UNITALS EMBEDDED IN FINITE PROJECTIVE PLANES

by

Kenneth L. Wantz

A dissertation submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematical Sciences

Fall 1995

UNITALS EMBEDDED IN FINITE PROJECTIVE PLANES

by

Kenneth L. Wantz

Approved: ______________________________

L. Pamela Cook, Ph.D.
Chair of the Department of Mathematical Sciences

Approved: ______________________________

John C. Cavanaugh, Ph.D.
Interim Associate Provost for Graduate Studies

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: ______________________________

Gary L. Ebert, Ph.D.
Professor in charge of dissertation

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: ______________________________

Felix Lazebnik, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: ______________________________

Renate Scheidler, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: ______________________________

Andrew J. Woldar, Ph.D.
Member of dissertation committee

ACKNOWLEDGEMENTS

My appreciation and respect are due to Gary Ebert, my thesis advisor. I am grateful for his excellence in his field, his excitement over my accomplishments, and his exceptional investment of time and attention.

Many thanks are in order to the committee members for their attention to detail and affirming comments. In addition, I found the perspective and scrutiny of R. D. Baker very beneficial in the final stages of completing Chapter 4. I also wish to acknowledge the fellow graduate students who have encouraged, enriched, and endured these years with me.

I am indebted to my wife Elizabeth for her unfailing devotion and unconditional acceptance throughout all the events of life, particularly this monumental portion. As a thankful father, I wish to acknowledge Ruthanna Grace, whose birth inaugurated a most fruitful period of research. Moreover, the support of all those that constitute "family" has been invaluable.

Without question, my greatest provision of peace, courage, and perseverance has been the Eternal Source. "In all thy ways acknowledge him, and he shall direct thy paths" (Proverbs 3:6 KJV).

TABLE OF CONTENTS

ABSTRACT

A unital is a 2-$(q^3+1, q+1, 1)$-design. Unitals embedded in finite projective planes are studied in two settings: the classical projective plane $PG(2, q^2)$ and the Hughes plane of order q^2. The main results involve a characterization of Buekenhout-Metz unitals in the former and the identification of a new family of unitals in the latter.

In the study of the Buekenhout-Metz unitals embedded in $PG(2, q^2)$, the points of the unital which lie on the tangent lines through a point not belonging to the unital are classified. Moreover, a group theoretic characterization of Buekenhout-Metz unitals is obtained. It is shown that a unital U embedded in $PG(2, q^2)$ is a Buekenhout-Metz unital if and only if U admits a linear collineation group that is a semidirect product of a Sylow p-subgroup of order q^3 by a subgroup of order $q-1$. In addition, a new group theoretic characterization of the classical or Hermitian unital is obtained.

Several tools involving incidence in the Hughes plane are developed in order to study unitals embedded therein. New results are obtained regarding the Rosati unital embedded in the Hughes plane. The orbit structure of the points of the Rosati unital under the group which leaves the unital invariant is determined. Furthermore, the points of the Rosati unital which lie on the tangent lines through a point off the unital are determined. The Rosati unital is found to be a member of a previously unknown family of unitals in the Hughes plane. The collineation group leaving the unitals invariant is determined, as well as the orbit structure under a certain point-stabilizer. This new family of unitals is sorted according to projective equivalence and the Rosati unital is found to be self-dual.

Chapter 1

INTRODUCTION

If one were to describe Euclidean geometry as the geometry obtainable by compass and straight edge, then *projective geometry* could be described as the geometry obtained from a straight edge alone (Coxeter [22] page 1). Mankind naturally views and desribes the world "projectively", from the simplistic notion that the rails of a railroad track eventually meet beyond the horizon, to the complexities of perspective drawing in art. This concept of "central projection" still proves invaluable in the development of modern computer graphics.

The discussion of the historical roots of projective geometry should perhaps begin with the discoveries of Pappus of Alexandria in the third century. In the 1600s, both Johann Kepler and Girard Desargues began to wrestle with the notion of a "point at infinity". Later, in the nineteenth century, Poncelet laid the foundation for the field of projective geometry by introducing the concept of a "line at infinity" containing these points. In 1872, Felix Klein instituted the Erlangen program which classified geometries and "gave projective geometry the prominent place it deserves" (Smart [58] page 250). The Erlangen program was based on a distinctly algebraic viewpoint, namely, that the essential properties of a geometry could be determined by studying the group of "automorphisms" of the geometry.

