad (2.2)$$

We choose the additive function $\alpha^{\delta(t)} = t\alpha$, for $t \in GF(q)$. Then g_t must satisfy

$$g_t(a^{\widehat{\alpha}'} + \alpha') + g_t((a')^{\widehat{\alpha}} + \alpha) = t \left[a^{\widehat{\alpha}'} P \alpha'^T + a^{\widehat{\alpha}'} P (\alpha')^T \right] \quad (2.3)$$

Note that if we let $\alpha = \alpha'$ we get $g_t(0) = 0$.

Next suppose that $\alpha = (\alpha_1, \alpha_2)$ and $\alpha' = (\alpha'_1, \alpha'_2)$, and we consider the following cases.

(i) $T(\alpha) = T(\alpha') = 1$: Then from equation 2.3 we get

$$g(\alpha_1 + \alpha'_2, \alpha_2 + \alpha'_1) = g(\alpha_2 + \alpha'_1, \alpha_1 + \alpha'_2)$$

(ii) $T(\alpha) \neq T(\alpha')$: Then from equation 2.3 we get

$$g(\alpha_1 + \alpha'_1, \alpha_2 + \alpha'_2) + g(\alpha_2 + \alpha'_1, \alpha_1 + \alpha'_2) = t \left[\alpha_1 \alpha'_2 + \alpha_2 \alpha'_1 + \alpha_1 \alpha'_1 + \alpha_2 \alpha'_2 \right]$$

(iii) Let $T(\alpha) = 0$: Then from equation 2.1 we get

$$g_t(\alpha) + g_t(\alpha') + g_t(\alpha + \alpha') = \alpha \begin{pmatrix} 0 & t \\ t & 0 \end{pmatrix} (\alpha')^T$$

Before we determine acceptable functions g_t , we characterize all functions from $GF(q) \times GF(q)$ to $GF(q)$ as polynomials.

Theorem 2.9.1 *Let $g_t(\alpha)$ be a function from $GF(q) \times GF(q)$ into $GF(q)$. Then there is a distinct polynomial associated with $g_t(\alpha)$ of the form*

$$g_t(\alpha) = \sum_{0 \leq j, k \leq q-1} c_{j,k} \alpha_1^k \alpha_2^j, \text{ where } c_{j,k} \in GF(q)$$

Proof: See Theorem A.7 in Appendix A. ■

Thinking of $g_t(\alpha)$ as a polynomial, if we evaluate the function $g_t(\alpha)$ only on elements from $GF(q) \cong \{\alpha = (\alpha_1, 0) : \alpha_1 \in GF(q)\}$, because the function is additive on these elements, it must be of the form

$$g_t(\alpha) = a_1 \alpha_1^2 + a_2 \alpha_1^{2^2} + \cdots + a_{e-1} \alpha_1^{2^{e-1}} + \sum_{\substack{0 \leq i \leq q-1 \\ 1 \leq j \leq q-1}} c_{i,j} \alpha_1^i \alpha_2^j,$$

where $a_0 = 0$ since $g_t(0) = 0$. Then recalling that $g_t(\alpha) = g_t(\alpha P)$ we have the following restriction for g_t .

$$g_t(\alpha) = a_1 (\alpha_1 + \alpha_2)^2 + \cdots + \sum_{1 \leq j < k \leq 2^e - 1} c_{j,k} (\alpha_1^k \alpha_2^j + \alpha_1^j \alpha_2^k) + \sum_{1 \leq i \leq 2^e - 1} d_i (\alpha_1 \alpha_2)^i$$

Using the fact that $g_t(\alpha + \alpha') + g_t(\alpha) + g_t(\alpha') = t[\alpha_1 \alpha'_2 + \alpha_2 \alpha'_1]$ we compute the following:

$$\begin{aligned}
& g_t(\alpha + \alpha') + g_t(\alpha) + g_t(\alpha') \\
&= a_1(\alpha_1 + \alpha_2)^2 + \cdots + \sum_{1 \leq i \leq 2^e - 1} d_i(\alpha_1 \alpha_2)^i + \sum_{1 \leq j < k \leq 2^e - 1} c_{j,k}(\alpha_1^k \alpha_2^j + \alpha_1^j \alpha_2^k) + \\
& a_1(\alpha'_1 + \alpha'_2)^2 + \cdots + \sum_{1 \leq i \leq 2^e - 1} d_i(\alpha'_1 \alpha'_2)^i + \sum_{1 \leq j < k \leq 2^e - 1} c_{j,k}(\alpha_1'^k \alpha_2'^j + \alpha_1'^j \alpha_2'^k) + \\
& a_1(\alpha_1 + \alpha'_1 + \alpha_2 + \alpha'_2)^2 + \sum_{1 \leq i \leq 2^e - 1} d_i(\alpha_1 + \alpha'_1)(\alpha_2 + \alpha'_2)^i + \\
& \sum_{1 \leq j < k \leq 2^e - 1} c_{j,k} \left([\alpha_1 + \alpha'_1]^k [\alpha_2 + \alpha'_2]^j + [\alpha_1 + \alpha'_1]^j [\alpha_2 + \alpha'_2]^k \right) \\
&= \sum_{1 \leq j < k \leq 2^e - 1} c_{j,k} \left(\alpha_1^k \alpha_2^j + \alpha_1^j \alpha_2^k + \alpha_1'^k \alpha_2'^j + \alpha_1'^j \alpha_2'^k + [\alpha_1 + \alpha'_1]^k [\alpha_2 + \alpha'_2]^j + \right. \\
& \left. [\alpha_1 + \alpha'_1]^j [\alpha_2 + \alpha'_2]^k \right) + \sum_{1 \leq i \leq 2^e - 1} d_i \left[(\alpha_1 \alpha_2)^i + (\alpha'_1 \alpha'_2)^i + [\alpha_1 + \alpha'_1]^j [\alpha_2 + \alpha'_2]^j \right] \\
&= \alpha \begin{pmatrix} 0 & t \\ t & 0 \end{pmatrix} \alpha'^T \\
&= t[\alpha_1 \alpha'_2 + \alpha'_1 \alpha_2]
\end{aligned}$$

We now make the substitution $\alpha' = \alpha P$ and get

$$\sum_{1 \leq i \leq 2^e - 1} d_i(\alpha_1 + \alpha_2)^{2i} = t(\alpha_1 + \alpha_2)^2$$

for all $\alpha_1, \alpha_2 \in GF(q)$. That is,

$$\sum_{1 \leq i \leq 2^e - 1} d_i \beta^i = t\beta \implies (t + d_1)\beta + d_2\beta^2 + \cdots + d_{q-1}\beta^{q-1} = 0$$

for all $\beta \in GF(q)$. But this is a polynomial of degree $q - 1$, and if every element of $GF(q)$ is a root it must be the zero polynomial. It follows that $d_1 = t$ and $d_i = 0$ when $i \neq 1$. We have shown that necessarily,

$$g_t(\alpha) = a_1(\alpha_1 + \alpha_2)^2 + \cdots + a_{e-1}(\alpha_1 + \alpha_2)^{2^e - 1} + t\alpha_1\alpha_2 + \sum_{1 \leq j < k \leq 2^e - 1} c_{j,k}(\alpha_1^k \alpha_2^j + \alpha_1^j \alpha_2^k)$$

Lets make the assumption $\alpha'_1 = \alpha_1$ and $\alpha_2 \neq 0 = \alpha'_2$. Then

$$\begin{aligned} t\alpha_1\alpha_2 &= \alpha \begin{pmatrix} 0 & t \\ t & 0 \end{pmatrix} \alpha'^T \\ &= g_t(\alpha + \alpha') + g_t(\alpha) + g_t(\alpha') \\ &= t\alpha_1\alpha_2 + \sum_{1 \leq j < k \leq 2^e - 1} c_{j,k}(\alpha_1^k \alpha_2^j + \alpha_1^j \alpha_2^k). \end{aligned}$$

So we have

$$\sum_{1 \leq j < k \leq 2^e - 1} c_{j,k}(\alpha_1^k \alpha_2^j + \alpha_1^j \alpha_2^k) = 0.$$

Since for a fixed α_2 , this is a polynomial of degree less than or equal to $2^e - 1$ that is zero at all $\alpha_1 \in GF(q)$, we must have $c_{j,k} = 0$ for all $1 \leq j, k \leq 2^e - 1$.

We have shown the following.

Theorem 2.9.2 *Let $g_t(\alpha) : GF(q) \times GF(q) \mapsto GF(q)$. Then let $A(t) = \left\{ \left[\alpha, t\alpha, g_t(\alpha) \right] \right\}$ be a subset of the elation group E . A necessary condition that $A(t)$ be a subgroup is that $g_t(\alpha)$ be a function of the form*

$$g_t(\alpha) = \alpha \begin{pmatrix} f(t) & t \\ 0 & f(t) \end{pmatrix} \alpha^T + \sum_{i=1}^{e-1} \left[a_i (\alpha_1 + \alpha_2)^{2^i} \right].$$

We are now ready to talk about 4-gonal families when $g_t(\alpha)$ fits the forms defined above. Define the subgroup $A(\infty)$ as

$$A(\infty) = \left\{ \left[0, \alpha, 0 \right] \right\}$$

and form a set of $1 + q$ subgroups of order q^2 as

$$\mathbb{F} = \{A(t) : t \in GF(q) \cup \infty\}$$

and then let $A(t)^*$ equal $A(t) \cdot Z(E)$ which gives

$$A(t)^* = \left\{ \left[\alpha, t\alpha, c \right] : \alpha \in GF(q) \times GF(q), c \in GF(q) \right\}$$

It is clear that if we form $A^*(t)$ in this manner, then only subgroups $A(t)$ that trivially intersect the center will allow \mathbb{F} and \mathbb{F}^* to satisfy $K2$.

We want to know which of the families built from \mathbb{F} and \mathbb{F}^* satisfy $K1$, as we already know they satisfy $K2$. Essentially, we are looking at relationships between values on the diagonal entries of a $g(t)$ and $g(s)$ that allow the sets to form an EGQ. Once this is decided we will decide which GQ are isomorphic to the classical $H(3, q^2)$.

Recall that $K1$ says that $A(t)A(s) \cap A(k) = \{id\}$ when s, t , and k are distinct. The following result will be helpful.

Theorem 2.9.3 (Payne) *Let $A(t)$, $A(s)$, and $A(k)$ be subgroups of order q^2 . Then $A(t)A(s) \cap A(k) = \{id\}$ if and only if $A(t^\pi)A(s^\pi) \cap A(k^\pi) = \{id\}$ for every permutation π of s, t, k .*

We will check $A(t)A(s) \cap A(k) = \{id\}$ when $k = \infty$ and $s, t, k \neq \infty$. Choose $g = \pi[\alpha, t\alpha, g_t(\alpha)] \in A(t)$ and also choose $g' = \pi[\alpha', s\alpha', g_s(\alpha')] \in A(s)$, with $t \neq s$ and $g_t(\alpha)$ defined as

$$g_t(\alpha) = \alpha \begin{pmatrix} f(t) & t \\ 0 & f(t) \end{pmatrix} \alpha^T + \sum_{i=1}^{e-1} [a_i(\alpha_1 + \alpha_2)^{2^i}]$$

Then for the product $g \cdot g'$ we get

$$\begin{aligned} g \cdot g' &= [\alpha, t\alpha, \alpha \begin{pmatrix} f(t) & t \\ 0 & f(t) \end{pmatrix} \alpha^T] \cdot [\alpha', s\alpha', \alpha' \begin{pmatrix} f(s) & s \\ 0 & f(s) \end{pmatrix} \alpha'^T] \\ &= [\alpha + \alpha' \hat{\alpha}, t\alpha + s\alpha' \hat{\alpha}, \star] \end{aligned}$$

where

$$\begin{aligned} \star &= f(t)[\alpha_1^2 + \alpha_2^2] + f(s)[(\alpha'_1)^2 + (\alpha'_2)^2] + t\alpha_1\alpha_2 + s\alpha'_1\alpha'_2 + \\ &\quad \cdots + \sum_{i=1}^{e-1} [a_i(\alpha_1 + \alpha_2 + \alpha'_1 + \alpha'_2)^{2^i}] \end{aligned}$$

For any $\alpha \in GF(q^2)$, $g \cdot g'$ is in $A(k)$, where $k = \infty$, if and only if the following conditions hold.

(i) $\alpha = \alpha'$ which means that $\alpha P \alpha'^T = 0$.

(ii) $\left[f(t) + f(s) \right] (\alpha_1^2 + \alpha_2^2) + \left[t + s \right] \alpha_1 \alpha_2 = 0$ for any $id \neq \alpha \in GF(q^2)$.

If we were to have $f(t) = f(s)$ for distinct s and t , then choose α with $\alpha_1 = 0$ and $\alpha_2 \neq 0$ to violate $K1$. It follows that $f(t)$ must be a bijection on $GF(q)$. Furthermore, property (ii) is equivalent to

$$tr \left[\frac{f(t) + f(s)}{t + s} \right] = 1.$$

Next suppose that $k \in GF(q)$. Then we violate $K1$ provided we satisfy the following two conditions.

(i) $\{\alpha, \alpha'\}$ is a $GF(q)$ -dependent set with

$$\alpha' = \left(\frac{k+t}{k+s} \right) \alpha \implies \alpha'_1 = \left(\frac{k+t}{k+s} \right) \alpha_1 \text{ and } \alpha'_2 = \left(\frac{k+t}{k+s} \right) \alpha_2$$

(ii)

$$\begin{aligned} & \left[f(k) + f(k) \left(\frac{k+t}{k+s} \right)^2 + f(t) + f(s) \left(\frac{k+t}{k+s} \right)^2 \right] (\alpha_1^2 + \alpha_2^2) + \\ & \left[k + k \left(\frac{k+t}{k+s} \right)^2 + t + s \left(\frac{k+t}{k+s} \right)^2 \right] \alpha_1 \alpha_2 = 0 \end{aligned}$$

for all non-identity $\alpha = (\alpha_1, \alpha_2)$. This condition, when simplified, says that we satisfy $K1$ if and only if for all distinct $s, t, k \in GF(q)$ we satisfy

$$tr \left(\frac{f(k)[s^2 + t^2] + f(t)[k^2 + s^2] + f(s)[k^2 + t^2]}{k[s^2 + t^2] + t[k^2 + s^2] + s[k^2 + t^2]} \right) = 1$$

Since all cases for $K1$ will be some permutation of the last two cases we know that we have found necessary conditions for $F = \{A(t) : t \in GF(q) \cup \infty\}$ to satisfy $K1$.

From here we would like to see if WLOG we can assume that $f(0) = 0$.

If $\alpha = (\alpha_1, \alpha_2)$, consider the map

$$\Delta : [\alpha, \beta, c] \mapsto [\alpha, \beta, c + \delta(\alpha_1^2 + \alpha_2^2)]$$

where $\delta \in GF(q)$. Clearly, $\Delta : id \mapsto id$. Next see that

$$\begin{aligned} \Delta(g \cdot g') &= \Delta \left([\alpha, \beta, c] \cdot [\alpha', \beta', c'] \right) \\ &= \Delta \left([\alpha + (a')^{\hat{\alpha}}, \beta + (\beta')^{\hat{\alpha}}, c + c' + (a')^{\hat{\alpha}} P \beta^T] \right) \\ &= \left[\alpha + (a')^{\hat{\alpha}}, \beta + (\beta')^{\hat{\alpha}}, c + c' + (a')^{\hat{\alpha}} P \beta^T + \right. \\ &\quad \left. \delta \left([\alpha_1 + (\alpha'_1)^{\hat{\alpha}}]^2 + [\alpha_2 + (\alpha'_2)^{\hat{\alpha}}]^2 \right) \right] \\ &= \pi \left[\alpha, \beta, c + \delta (\alpha_1^2 + \alpha_2^2) \right] \circ \phi^{T(\alpha)} \cdot \pi \left[\alpha', \beta', c' + \delta (\alpha_1'^2 + \alpha_2'^2) \right] \circ \phi^{T(\alpha')} \\ &= \Delta(g) \cdot \Delta(g') \end{aligned}$$

and Δ is an automorphism of E . It is easy to see that when $f(t)$ is a bijection on $GF(q)$, then

$$\Delta : A_f(t) \mapsto A_h(t)$$

where

$$A_f(t) = \left\{ \left[\alpha, t\alpha, \alpha \begin{pmatrix} f(t) & t \\ 0 & f(t) \end{pmatrix} \alpha^T + \sum_{i=1}^{e-1} [a_i(\alpha_1 + \alpha_2)^{2^i}] \right] \right\}$$

and

$$A_h(t) = \left\{ \left[\alpha, t\alpha, \alpha \begin{pmatrix} h(t) & t \\ 0 & h(t) \end{pmatrix} \alpha^T + \sum_{i=1}^{e-1} [a_i(\alpha_1 + \alpha_2)^{2^i}] \right] \right\}$$

where $h(t) = f(t) + f(0)$.

Furthermore, Δ fixes every point $A^*(t)$. Since Δ is an automorphism of E and its coset geometries we can WLOG assume that

$$A(t) = \left\{ \left[\alpha, t\alpha, \alpha \begin{pmatrix} f(t) & t \\ 0 & f(t) \end{pmatrix} \alpha^T + \sum_{i=1}^{e-1} [a_i(\alpha_1 + \alpha_2)^{2^i}] \right] \right\}$$

where $f(t)$ is a bijection such that $f(0) = 0$. In this setting we satisfy $K1$ if and only if the following conditions hold.

(i)

$$\text{tr} \left[\frac{f(t) + f(s)}{t + s} \right] = 1, \quad t \neq s$$

(ii)

$$\text{tr} \left[\frac{f(t)}{t} \right] = 1, \quad t \neq 0$$

(iii)

$$\text{tr} \left(\frac{f(t)s^2 + f(s)t^2}{ts^2 + st^2} \right) = 1$$

These conditions are certainly true if we choose the function $f(t) = \beta t$, where $\text{tr}(\beta) = 1$. We aim to show the following theorem.

Theorem 2.9.4 *Consider the set*

$$F = \left\{ A(t) = \left\{ \left[\alpha, t\alpha, g_t(\alpha) \right] \right\} : t \in GF(q) \right\} \cup \left\{ A(\infty) = \left\{ [0, \alpha, 0] \right\} \right\}$$

$$\text{where } g_t(\alpha) = \alpha \begin{pmatrix} f(t) & t \\ 0 & f(t) \end{pmatrix} \alpha^T + \sum_{i=1}^{e-1} \left[a_i (\alpha_1 + \alpha_2)^{2^i} \right].$$

Then if we let $F^* = \left\{ A^*(t) = A(t) \cdot Z(E) \right\} \cup \left\{ A^*(\infty) = A(\infty) \cdot Z(E) \right\}$, a necessary condition that \mathbb{F} be a 4-gonal family is that $f(t) = \beta t$ for some fixed $\beta \in GF(q)$ such that $\text{tr}(\beta) = 1$.

Proof: Using condition (i) above, the result follows from Theorem 2.9.5 due to Pentilla and O'Keefe, letting $\gamma = 1$. ■

Theorem 2.9.5 *Let $f : GF(q) \mapsto GF(q)$ be a function satisfying $f(0) = 0$ and let $\gamma \in \text{Aut } GF(q)$. The equation*

$$\text{tr} \left[\frac{f(x) + f(y)}{(x + y)^\gamma} \right] = 1$$

for all $x, y \in GF(q)$ with $x \neq y$ if and only if $f(x) = \beta x^\gamma$ for some $\beta \in GF(q)$ with $\text{tr}(\beta) = 1$.

Proof: We rely on the proof in [16].

Let m be an integer satisfying $1 \leq m \leq q - 1$, $(m, q - 1) = 1$ and

$$\text{tr} \left[\frac{f(x) + f(y)}{(x + y)^m} \right] = 1$$

for all $x, y \in GF(q)$ with $x \neq y$. It follows immediately that F is a permutation of $GF(q)$, for otherwise there exist $x, y \in GF(q)$ with $f(x) = f(y)$ and

$$\text{tr} \left[\frac{f(x) + f(y)}{(x + y)^m} \right] = \text{tr}(0) = 0$$

Let \mathcal{R} be the minimal set of residues modulo $q - 1$ such that for any $z \in \{0, \dots, q - 2\}$ there exists a unique $y \in \mathcal{R}$ and $i \in \{0, \dots, h - 1\}$ such that $z \equiv 2^i y \pmod{q - 1}$. We remark that $0 \in \mathcal{R}$. For $p \in \mathcal{R}$, let $l_p = |\{p2^i : i = 0, \dots, h - 1\}|$ (that is, l_p is the length of the orbit of p under $\text{Aut } GF(q)$). Let $f(x) = \sum_{i=0}^{q-2} a_i x^i$ and let

$$\alpha_{pk} = \left(\overline{a_{p2^k+m}} \right)^{2^{-k}},$$

where $\overline{p2^k + m}$ is the unique integer such that $0 \leq \overline{p2^k + m} < q - 1$ and $\overline{p2^k + m} \equiv p2^k + m \pmod{q - 1}$. It was shown in Glynn [11] that

$$\sum_{n=1}^{h/l_p} \left(\sum_{k=0}^{l_p-1} \alpha_{pk} \left[(z + 1)^{p+m2^{-k}} + z^{p+m2^{-k}} \right] \right)^{2^{nl_p}} = 0$$

for all $z \in GF(q)$ and for all $p \in \mathcal{R} \setminus \{0\}$. Further, $\text{tr}(a_m) = 1$.

Suppose that $m = \gamma \in \text{Aut } GF(q)$. Since m is a power of 2, the arguments in Glynn's Lemma 4.10 [11] show that the only non-zero α_{pk} is $\alpha_{00} = a_m$ (the

coefficient of x^m in f), hence $f(x) = ax^\gamma$ for some $a \in GF(q)$ with $tr(a) = 1$.