Finite projective geometry is primarily a phenomenon of the twentieth century. It has influenced and been influenced by many of the mathematical fields spawned in this century. Finite geometries provided some of the earliest examples of block designs used by R. A. Fisher in the design of experiments in the 1930s. Also, the interaction of finite geometry with group theory, particularly the study of finite simple groups, has been mutually beneficial. Since World War II, finite geometry has contributed to coding theory; in particular, it provides the basis for the Hamming codes. Although this list is far from complete, we finally note that the potential for the use of finite geometry in cryptography has been demonstrated by the development of certain multi-level threshold schemes.

1.1 Projective and Affine Planes

A *projective plane* is a set of objects, called *points*, and a collection of subsets of points, called *lines*, satisfying:

(i) every pair of distinct points lie on a unique common line;

(ii) every pair of distinct lines must meet in a unique common point;

(iii) there exists a set of four points such that no three points are collinear.

The *classical* projective plane is obtained from a three-dimensional vector space V over a field F by defining points to be one-dimensional subspaces and lines to be two-dimensional subspaces of V. Let $GF(q)$ denote a finite field of order q, where q is a prime power. Then the classical projective plane over $GF(q)$ is denoted by $PG(2,q)$. We note that nonclassical projective planes do exist, that is, planes which are not "coordinatized" by a field. This document will deal solely with finite projective planes, i.e., those having a finite number of points and lines. The first known finite example of a nonclassical projective plane was found by Veblen and Wedderburn [61] in 1906. This example was later found to belong to an infinite class of nonclassical projective planes discovered by Hughes [38]. Hereafter, π will refer to $PG(2,q)$, while Π will denote an arbitrary finite projective plane.

Using the three axioms given above, one can show that there is a unique integer $n \geq 2$, called the *order*, associated with any finite projective plane such that the plane consists of n^2+n+1 points and n^2+n+1 lines. Moreover, each line contains exactly $n+1$ points and $n+1$ lines pass through each point. For our purposes, n will always be a power of a prime number; indeed, this is true of all known finite projective planes.

Let $\pi = PG(2,q)$ with V being the underlying three-dimensional vector space over $F = GF(q)$. As each point of π consists of all F-scalar multiples of a non-zero vector in V, we may choose a normalized representative for each point. For instance, if one is using left-normalized representatives, the points of π may be represented by the vectors $(0,0,1), (0,1,z)$, and $(1,y,z)$ for $y, z \in F$. When there is no danger of confusion, we will often refer to a point by any one of its nonzero representatives. As each line of π corresponds to a hyperplane of V, it consists of all points (x,y,z) for which $Ax+By+Cz=0$, for some constants $A,B,C \in F$, not all zero. Thus lines of π may be represented by triples $[A,B,C]$, also viewed as vectors in V. We see that $(x,y,z) \in [A,B,C]$ if and only if $(x,y,z) \cdot [A,B,C] = 0$. Since any nonzero scalar multiple of $[A,B,C]$ will contain precisely the same points of π, we may normalize these line coordinates as well. Using square brackets to denote line coordinates and choosing right-normalized representatives for instance, the lines of π may be represented by the vectors $[1,0,0], [A,1,0]$, and $[A,B,1]$ for $A,B \in F$. Points and lines of π will be described in terms of such *homogeneous coordinates* throughout this document. As a matter of convenience, we may normalize from the left, right, or even the center coordinate. Finally, as π consists of q^2+q+1 points and q^2+q+1 lines, we see that $PG(2,q)$ is a projective plane of order q.

An *affine plane* is a set of objects, called *points*, and a collection of subsets of points, called *lines*, satisfying:

(i) every pair of distinct points lie on a unique common line;

(ii) given any point P and a line l, with $P \notin l$, there exists a unique line l' such that $P \in l'$ and $l \cap l' = \emptyset$;

(iii) there exist three noncollinear points.