The converse is immediate, since

$$tr \left[\frac{ax^\gamma + ay^\gamma}{(x+y)^\gamma} \right] = tr(a) = 1$$

■

2.10 Property(G)

In the remaining sections we show that when we consider the function $\alpha^{\delta(t)} = t\alpha$, the only *EGQ* which arise are classical. We start with the following definition for Property (G).

Definition 2.10.1 *A GQ \mathcal{S} with parameters (q^2, q) has Property (G) at the point p provided the following holds. Let L_1 and M_1 be distinct lines incident with the point p . Let M_1, M_2, M_3, M_4 be distinct lines and L_1, L_2, L_3, L_4 be distinct lines for which $L_i \sim M_j$ whenever $i + j \leq 7$. Then $L_4 \sim M_4$.*

Figure 2.1 may be helpful.

To help see the motivation behind this definition we restate the following theorem.

Theorem 2.10.2 (R.C. Bose) [3] *Let \mathcal{S} be a GQ with parameters (s, t) . Then the following statements are equivalent:*

- (i) $t = s^2$
- (ii) *For some pair (x, y) of non-collinear points, each triad (x, y, z) has a constant number of centers, in which case this constant is $1 + s$.*

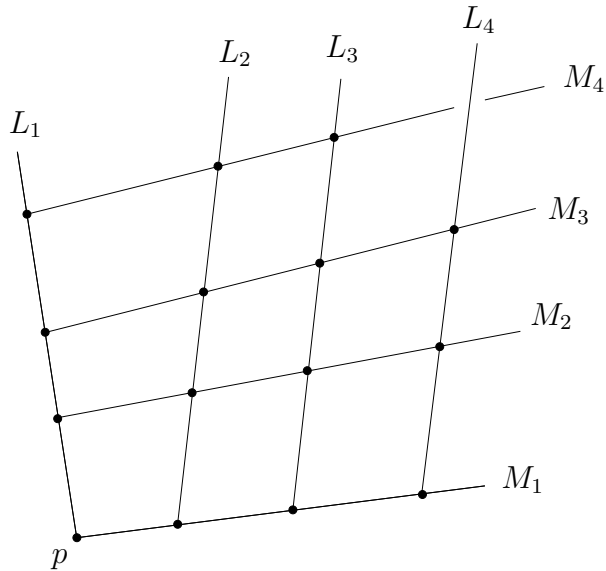


Figure 2.1: Property(G)

(iii) *Every triad of points has a constant number of centers, in which case this constant is $1 + s$.*

This theorem tells us that every triad of points in a GQ with parameters (q, q^2) has exactly $1 + q$ centers. Dually, it follows that every triad of lines in a GQ with parameters (q^2, q) has exactly $q + 1$ transversals. This result is known as the theorem of Bose. Now let L_1, L_2, L_3 be distinct skew lines and M_1, M_2, M_3, M_4 be transversals of L_1, L_2, L_3 such that M_1 and L_1 are both incident with the point p . We would like to know if each of the transversals of M_1, M_2, M_3 also intersect the line M_4 . If so, we are guaranteed to have a $(q + 1) \times (q + 1)$ grid about the point p .

Results by both J. Thas and Matt Brown have shown that any GQ with

parameters (q^2, q) and having property (G) at a point must be a flock- GQ . We wish to show that all EGQ arising from these 4-gonal families in exotic elation groups of $H(3, q^2)$ are flock- GQ .

We start with the following facts about incidence in these exotic GQ , where the notation $\overset{t}{\sim}$, $t \in \tilde{\mathbb{F}}$, suggests that two points are collinear via a line of type $A(t) \cdot g$. Also, for the remainder of this section, disregard the notation $\hat{\alpha} = P^{T(\alpha)}$ and simply consider $\hat{\alpha}$ as an element of $GF(q^2)$.

(i)

$$\begin{aligned}
[\alpha, \beta, c] &\overset{\infty}{\sim} A^*(\infty) \cdot [\alpha, \beta, c] \\
&= \left\{ [0, \beta', c'] : \beta' \in \mathbb{F}_q^2, c' \in \mathbb{F}_q \right\} \cdot [\alpha, \beta, c] \\
&= \left\{ [\alpha, \beta' + \beta, c' + c + \alpha P^{1+T(\alpha)} \beta'^T] : \beta' \in \mathbb{F}_q^2, c' \in \mathbb{F}_q \right\} \\
&= \left\{ [\alpha, \beta, c] : \beta \in \mathbb{F}_q^2, c \in \mathbb{F}_q \right\} \\
&= \left\{ [0, \beta, c] : \beta \in \mathbb{F}_q^2, c \in \mathbb{F}_q \right\} \cdot [\alpha, 0, 0] \\
&= A^*(\infty) \cdot [\alpha, 0, 0]
\end{aligned}$$

(ii)

$$\begin{aligned}
[\alpha, \beta, c] &\overset{\infty}{\sim} A(\infty) \cdot [\alpha, \beta, c] \\
&= \left\{ [0, \beta', 0] : \beta' \in \mathbb{F}_q^2 \right\} \cdot [\alpha, \beta, c] \\
&= \left\{ [\alpha, \beta' + \beta, c + \alpha P \beta'^T] : \beta' \in \mathbb{F}_q^2 \right\}
\end{aligned}$$

(iii)

$$\begin{aligned}
[\alpha, \beta, c] &\stackrel{t}{\sim} A^*(t) \cdot [\alpha, \beta, c] \\
&= \left\{ [\alpha', t\alpha', c'] : \alpha' \in \mathbb{F}_q^2, c' \in \mathbb{F}_q \right\} \cdot [\alpha, \beta, c] \\
&= \left\{ \left[\alpha' + \alpha P^{T(\alpha')}, t\alpha' + \beta P^{T(\alpha')}, c' + c + \alpha P^{1+T(\alpha)} \beta'^{tT} \right] \right\} \\
&= \left\{ \left[\alpha' + \alpha P^{T(\alpha')}, t \left(\alpha' + \alpha P^{T(\alpha')} \right) + t\alpha P^{T(\alpha')} + \beta P^{T(\alpha')}, c^* \right] \right\} \\
&= \left\{ \left[\alpha' + \alpha P^{T(\alpha')}, t \left(\alpha' + \alpha P^{T(\alpha')} \right) + (t\alpha + \beta) P^{T(\alpha')}, c^* \right] \right\} \\
&= A^*(t) \cdot [0, (t\alpha + \beta) P^{T(\alpha)}, 0]
\end{aligned}$$

(iv)

$$\begin{aligned}
[\alpha, \beta, c] &\stackrel{t}{\sim} A(t) \cdot [\alpha, \beta, c] \\
&= \left\{ [\alpha', t\alpha', g_t(\alpha')] \right\} \cdot [\alpha, \beta, c] \\
&= \left\{ \left[\alpha' + \alpha P^{T(\alpha')}, t\alpha' + \beta P^{T(\alpha')}, c + g_t(\alpha') + t \cdot \alpha' P^{1+T(\alpha')} \alpha'^T \right] \right\} \\
&= \left\{ \left[\alpha' + \alpha P^{T(\alpha')}, t \left(\alpha' + \alpha P^{T(\alpha')} \right) + (t\alpha + \beta) P^{T(\alpha')}, c + \right. \right. \\
&\quad \left. \left. g_t(\alpha P^{T(\alpha')}) + g_t(\alpha' + \alpha P^{T(\alpha')}) \right] \right\} \\
&= A(t) \cdot [0, (t\alpha + \beta) P^{T(\alpha)}, c + g_t(\alpha)]
\end{aligned}$$

To see this, we use $g_t(\alpha + \alpha') + g_t(\alpha) + g_t(\alpha') = \alpha' P \alpha^T$ and $g_t(\alpha) = g_t(\alpha P)$.

In Figure 2.2 we have constructed a 3×3 grid at the point (∞) , with lines $[A(\infty)]$ and $[A(t)]$, and containing the fixed point $[\alpha, \beta, c]$.

The coordinates of each point and line are given in the following list:

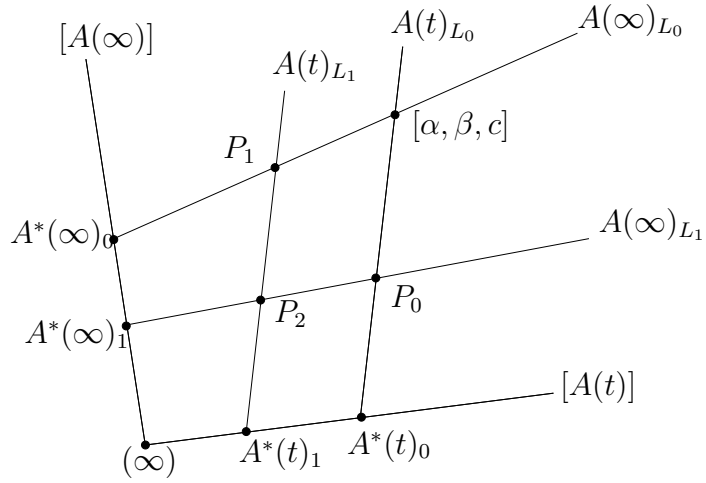


Figure 2.2: 3×3 Grid.

$$A(\infty)_{L_0} = A(\infty) \cdot [\alpha, \beta, c]$$

$$A(\infty)_{L_1} = A(\infty) \cdot [\alpha^*, 0, g_t(\alpha^*) + g_t(\alpha) + c]$$

$$A(t)_{L_0} = A(t) \cdot [0, (t\alpha + \beta)P^{T(\alpha)}, g_t(\alpha) + c]$$

$$A(t)_{L_1} = A(t) \cdot [0, (t\alpha + \beta + \beta')P^{T(\alpha)}, c + g_t(\alpha) + \alpha P\beta^{T^T}]$$

$$P_0 \stackrel{t}{=} [\alpha^*, t\alpha^* + (t\alpha + \beta)P^{T(\alpha+\alpha^*)}, c + g_t(\alpha) + g_t(\alpha^*)]$$

$$P_1 \stackrel{\infty}{=} [\alpha, \beta' + \beta, c + \alpha P\beta^{T^T}]$$

$$P_2 \stackrel{t}{=} \begin{cases} [\check{\alpha}, t\check{\alpha} + (t\alpha + \beta + \beta')P^{T(\alpha+\check{\alpha})}, g_t(\check{\alpha}) + g_t(\alpha) + c + t\alpha P\check{\alpha}] \\ [\alpha^*, \hat{\beta} + \beta^* + (t\alpha + \beta)P^{T(\alpha+\alpha^*)}, g_t(\alpha^*) + g_t(\alpha) + c + \alpha^* P\hat{\beta}^{T^T}] \end{cases}$$

We must have $\alpha^* = \check{\alpha}$, so we rewrite the coordinate for P_2 .

$$P_2 =_{\infty}^t \left\{ \begin{array}{l} \left[\alpha^*, t\alpha^* + (t\alpha + \beta + \beta')P^{T(\alpha+\alpha^*)}, g_t(\alpha^*) + g_t(\alpha) + c + t\alpha P\alpha^{*T} \right] \\ \left[\alpha^*, \hat{\beta} + t\alpha^* + (t\alpha + \beta)P^{T(\alpha+\alpha^*)}, g_t(\alpha^*) + g_t(\alpha) + c + \alpha^* P\hat{\beta}^T \right] \end{array} \right.$$

The point P_2 exists if and only if the following conditions hold:

$$\begin{aligned} t\alpha^* + \beta'P^{T(\alpha+\alpha^*)} &= \hat{\beta} + t\alpha^* \\ t\alpha P\alpha^{*T} &= \alpha^* P\hat{\beta}^T \end{aligned}$$

The theorem of Bose guarantees that a solution will exist. We now consider the case where $L_1 = [A(t)]$ and $M_1 = [A(s)]$, $t \neq s$.

In Figure 2.3 we have constructed a 3×3 grid at the point (∞) , having lines $[A(t)]$ and $[A(s)]$, and the fixed point $[\alpha, \beta, c]$.

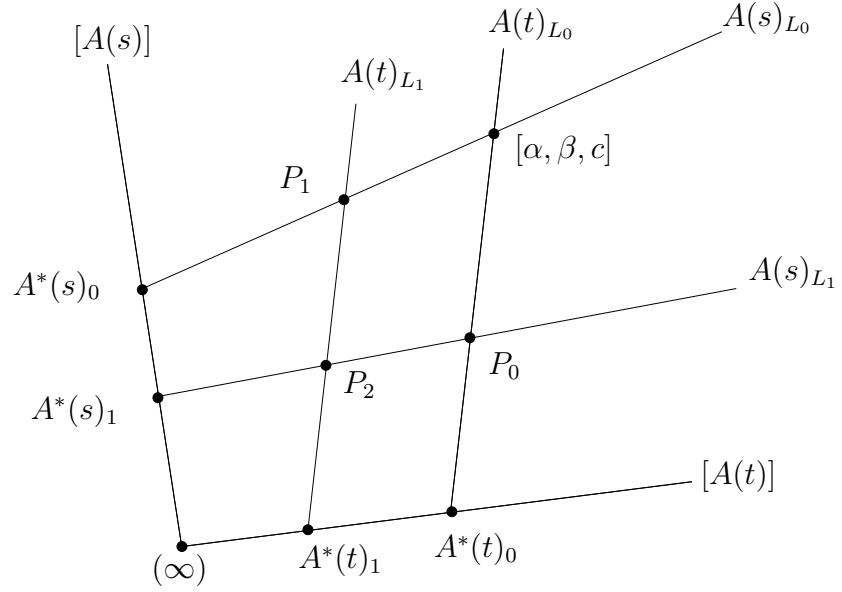


Figure 2.3: 3×3 Grid.

$$A(s)_{L_0} = A(s) \cdot [0, (s\alpha + \beta)P^{T(\alpha)}, g_s(\alpha) + c]$$

$$A(t)_{L_0} = A(t) \cdot [0, (t\alpha + \beta)P^{T(\alpha)}, g_t(\alpha) + c]$$

$$A(t)_{L_1} = A(t) \cdot \left[0, \left([t + s]\alpha_s + (s\alpha + \beta)P^{T(\alpha + \alpha_s)} \right) P^{T(\alpha_s)}, \right. \\ \left. g_t(\alpha_s) + g_s(\alpha_s) + g_s(\alpha) + c \right]$$

$$P_1 \stackrel{t}{=} [\alpha_s, s\alpha_s + (s\alpha + \beta)P^{T(\alpha + \alpha_s)}, g_s(\alpha_s) + g_s(\alpha) + c]$$

$$P_0 \stackrel{s}{=} [\alpha_t, t\alpha_t + (t\alpha + \beta)P^{T(\alpha + \alpha_t)}, g_t(\alpha_t) + g_t(\alpha) + c]$$

$$P_2 \stackrel{t}{=} \begin{cases} \left[\alpha^*, t\alpha^* + \left(\left([t + s]\alpha_s + (s\alpha + \beta)P^{T(\alpha + \alpha_s)} \right) P^{T(\alpha_s)} \right) P^{T(\alpha^*)}, \right. \\ \quad \left. g_t(\alpha^*) + g_t(\alpha_s) + g_s(\alpha_s) + g_s(\alpha) + c \right] \\ \left[\alpha', s\alpha' + \left(\left([t + s]\alpha_t + (t\alpha + \beta)P^{T(\alpha + \alpha_t)} \right) P^{T(\alpha_t)} \right) P^{T(\alpha')}, \right. \\ \quad \left. g_s(\alpha') + g_s(\alpha_t) + g_t(\alpha_t) + g_t(\alpha) + c \right] \end{cases}$$

We must have $\alpha^* = \alpha'$, and so we rewrite the coordinates for P_2 .

$$P_2 = \begin{cases} \left[\alpha^*, t\alpha^* + \left(([t+s]\alpha_s + (s\alpha + \beta)P^{T(\alpha+\alpha_s)})P^{T(\alpha_s)} \right) P^{T(\alpha^*)}, \right. \\ \qquad \qquad \qquad \left. g_t(\alpha^*) + g_t(\alpha_s) + g_s(\alpha_s) + g_s(\alpha) + c \right] \\ \\ \left[\alpha^*, s\alpha^* + \left(([t+s]\alpha_t + (t\alpha + \beta)P^{T(\alpha+\alpha_t)})P^{T(\alpha_t)} \right) P^{T(\alpha^*)}, \right. \\ \qquad \qquad \qquad \left. g_s(\alpha^*) + g_s(\alpha_t) + g_t(\alpha_t) + g_t(\alpha) + c \right] \end{cases}$$

For notational “simplicity”, given fixed pairs of elements $\alpha, \beta \in \mathbb{F}_q^2$ and $s, t \in \mathbb{F}_q$, define the following functions:

$$\begin{aligned} f^s(\gamma) &= \left([t+s]\gamma + (s\alpha + \beta)P^{T(\alpha+\gamma)} \right) P^{T(\gamma)} \\ f^t(\gamma) &= \left([t+s]\gamma + (t\alpha + \beta)P^{T(\alpha+\gamma)} \right) P^{T(\gamma)} \\ h^s(\gamma) &= g_t(\gamma) + g_s(\gamma) + g_s(\alpha) \\ h^t(\gamma) &= g_t(\gamma) + g_s(\gamma) + g_t(\alpha) \end{aligned}$$

So we have a 3×3 grid if and only if the following conditions hold:

$$\begin{aligned} t\alpha^* + f_s(\alpha_s)P^{T(\alpha^*)} &= s\alpha^* + f_t(\alpha_t)P^{T(\alpha^*)} \\ g_t(\alpha^*) + h_s(\alpha_s) &= g_s(\alpha^*) + h_t(\alpha_t) \end{aligned}$$

The theorem of Bose guarantees that such a 3-tuple $\alpha^*, \alpha_t, \alpha_s$ must exist.

In Figure 2.4 we have constructed a near 4×4 grid containing the 3×3 grid with point $[\alpha, \beta, c]$.

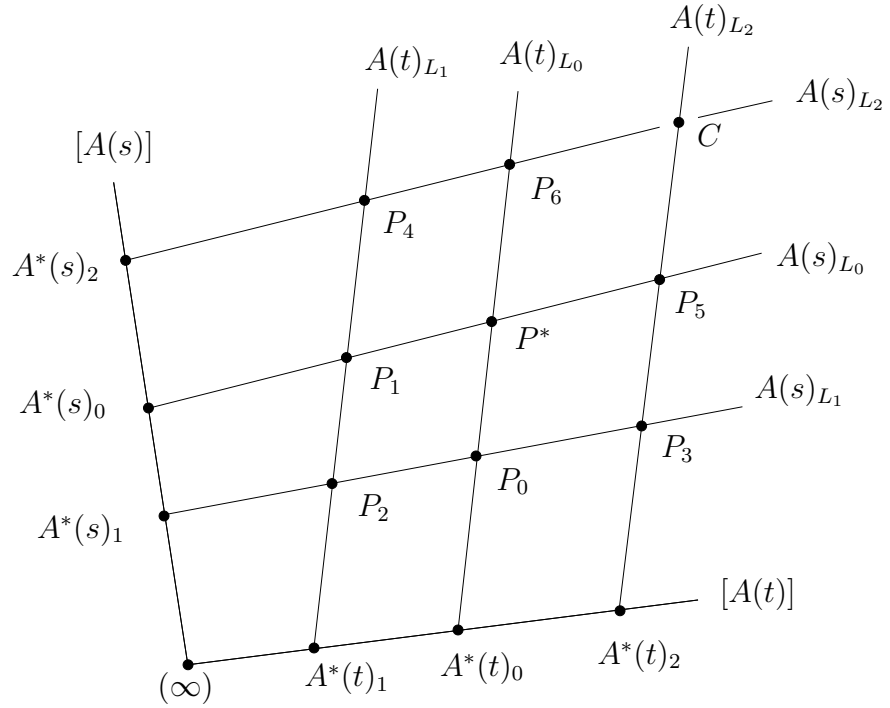


Figure 2.4: Near 4×4 Grid.

The computations used to determine the previous 3×3 grid give us the following information for the points and lines of the near 4×4 grid:

$$P^* = [\alpha, \beta, c]$$

$$A(t)_{L_0} = A(t) \cdot [0, (t\alpha + \beta)P^{T(\alpha)}, g_t(\alpha) + c]$$

$$A(t)_{L_1} = A(t) \cdot [0, f^s(\alpha_s), h^s(\alpha_s) + c]$$

$$A(t)_{L_2} = A(t) \cdot [0, f^s(\bar{\alpha}_s), h^s(\bar{\alpha}_s) + c]$$

$$A(s)_{L_0} = A(t) \cdot [0, (s\alpha + \beta)P^{T(\alpha)}, g_s(\alpha) + c]$$

$$A(s)_{L_1} = A(t) \cdot [0, f^t(\alpha_t), h^t(\alpha_t) + c]$$

$$A(s)_{L_2} = A(t) \cdot [0, f^t(\bar{\alpha}_t), h^t(\bar{\alpha}_t) + c]$$

$$P_0 \stackrel{t}{=} [\alpha_t, t\alpha_t + (t\alpha + \beta)P^{T(\alpha+\alpha_t)}, g_t(\alpha_t) + g_t(\alpha) + c]$$

$$P_1 \stackrel{s}{=} [\alpha_s, s\alpha_s + (s\alpha + \beta)P^{T(\alpha+\alpha_s)}, g_s(\alpha_s) + g_s(\alpha) + c]$$

$$P_2 \stackrel{t}{=} \left\{ \begin{array}{l} [\alpha^*, t\alpha^* + f^s(\alpha_s)P^{T(\alpha^*)}, g_t(\alpha^*) + h^s(\alpha_s) + c] \\ [\alpha^*, s\alpha^* + f^t(\alpha_t)P^{T(\alpha^*)}, g_s(\alpha^*) + h^t(\alpha_t) + c] \end{array} \right.$$

$$P_3 \stackrel{t}{=} \left\{ \begin{array}{l} [\hat{\alpha}, t\hat{\alpha} + f^s(\bar{\alpha}_s)P^{T(\hat{\alpha})}, g_t(\hat{\alpha}) + h^s(\bar{\alpha}_s) + c] \\ [\hat{\alpha}, s\hat{\alpha} + f^t(\alpha_t)P^{T(\hat{\alpha})}, g_s(\hat{\alpha}) + h^t(\alpha_t) + c] \end{array} \right.$$

$$P_4 \stackrel{t}{=} \left\{ \begin{array}{l} [\check{\alpha}, t\check{\alpha} + f^s(\alpha_s)P^{T(\check{\alpha})}, g_t(\check{\alpha}) + h^s(\alpha_s) + c] \\ [\check{\alpha}, s\check{\alpha} + f^t(\bar{\alpha}_t)P^{T(\check{\alpha})}, g_s(\check{\alpha}) + h^t(\bar{\alpha}_t) + c] \end{array} \right.$$

$$P_5 \stackrel{s}{=} [\bar{\alpha}_s, s\bar{\alpha}_s + (s\alpha + \beta)P^{T(\bar{\alpha}_s)}, g_s(\bar{\alpha}_s) + g_s(\alpha) + c]$$

$$P_6 \stackrel{t}{=} [\bar{\alpha}_t, t\bar{\alpha}_t + (t\alpha + \beta)P^{T(\alpha+\bar{\alpha}_t)}, g_t(\bar{\alpha}_t) + g_t(\alpha) + c]$$

Given this near 4×4 grid, the points $P_2, P_3,$ and P_4 tell us that we satisfy the following conditions:

$$\begin{aligned}
t\alpha^* + f^s(\alpha_s)P^{T(\alpha^*)} &= s\alpha^* + f^t(\alpha_t)P^{T(\alpha^*)} \\
t\hat{\alpha} + f^s(\bar{\alpha}_s)P^{T(\hat{\alpha})} &= s\hat{\alpha} + f^t(\alpha_t)P^{T(\hat{\alpha})} \\
t\check{\alpha} + f^s(\alpha_s)P^{T(\check{\alpha})} &= s\check{\alpha} + f^t(\bar{\alpha}_t)P^{T(\check{\alpha})}
\end{aligned}$$

Multiplying each equation by the appropriate power of P and adding equations we see that if we put

$$\bar{\alpha} = \alpha^* P^{T(\hat{\alpha}+\check{\alpha})} + \hat{\alpha} P^{T(\alpha^*+\check{\alpha})} + \check{\alpha} P^{T(\alpha^*+\hat{\alpha})} \quad (2.4)$$

then we also satisfy the following condition:

$$t\bar{\alpha} + f^s(\bar{\alpha}_s)P^{T(\bar{\alpha})} = s\bar{\alpha} + f^t(\bar{\alpha}_t)P^{T(\bar{\alpha})} \quad (2.5)$$

Given this near 4×4 grid we also satisfy another set of conditions:

$$\begin{aligned}
g_t(\alpha^*) + h^s(\alpha_s) &= g_s(\alpha^*) + h^t(\alpha_t) \\
g_t(\hat{\alpha}) + h^s(\bar{\alpha}_s) &= g_s(\hat{\alpha}) + h^t(\alpha_t) \\
g_t(\check{\alpha}) + h^s(\alpha_s) &= g_s(\check{\alpha}) + h^t(\bar{\alpha}_t)
\end{aligned}$$

Adding these equations together we get the equivalent condition:

$$g_t(\alpha^*) + g_t(\hat{\alpha}) + g_t(\check{\alpha}) + h^s(\bar{\alpha}_s) = g_s(\alpha^*) + g_s(\hat{\alpha}) + g_s(\check{\alpha}) + h^t(\bar{\alpha}_t) \quad (2.6)$$

We now ask if there is some point C which completes the 4×4 grid to give us property (G). This point would have to have the following coordinates:

$$C_s^t = \begin{cases} \left[\dot{\alpha}, t\dot{\alpha} + f^s(\bar{\alpha}_s)P^{T(\dot{\alpha})}, g_t(\dot{\alpha}) + h^s(\bar{\alpha}_s) + c \right] \\ \left[\dot{\alpha}, s\dot{\alpha} + f^t(\bar{\alpha}_t)P^{T(\dot{\alpha})}, g_s(\dot{\alpha}) + h^t(\bar{\alpha}_t) + c \right] \end{cases}$$

We note that if there is a solution it will be a unique solution.

This point is on both $A(t)_{L_2}$ and $A(s)_{L_2}$ if and only if

$$t\dot{\alpha} + f^s(\bar{\alpha}_s)P^{T(\dot{\alpha})} = s\dot{\alpha} + f^t(\bar{\alpha}_t)P^{T(\dot{\alpha})} \quad (2.7)$$

$$g_t(\dot{\alpha}) + h^s(\bar{\alpha}_s) = g_s(\dot{\alpha}) + h^t(\bar{\alpha}_t) \quad (2.8)$$

If we let $\dot{\alpha} = \bar{\alpha}$ as defined in equation 2.4 we have satisfied equation 2.7.

Then using equation 2.6 and the fact that

$$g_t(\alpha + \alpha') = g_t(\alpha) + g_t(\alpha') + \alpha \begin{pmatrix} 0 & t \\ t & 0 \end{pmatrix} \alpha'^T$$

we see that satisfying equation 2.8 depends on satisfying

$$t(\alpha^*P\hat{\alpha} + \alpha^*P\check{\alpha} + \hat{\alpha}P\check{\alpha}) = s(\alpha^*P\hat{\alpha} + \alpha^*P\check{\alpha} + \hat{\alpha}P\check{\alpha}).$$

Equivalently, since $t \neq s$, we must satisfy

$$\alpha^*P\hat{\alpha} + \alpha^*P\check{\alpha} + \hat{\alpha}P\check{\alpha} = 0$$

The point is that a solution to equations 2.7 and 2.8 does not depend on the choice of the function g_t . Then recalling that at least one choice g_t produces $H(3, q^2)$, which S.E.Payne has shown, see [8], has property(G) at the point (∞) , we see that we will satisfy equations 2.7 and 2.8 for any choice of g_t .

Therefore, when the near 4×4 grid contains lines $[A(t)]$ and $[A(s)]$ incident with (∞) , we have satisfied property(G) at the point (∞) . Similar computations show this is also true when the near 4×4 grid contains the lines $[A(\infty)]$ and $[A(t)]$, although we omit the details here.

2.11 A Theorem of Matt Brown

We now state a powerful result due to Matt Brown, see [5].

Theorem 2.11.1 *Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$ be a $GQ(q, q^2)$, $q > 1$, and assume that \mathcal{S} satisfies property(G) at some line l . Then \mathcal{S} is the dual of a flock- GQ .*

It follows that each EGQ constructed from the exotic elation groups of $H(3, q^2)$ are flock- GQ .

2.12 The Final Push

Consider the following theorem from [28].

Theorem 2.12.1 *Let \mathcal{S} be a GQ and let H be a group of whorls about the point x acting transitively on the set $X = P \setminus \{x\}^\perp$. The set of elations in H does not form a group if and only if (at least) one of the following conditions is satisfied:*

- (1) *There is a $j \geq 2$ for which $|\text{fix}(\sigma)| = j$ for some $\sigma \in H$.*
- (2) *There is a proper thick sub-GQ of \mathcal{S} containing x (and all the lines through x) fixed pointwise by a non-identity element of H .*

Theorem 2.12.2 *Let $\mathcal{S}(\mathcal{F})$ be a non-classical flock generalized quadrangle of order (q^2, q) , $q > 1$, q -even. Then the set of all elations about (∞) does form a group.*

Recall that ϕ is a whorl about (∞) that fixes more than one point in $P \setminus \{(\infty)\}$. It follows that every “exotic” EGQ that we have constructed is classical, and hence isomorphic to the Hermitian surface $H(3, q^2)$.

2.13 Suggested Problems

In this section we suggest how to further this research. First, and possibly the most obvious question:

Question (1): Are there any new examples of EGQ that may be constructed from these new groups?

We might also ask the following question:

Question (2): Are there conditions that guarantee an EGQ have non-isomorphic elation groups?

The following conjecture was recently made by K. Thas.

Conjecture 2.13.1 (K. Thas) *If $\text{Property}(F)$ does not hold for $(\mathcal{S}^{(p)}, G)$, then \mathcal{S} has non-isomorphic elation groups.*

Property (F) depends on whether each $A^* \in F^*$ is normal in the elation group.

Appendix A. Theorems

Lemma A.1 $d \sum_{i=1}^d t_i^2 \geq \left(\sum_{i=1}^d t_i \right)^2$.

Proof: Taken from [1].

Set $dm = \sum_{i=1}^d t_i$. Then after some straightforward manipulations we see that

$$0 \leq \sum_{i=1}^d (m - t_i)^2 = -\frac{\left(\sum_{i=1}^d t_i \right)^2}{d} + \sum_{i=1}^d t_i^2$$

The result easily follows. ■

We will use this lemma to help prove the following inequality due to Higman.

Theorem A.1 *Let $\mathcal{S} = (P, B, I)$ be a GQ of order (s, t) . Then $s \leq t^2$ and dually $t \leq s^2$. Furthermore, $t = s^2$ if and only if for some pair (x, y) of non-collinear points every triad (x, y, w) has exactly $s + 1$ centers if and only if every triad of points has exactly $1 + s$ centers.*

Proof: Taken from [22].

Now we let x, y be fixed non-collinear points with perp given by

$$\{x, y\}^\perp = \{z_0, \dots, z_t\},$$

and let $V = \{w_1, \dots, w_d\}$ be the set of all points such that $\{x, y, w\}$ is a triad. It follows that $d = s^2t - st - s + t$. Now for $1 \leq i \leq d$, let t_i be the number of z_j such that $z_j \in \{x, y, w_i\}^\perp$. And for $0 \leq i \leq t + 1$ let n_i be the number of triads $\{x, y, w\}$ with exactly i centers. Counting the total number of triads we get

$$\sum_{i=0}^{t+1} n_i = s^2t - st - s + t$$

Now counting the total number of ordered pairs (w, z) such that $z \in \{x, y, w\}^\perp$ we get

$$\sum_{i=1}^d t_i = \sum_{i=0}^{t+1} i n_i = (t+1)(t-1)s = (t^2 - 1)s$$

This follows since for each of the $t + 1$ points in $\{x, y\}^\perp$ there are s points on each of the $t - 1$ lines not through x or y .

Now counting the number of ordered triples (w, z, z') such that $w \in \{x, y, z, z'\}^\perp$ we get

$$\sum_{i=1}^d t_i(t_i - 1) = \sum_{i=0}^{t+1} i(i-1)n_i = \binom{t+1}{2} \cdot (t-1) \cdot 2 = (t^2 - 1)t$$

This follows since for each of the $\binom{t+1}{2}$ ways to pick z, z' from $\{x, y\}^\perp$, there are exactly $t - 1$ points (not in $\{x, y\}^\perp$) which are the intersection of lines through z, z' . But the triples are ordered and so it is obvious that

$$\sum_{i=1}^d t_i^2 = (t^2 - 1)(s + t)$$

If we put $dm = \sum_{i=1}^d t_i$ it follows from Lemma 1 that

$$0 \leq \sum_{i=1}^d (m - t_i)^2 = t(s-1)(s^2 - t)$$

It is now an easy conclusion that $t \leq s^2$. Furthermore, if $t = s^2$ we must have $m = t_i$ for each $1 \leq i \leq d$ and every triad has the same number of centers. In this case there are $s^4 - s^3 + s^2 - s$ total triads each having the same number k of centers. It follows that

$$k(s^4 - s^3 + s^2 - s) = \sum_{i=1}^d t_i = (s^4 - 1)s = s^5 - s$$

and we must have $k = s + 1$. ■

Theorem A.2 *Let G be a group of order s^2t and let $\mathbb{F} = \{A_0, A_1, \dots, A_t\}$ be a family of $t + 1$ subgroups, each with order s , and let $\mathbb{F}^* = \{A_0^*, A_1^*, \dots, A_t^*\}$ be another family of $t + 1$ subgroups, each having order st where $A_i \leq A_i^*$ for each $0 \leq i \leq t$. Then if we build the coset geometry $\mathcal{S}^{(\infty)}$ as prescribed above, $\mathcal{S}^{(\infty)}$ is a GQ, having order (s, t) , if and if properties K1 and K2 hold, where*

$$K1: A_j A_i \cap A_k = \{id\} \text{ for all distinct } i, j, k.$$

$$K2: A_j^* A_i = \{id\} \text{ for all } i \neq j.$$

Proof: We follow the proof in [20].

Two lines must be incident with at most one common point. We observe that two distinct lines of type (ii) are incident only at the point (∞) . Then for

each $0 \leq j \leq r$, the cosets $\{A_jg : g \in G\}$ partition the group elements, from which it follows that two lines A_jg and A_jh may only be incident at a point A_j^*g . Next suppose that two points are incident with two lines A_jg and A_ih , $i \neq j$. Since any element in a coset A_jg or A_ih can be chosen as a coset representative, we can WLOG assume that the points are group elements g and h . But then $g, h \in A_jg \cap A_ih$, or equivalently $id, gh^{-1} \in A_j \cap A_i$. We have shown that no two points are incident with two different lines if and only if $A_i \cap A_j = \{id\}$ for each $i \neq j$. From now, we assume that the following property holds:

$$P1 : A_i \cap A_j = \{id\} \text{ for all } i \neq j.$$

Next we show that there are no triangles in the geometry. First, there can be no triangle with vertex (∞) as no two points A_i^*g and A_j^*h , $i \neq j$, are on a common line, and no element g is incident with the point (∞) . Furthermore, since the cosets A_jg partition the group (and so intersect only on the line $[A_j]$), there can be no triangle with vertices A_j^*g, A_j^*h , and g , where $A_j^*g \neq A_j^*h$. We have two additional cases to consider.

First, suppose that A_j^*g, g , and h are the vertices of a triangle. Then there are cosets A_jg and A_jh which are contained in A_j^*g , and the elements g, h are in some coset A_ih , $i \neq j$. See Figure A.1.

But this is if and only if $g, h \in A_j^*g \cap A_ih$, or equivalently $id, hg^{-1} \in A_j^* \cap A_i$. It follows that no triangles of this type occur if and only if the following property holds.

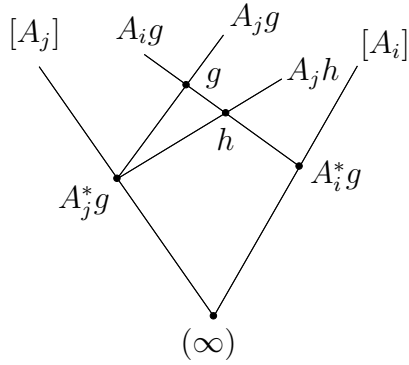


Figure A.1: $P2 : A_j^* \cap A_i = \{id\}$ for all $i \neq j$.

$$P2 : A_j^* \cap A_i = \{id\} \text{ for all } i \neq j.$$

From now assume that property $P2$ holds. We now have to show that there are no triangles in the geometry that have g, h , and u as its vertices as in Figure A.2.

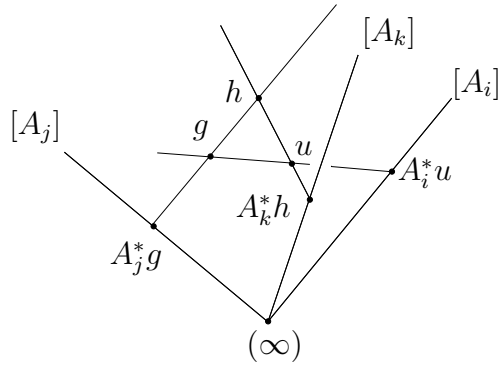


Figure A.2: $P3 : A_j A_i \cap A_k = \{id\}$ for all distinct i, j, k .

Assume that such a triangle exists. Then the following coset relationships would hold.

$$A_k h = A_k u \longrightarrow hu^{-1} \in A_k$$

$$A_i g = A_i u \longrightarrow gu^{-1} \in A_i$$

$$A_j g = A_j h \longrightarrow hg^{-1} \in A_j$$

But then $(hg^{-1}) \cdot (gu^{-1}) = hu^{-1}$ implies that $|A_j A_i \cap A_k| \geq 2$. Next assume that $|A_j A_i \cap A_k| \geq 2$. Then if $id \neq g \in A_j A_i \cap A_k$ we see that $A_k = A_k g$ and $g = a_j a_i$, giving us $A_j a_i = A_j g$ and since $g \neq a_i$ (which follows since $g \in A_k$ and property P_2 holds) the line $A_j g$ has the points g and a_i . But then the line A_i intersects $A_j g$ at the point a_i and the line A_k at the point id , giving us a triangle with vertices g, a_i , and id . See Figure A.3.

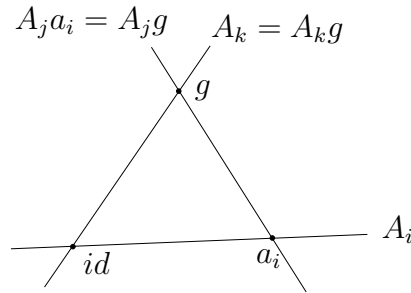


Figure A.3: $P3 : A_j A_i \cap A_k = \{id\}$ for all distinct i, j, k .

We have shown that no triangles exist, having vertices g, h and u , if and only if the following property holds.

$P3 : A_j A_i \cap A_k = \{id\}$ for all distinct i, j, k .

From now on we assume that property P_3 also holds. Our final step is to show that given a line l and a point P not on L there is a unique point-line pair (Q, m) such that $PI mIQIl$.

First, if (∞) is not on a line $A_i g$ then there is unique line $[A_i]$ and point $A_i^* h$ such that $(\infty)I[A_i]IA_i^* gIA_i g$. Next suppose that the point $A_i^* g$ is not incident with a line $A_i h$. Then then there is unique line $[A_i]$ and point $A_i^* h$ such that $A_i^* gI[A_i]IA_i^* hIA_i h$. We have to consider two additional cases.

First, suppose that the point $A_i^* g$ is not incident with a line $A_j h$, $i \neq j$. We need to find, as is pictured in Figure A.4, a point $x \in A_i^* g$ and a line $A_i g$ (uniqueness follows from property $P2$) such that $x \in A_i g \cap A_j h$.

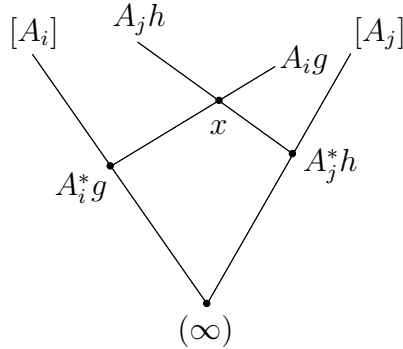


Figure A.4: $P4 : A_i^* A_j = G$ for all $i \neq j$.

So $A_i g = A_i x$, $A_j h = A_j x$, $A_i^* g = A_i^* x$, and $A_j^* h = A_j^* x$, giving us $x \in A_i^* g \cap A_j h$. But, the cosets $A_i^* g$ and $A_j h$ were chosen arbitrarily, and so for

each $g, h \in G$ there would have to be elements $a_i^* \in A_i^*$ and $a_j \in A_j$ such that $a_i^*g = a_jh$, or $gh^{-1} = (a_i^*)^{-1}a_j \in A_i^*A_j$. We have shown that this case holds if and only if the following property holds.

$$P4 : A_i^*A_j = G \text{ for all } i \neq j.$$

Obviously, for each $g \in G$, there is a unique line containing g and incident with a point on each line $[A_i]$. So finally, suppose that the point g is not incident with a line A_ih , that is $g \notin A_ih$. First define

$$\Omega = \cup\{A_i : 0 \leq r \leq r\}$$

Since P_1 and P_2 hold, each coset of A_i different from A_i but contained in A_i^* is disjoint from A_j , and we have the following

$$A_i^* \subseteq A_i \cup \{A_i g : A_i g \cap \Omega = \emptyset\}$$

Since $g \notin A_ih$, we can WLOG assume that the point is $id \notin A_i g$. First consider the case $g \in A_i^* \setminus A_i$. Here $A_i^*g = A_i^*$ is a point on the lines $A_i g$ and A_i , the second of which is collinear with the point id .

So we may assume that $g \notin A_i^*$. We need to find a line A_j such that $|A_j \cap A_i g| = 1$. So there must be an $i \neq j$ such that $A_j \cap A_i g \neq \emptyset$.

So if $A_i g$ is a coset of A_i disjoint from Ω , it must be that $A_i g \subset A_i^*$. But we have already shown that $A_i^* \subseteq A_i \cup \{A_i g : A_i g \cap \Omega = \emptyset\}$. So assuming that P_1 through P_4 holds, this case holds if and only if the following property holds.

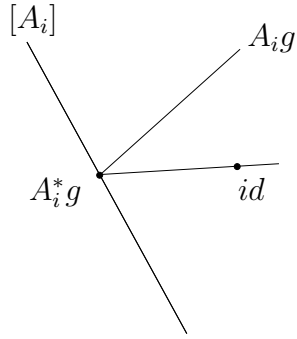


Figure A.5: $P_5 : A_i^* = A_i \cup \{A_i g : A_i g \cap \Omega = \emptyset\}$

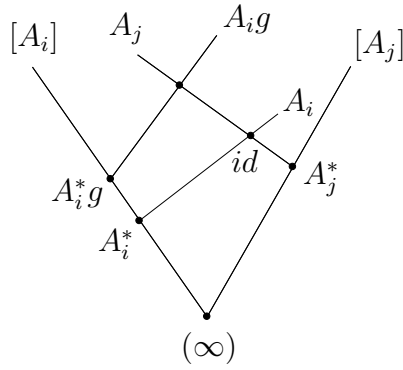


Figure A.6: $P_5 : A_i^* = A_i \cup \{A_i g : A_i g \cap \Omega = \emptyset\}$

$$P_5 : A_i^* = A_i \cup \{A_i g : A_i g \cap \Omega = \emptyset\}$$

Looking back at the properties P_1, \dots, P_5 it is easy to see that P_2 implies P_1 , and since G is finite, P_2 also implies P_4 . Hence we need only assume that properties P_2, P_3 , and P_5 hold. It turns out that P_5 holds if and only if $r = t$. We show this, and that the coset geometry is a $GQ(s, t)$, if and only if $r = t$ and properties P_2 and P_3 hold. Assuming that P_2 and P_3 hold we need the

following lemmas.

Lemma A.2 *Let $g \in G$ and $i \neq j$. Then $|A_j g \cap A_i| \leq 1$.*

Proof: (Lemma A.2) Suppose that both $x, y \in A_j g \cap A_i$. Then $x = a_j g = a_i$ and $y = a'_j g = a'_i$. Hence, $g = a'_i a'^{-1}_j = a_i a^{-1}_j$, and $a_i^{-1} a'_i = a_j^{-1} a'_j \neq id$ and we have violated property P_1 , and so also P_2 . ■

Lemma A.3 *Let $g \in \Omega \setminus A_j$. Then $A_j g \cap \Omega = \{g\}$.*

Proof: (Lemma A.3). Notice that $g \in A_i$, for some $i \neq j$, so $g = a_i$. But then $A_j \neq A_j g \subset A_j A_i$, whose intersection with every other A_k is the identity. Since $id \notin A_j g$ we must have $A_j g$ intersecting Ω only in the element g . ■

We next claim that if $S = (P, B, I)$ is the coset geometry defined above, then assuming properties $P2$ and $P3$, property $P5$ holds if and only if $r = t$. As there are $r + 1$ subgroups of order s in Ω , it is easy to see that $|\Omega \setminus A_j| = r(s - 1)$. This means that there are exactly $1 + r(s - 1)$ distinct cosets of A_j that intersect Ω , and so there are $st - [1 + r(s - 1)]$ cosets of A_i that are disjoint from Ω . If we assume that P_5 holds we get $|A_i^*| = st = s + s[st - 1 - r(s - 1)]$ which gives us $st(s - 1) = rs(s - 1)$, which holds if and only if $r = t$.

We relabel properties $P2$ and $P3$, as $K2$ and $K1$ respectively. Now with $r = t$ it is trivial to count that each line is incident with exactly $s + 1$ points, and that each point is on exactly $t + 1$ lines. This completes the proof. ■

Theorem A.3 *Using the Kantor family $(G^\otimes, \mathcal{J}(\mathcal{C}), \mathcal{J}^*(\mathcal{C}))$ as prescribed above, let $\mathcal{S} = GQ(\mathcal{C})$ be the EGQ. Then \mathcal{S} is a $GQ(q^2, q)$ isomorphic to the Hermitian surface $H(3, q^2)$.*

Proof: See [22]. ■

Theorem A.4 *The quadrangle $H(3, q^2)$ is isomorphic to the point-line dual of $Q(5, q)$.*

Proof: Taken from [22].

Let Q be an elliptic quadric of $PG(5, q)$, and extend $PG(5, q)$ to $PG(5, q^2)$. Then the extension of Q is an hyperbolic quadric Q^+ in $PG(5, q^2)$. Hence, Q^+ is the Klein quadric corresponding to the lines of $PG(3, q^2)$. So to Q in Q^+ there correspond a set V of lines in $PG(3, q^2)$, To a given line L of $Q(5, q)$ there correspond $q + 1$ coplanar lines through a point x of $PG(3, q^2)$. Let H be the set of points on the lines of V . Then with each point of $Q(5, q)$ there corresponds a line of V , and with each line of $Q(5, q)$ there corresponds a point of H . With distinct lines L, L' of $Q(5, q)$ correspond distinct points x, x' of H (a plane of Q^+ contains at most one line of Q). Since each point y of $Q(5, q)$ is on $q^2 + 1$ lines of $Q(5, q)$, these $q^2 + 1$ lines are mapped onto the $q^2 + 1$ points of the image of y . Hence we obtain an anti-isomorphism from $Q(5, q)$ onto the structure (H, V, I) , where I is the natural incidence relation. So (H, V, I) is a GQ of order (q^2, q) embedded in $PG(3, q^2)$. Then the following result of F. Buekenhout and C. Lefevre guarantees that (H, V, I) must be $H(3, q^2)$. ■

Theorem A.5 (Buekenhout, Lefevre) [4] *A projective GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ with ambient space $PG(n, q)$ must be obtained in one of the following ways:*

- (i) *There is a unitary or symplectic polarity π of $PG(n, q)$, $n = 3$ or 4 , such that \mathcal{P} is the set of absolute points of π and \mathcal{B} is the set of totally isotropic lines of π .*
- (ii) *There is a nonsingular quadric Q of projective index 1 in $PG(n, q)$, $n = 3, 4$ or 5 , such that \mathcal{P} is the set of points of Q and \mathcal{B} is the set of lines on Q .*

Proof: See [22].

■

Theorem A.6 *If $f : GF(q) \mapsto GF(q)$ is an additive function, then*

$$f(x) = a_0x + a_1x^p + a_2x^{p^2} + \cdots + a_{e-1}x^{p^{e-1}}$$

where $a_i \in GF(q)$.

Proof: Let $q = p^e$ and $f : GF(q) \mapsto GF(q)$ be the $GF(q)$ -additive (and $GF(p)$ -linear) function

$$f(x) = a_0x + a_1x^p + a_2x^{p^2} + \cdots + a_{e-1}x^{p^{e-1}}$$

Suppose that $f(x) = 0$ for all $x \in GF(q)$. Then since the $\deg[f(x)] = e - 1$ it must be the zero polynomial, and so $a_0 = a_1 = \cdots = a_{e-1} = 0$. Hence, the set $\{x, x^p, \dots, x^{p^{e-1}}\}$ are linearly independent in the additive group (or vector space) of $GF(p)$ -linear functions and so form a basis of a subspace of dimension

e. It follows that there are exactly q^e distinct functions of this form.

Now consider the entire additive group of operators $T : GF(q) \mapsto GF(q)$ where we think of the field as an e -dimensional vector space over \mathbb{Z}_p . The dimension of this vector space is the same as the dimension of all $e \times e$ matrices over $GF(p)$ which is e^2 (since there is a basis of matrices each with a single non-zero entry). Since the matrices have coefficients in \mathbb{Z}_p there are exactly $p^{e^2} = (p^e)^e = q^e$ linear operators T . But this is exactly the same number of $GF(q)$ -additive functions (which are $GF(p)$ -linear). Therefore, we have found all $GF(q)$ -additive functions. ■

Theorem A.7 *Let $g_t(\alpha)$ be a function from $GF(q) \times GF(q)$ into $GF(q)$. Then there is a distinct polynomial associated with $g_t(\alpha)$ of the form*

$$g_t(\alpha) = \sum_{0 \leq j, k \leq q-1} c_{j,k} \alpha_1^k \alpha_2^j, \text{ where } c_{j,k} \in GF(q)$$

Proof: Any polynomial of the form

$$g_t(\alpha = (\alpha_1, \alpha_2)) = \sum_{0 \leq i, j \leq q-1} c_{i,j} \alpha_1^i \alpha_2^j, \text{ where } c_{i,j} \in GF(q)$$

is a function from $GF(q) \times GF(q) \mapsto GF(q)$. We show that no two of these polynomials represent the same function.

Suppose that we have

$$f_t(\alpha) = \sum_{0 \leq i, j \leq q-1} c_{i,j} \alpha_1^i \alpha_2^j \quad \text{and} \quad g_t(\alpha) = \sum_{0 \leq i, j \leq q-1} d_{i,j} \alpha_1^i \alpha_2^j$$

Then suppose that

$$\begin{aligned}
0 = h(\alpha) &= f_t(\alpha) - g_t(\alpha) \\
&= \sum_{0 \leq i, j \leq q-1} c_{i,j} \alpha_1^i \alpha_2^j - \sum_{0 \leq i, j \leq q-1} d_{i,j} \alpha_1^i \alpha_2^j \\
&= \sum_{0 \leq i, j \leq q-1} (c_{i,j} - d_{i,j}) \alpha_1^i \alpha_2^j \text{ for all } \alpha_1, \alpha_2 \in GF(q)
\end{aligned}$$

If we fix $\alpha_2 = a$ then we get

$$\begin{aligned}
0 = h_t(\alpha) &= \sum_{0 \leq i, j \leq q-1} (c_{i,j} - d_{i,j}) \alpha_1^i a^j \\
&= \sum_{i=0}^{q-1} \left(\sum_{j=0}^{q-1} (c_{i,j} - d_{i,j}) a^j \right) \alpha^i
\end{aligned}$$

for all $\alpha \in GF(q)$.

But $h_t(\alpha)$ is a polynomial in α with degree less than q and so having q roots it must be the zero polynomial. It follows that

$$0 = \sum_{j=0}^{q-1} (c_{i,j} - d_{i,j}) a^j \text{ for all } a \in GF(q)$$

But this is again a polynomial in $a \in GF(q)$ of degree less than q with q roots and therefore we get $c_{i,j} = d_{i,j}$ for all $0 \leq i, j \leq q-1$, and no two distinct polynomials of this form will result in the same functional from $GF(q) \times GF(q)$

into $GF(q)$.

But now recall that there are exactly q^{q^2} functions from $GF(q) \times GF(q)$ into $GF(q)$ and this is the same number of distinct polynomials

$$f_t(\alpha) = \sum_{0 \leq j, k \leq q-1} c_{j,k} \alpha_1^k \alpha_2^j, \text{ where } c_{j,k} \in GF(q),$$

mapping $GF(q) \times GF(q)$ into $GF(q)$. This completes the proof.

■

Appendix B. The Hermitian Surface: A Unitary Representation

Let $q = 2^e$ and consider the projective space $PG(V)$, where V is an $(n+1)$ -dimensional vector space over $GF(q^2)$. Without loss of generality we can choose the Hermitian form $H : V \times V \mapsto GF(q)$ where

$$H(\bar{x}, \bar{y}) = x_1y_4^q + x_2y_3^q + x_3y_2^q + x_4y_1^q$$

That is, $H(\bar{x}, \bar{y}) = \bar{x}A(\bar{y}^q)^T$, where

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

The set of all absolute points and totally isotropic lines of $PG(3, q^2)$ forms the Hermitian surface $H(3, q^2)$. This is a GQ of order (q^2, q) .

The projective unitary group, denoted $PGU(4, q^2)$, is the subgroup of $PGL(4, q^2)$ preserving the Hermitian form. So $PGU(4, q^2) = \{B \in PGL(4, q^2) : BA(B^q)^T = kA, k \in GF(q^2)\}$ and $|PGU(4, q^2)| = q^6(q+1)(q^3+1)(q^4-1)$. If we adjoin the complete set of automorphisms of $GF(q^2)$ to $PGU(4, q^2)$, we form the group $P\Gamma U(4, q^2)$. This is the complete group of collineations of the Hermitian surface. Then $|P\Gamma U(4, q^2)| = |Aut(GF(q^2))| \cdot |PGU(4, q^2)| = 2e \cdot q^6(q+1)(q^3+1)(q^4-1)$.

The binary operation $*$ in $P\Gamma U(4, q^2)$ is composition of maps. Consider a point $x = (x_1, x_2, x_3, x_4) \in H(3, q^2)$ and elements $g = A \circ \sigma$ and $g' = A' \circ \sigma'$ in $P\Gamma U(4, q^2)$. We compute $x^{g \cdot g'}$ in a number of steps.

$$\begin{aligned}
x^A &= \left(\sum_{i=1}^4 x_1 a_{1,i}, \dots \right) \\
x^{A \circ \sigma} &= \left(\sum_{i=1}^4 x_1^\sigma a_{1,i}^\sigma, \dots \right) \\
x^{A \circ \sigma * A' \circ \sigma'} &= \left(\sum_4^{j=1} \left[\sum_{i=1}^4 x_1^{\sigma \cdot \sigma'} a_{1,i}^{\sigma \cdot \sigma'} \right] (a'_{1,j})^{\sigma'}, \dots \right) \\
&= \left(\sum_4^{j=1} \left[\sum_{i=1}^4 x_1 a_{1,i} \right] (a'_{1,j})^{\sigma^{-1}}, \dots \right)^{\sigma \cdot \sigma'}
\end{aligned}$$

It follows that in $P\Gamma U(4, q^2)$, we have the group product

$$A \circ \sigma * A' \circ \sigma' = \left(A \cdot (A')^{\sigma^{-1}} \right) \circ (\sigma \cdot \sigma').$$

Theorem B.1 *The set of all upper triangular matrices in $P\Gamma U(4, q^2)$ with ones on the diagonal forms a Sylow₂ subgroup of $P\Gamma U(4, q^2)$ having order q^6 .*

Proof: Consider the matrix

$$B = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & d & e \\ 0 & 0 & 1 & f \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Then

$$BA(B^q)^T = \begin{pmatrix} ab^q + ba^q + c + c^q & b + ad^q + e^q & a + f^q & 1 \\ e + da^q + b^q & d + d^q & 1 & 0 \\ f + a^q & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

and $B \in PGU(4, q^2)$ if and only if the following conditions hold: $d + d^q = 0$, $ab^q + ba^q + c + c^q = 0$, $f + a^q = 0$, and $e + da^q + b^q = 0$. It easily follows that there are q^6 such matrices in $PGU(4, q^2)$, and this set of matrices forms a Sylow₂ subgroup of $PGU(4, q^2)$. ■

We will call this group Sylow₂ subgroup U_2 . If we then adjoin to U_2 all of the field automorphisms of $GF(q^2)$ that have order a power of 2 we form a Sylow₂ subgroup (that we will denote Γ_2) of $P\Gamma U(4, q^2)$ having order $(\#aut) \cdot q^6$.

The group Γ_2 is the stabilizer of the flag in $H(3, q^2)$ having point $p = (0, 0, 0, 1)$ and line $x_1 = x_2 = 0$. We next construct the standard elation group about p .

If P is the set of all points of $H(3, q^2)$, we have $P \setminus \{p^\perp\} = \{(1, \alpha, \beta, \mu) \in PG(3, q^2) : \mu + \bar{\mu} + \alpha\bar{\beta} + \bar{\alpha}\beta = 0\}$. So there are q^5 points in $P \setminus \{p^\perp\}$, since $\alpha\bar{\beta} + \bar{\alpha}\beta \in GF(q)$ and $\mu + \bar{\mu}$ is the relative trace function mapping $\mu \in GF(q^2)$ to $GF(q)$. Furthermore, $p^\perp \setminus \{p\} = \{(0, 1, a, b) : a \in GF(q), b \in GF(q^2)\} \cup \{(0, 0, 1, c) : c \in GF(q^2)\}$, giving us all $q^3 + q^2 + 1$ points in p^\perp .

The group of matrices

$$M_p = \left\{ \begin{pmatrix} 1 & \alpha & \beta & \mu \\ 0 & 1 & 0 & \bar{\beta} \\ 0 & 0 & 1 & \bar{\alpha} \\ 0 & 0 & 0 & 1 \end{pmatrix} \in GL(4, q^2) : \mu + \bar{\mu} + \alpha\bar{\beta} + \bar{\alpha}\beta = 0 \right\}$$

is an elation group about p , as this group acts regularly on the set of points in $P \setminus \{p^\perp\}$ (the M_p -orbit of $(1, 0, 0, 0)$ is the set of points $\{(1, \alpha, \beta, \mu) : \mu + \bar{\mu} + \alpha\bar{\beta} + \bar{\alpha}\beta = 0\}$) and fixes every line through p .

Consider the group $G = \{(\alpha, \mu, \beta) : \alpha, \beta, \mu \in GF(q^2) : \mu + \bar{\mu} + \alpha\bar{\beta} + \bar{\alpha}\beta = 0\}$ with binary operation

$$(\alpha, \mu, \beta) \cdot (\alpha', \mu', \beta') = (\alpha + \alpha', \mu + \mu' + \alpha\bar{\beta}' + \beta\bar{\alpha}', \beta + \beta')$$

This group is the standard elation group of $H(3, q^2)$ (when viewed as an EGQ).

If we form the map

$$T : (\alpha, \mu, \beta) \mapsto \begin{pmatrix} 1 & \alpha & \beta & \mu \\ 0 & 1 & 0 & \bar{\beta} \\ 0 & 0 & 1 & \bar{\alpha} \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

we see that $T[(\alpha, \mu, \beta) \cdot (\alpha', \mu', \beta')] = T[(\alpha, \mu, \beta)] \cdot T[(\alpha', \mu', \beta')]$. Therefore, M_p is the standard elation group about p .

Next consider the Hermitian preserving involution

$$\phi : (a, b, c, d) \mapsto (\bar{a}, \bar{b}, \bar{c}, \bar{d}).$$

Then, ϕ fixes p . Moreover, $\phi : (0, 0, 1, w) \mapsto (0, 0, 1, \bar{w})$, and if $y \in GF(q)$ then $\phi : (0, 1, y, w) \mapsto (0, 1, y, \bar{w})$. Since all Hermitian lines through p will be either $L_y = \{(0, 1, y, 0) + w(0, 0, 0, 1)\} \cup \{(0, 0, 0, 1)\}$ or $L' = \{(0, 0, 1, 0) + w(0, 0, 0, 1)\} \cup \{(0, 0, 0, 1)\}$, we see that ϕ fixes all lines through p . Yet ϕ fixes the set of points in $\{(1, \alpha, \alpha, \mu) : \alpha, \mu \in GF(q)\}$, which are in $P \setminus \{p^\perp\}$. So ϕ is a whorl about p , and $M_p \times \langle \phi \rangle$ is a Sylow₂ subgroup of the group of whorls about p .

REFERENCES

- [1] L. BATTEN. *Combinatorics of Finite Geometries*, second edition. Cambridge University Press, Cambridge England. 1997.
- [2] A. BEUTELSPACHER AND U. ROSENBAUM. *Projective Geometry*. Cambridge University Press, Cambridge, England. 1998.
- [3] R.C. BOSE. Strongly regular graphs, partial geometries and partially balanced designs. *Pacific Journal of Mathematics*. 13 pp. 389-419. 1963.
- [4] F. BUEKENHOUT AND C. LEFEVRE. Generalized quadrangles in projective spaces. *Arch. Math.* 25 pp.540-552. 1974.
- [5] M. BROWN. Projective ovoids and generalized quadrangles. *Transactions of the American Mathematical Society*. 200?.
- [6] P.J. CAMERON *Projective and Polar Spaces* QMW Maths Notes 13. Queen Mary and Westfield College, London E1 4NS.
- [7] X. CHEN. On the groups that generate skew-translation generalized quadrangles. Unpublished manuscript.
- [8] I. CARDINALI AND S.E. PAYNE *The q -clan geometries with $q = 2^e$* . <http://www-math.cudenver.edu/spayne/>. 2002.
- [9] P. DEMBOWSKI. *Finite Geometries*. Springer-Verlag, Berlin, Germany, 1968.
- [10] W. FEIT AND G. HIGMAN. The existence of certain generalized polygons. *Journal of Algebra*, 1:114-131, 1964.
- [11] D.G. GLYNN The hering classification for inversive planes of even order. *Simon Stevin* 58, 319-353, 1984.
- [12] L.C. GROVE. *Classical Groups and geometric Algebra*, volume 39 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, Rhode Island. 2001.

- [13] D.G. HIGMAN. Partial geometries, generalized quadrangles and strongly regular graphs. *Atti convegno di geometria e sue applicazioni* (ed. A. Barlotti). Perugia, pp. 263-293. 1971.
- [14] W. KANTOR. Generalized polygons, SCABs and GABs. *Lecture Notes in Mathematics*, Vol 1181. Springer, Berlin. 1986.
- [15] M. LAW AND T. PENTTILA. Flocks, ovals and generalized quadrangles (Four Lectures in Napoli). 2000.
- [16] C.M. O'KEEFE AND T. PENTTILA. Characterisations of flock quadrangles. *Geometriae Dedicata*, Vol. 82 pp.171-191. 2000.
- [17] S.E. PAYNE. A new infinite family of generalized quadrangles. *Congr. Numer.*, Vol. 49 pp. 115-128. 1985
- [18] S.E. PAYNE. An essay on skew translation generalized quadrangles. *Geometriae Dedicata*, 32:93-118, 1989.
- [19] S.E. PAYNE. *Elation generalized quadrangles*. Hand written notes. <http://www-math.cudenver.edu/~spayne/>. 1994.
- [20] S.E. PAYNE. *Lectures on finite generalized quadrangles*. <http://www-math.cudenver.edu/~spayne/>. 2000.
- [21] S.E. PAYNE. Trace equation over finite fields of characteristic 2. *Notes from UCD geometry seminar*. 2004.
- [22] S.E. PAYNE AND J. THAS. *Finite Generalized Quadrangles*, volume 110 of *Research Notes in Mathematics*. Pitman Publishing Inc., Boston 1984.
- [23] S.E. PAYNE AND K. THAS. Notes on Elation Generalized Quadrangles. *European Journal of Combinatorics*, Vol. 24 pp.969-981. 2003.
- [24] TIM PENTTILA. Private Communication. 2004
- [25] T. PENTTILA AND C. PRAEGER. Ovoids and Translation Ovals. *J. London Math. Soc.*, (2) 56 (1997) 607-624.
- [26] J. ROTMAN. *An Introduction to the Theory of Groups*, Fourth edition. Springer-Verlag New York, Inc. 1995.
- [27] J.A. THAS. Generalized quadrangles and flocks of cones. *European Journal of Combinatorics*, Vol. 8 pp. 441-452. 1987.

- [28] K. THAS AND S.E. PAYNE. Foundations of generalized quadrangles. *European Journal of Combinatorics*, Vol. 27 pp.51-62. 2006.
- [29] J. TITS. Sur la trialité et certains groupes qui s'en déduisent. *Inst. Hautes Etudes Sci. Publ. Math.*, 2:14-60, 1959.
- [30] H. VAN MALDEGHEM. *Generalized Polygons*, volume 93 of *Monographs in Mathematics*. Birkhäuser Verlag, Berlin 1998.