Two lines are called *parallel* if they are identical or disjoint as sets. Using the above axioms, one can easily show that parallelism is an equivalence relation on the lines of an affine plane and each point lies on a unique line of each parallel class.

The *classical* affine plane is obtained from a two-dimensional vector space W over a field F by defining points to be vectors of W (including the zero vector) and lines to be additive cosets of one-dimensional subspaces of W. If F is a finite field of order q, we write $AG(2,q)$ for the classical affine plane. It should be noted once again that nonclassical affine planes, both finite and infinite, do exist. Associated with any finite affine plane is an integer $n \geq 2$, called the *order*, such that the plane consists of n^2 points and n^2+n lines. In addition, each line contains exactly n points and $n+1$ lines pass through each point. Thus there are $n+1$ parallel classes of lines, each class having size n. Finally, notice that $AG(2,q)$ has order q.

Let $\boldsymbol{\pi}$ be any affine plane. For each parallel class of lines, $\mathcal{L}$, define a new point, $\mathcal{L}^*$, which is added to each line of $\mathcal{L}$ and no other lines of $\boldsymbol{\pi}$. In addition, define a new line, l_∞, which contains all of these new points and no other point of $\boldsymbol{\pi}$. It is straightforward to show that this new structure is a projective plane. In this way, a unique projective plane is obtained from a given affine plane, by adding the so-called *line at infinity*. The resulting projective plane is called the *projective completion* of the affine plane $\boldsymbol{\pi}$.

Let Π be a projective plane with l a line of Π. We define Π^l to be the structure obtained from Π by deleting l and all its points. One can show that Π^l is an affine plane. For $\pi = PG(2,q)$, π^l is isomorphic to $AG(2,q)$ for any choice of l in π. In this case, we often choose l to be the line $x=0$ or the line $z=0$. For instance, when $x=0$ is the "line at infinity", π^l consists of the points $(1,x,y)$ for $x,y \in F$. Points of π^l naturally correspond to the standard model of $AG(2,q)$ via $(1,x,y) \leftrightarrow (x,y)$. Using this correspondence, a point $(1,x,y)$ of π will be referred to as an "affine point", while $(0,0,1)$ and $(0,1,x)$, for $x \in F$, are called "points at infinity". We note that for nonclassical projective planes Π, it is possible that Π^{l_1} and Π^{l_2} are nonisomorphic for distinct lines l_1 and l_2 of Π.

1.2 Collineations, Correlations, and Forms

A *collineation* of a projective (or affine) plane Π is an incidence preserving bijection on the points of Π which induces a bijection on the lines of Π. The group of all collineations of Π is denoted by $\mathrm{Aut}(\Pi)$ and any subgroup of $\mathrm{Aut}(\Pi)$ will be referred to as a *collineation group* of Π.

It may be shown that any nontrivial collineation which fixes every point on some line of Π (called the *axis*) must also fix all lines through some point of Π (called the *center*); moreover, such a collineation cannot fix any other points or lines of Π. Dually, any nontrivial collineation which fixes every line through some point of Π must also fix all points on some line, while fixing no other points or lines. Such a collineation, with axis l and center P, is called a *(P,l)-perspectivity.* If $P \in l$, the perspectivity is called an *elation.* If $P \notin l$, the perspectivity is called a *homology.* One may easily distinguish between elations and homologies with group theory. Specifically, if Π is a projective plane of order n and k is the order of a perspectivity $\alpha \in \mathrm{Aut}(\Pi)$, then either k divides n and α is an elation or k divides $n-1$ and α is a homology.

Let V be a three-dimensional vector space over $F = GF(q)$ and let θ be a field automorphism of F. A *semilinear transformation associated with* θ is a mapping $\psi : V \to V$ satisfying

(i) $\psi(u+v) = \psi(u) + \psi(v)$;

(ii) $\psi(kv) = k^\theta \psi(v)$,

for all $u, v \in V$ and all $k \in F$. If ψ is bijective, then ψ is called *nonsingular.* The set of all nonsingular semilinear transformations from V to V forms a group under composition which will be denoted by $\Gamma L(3,q)$. It is easy to see that $\Gamma L(3,q)$ is isomorphic to the semidirect product of $GL(3,q)$, the nonsingular 3×3 matrices over F, by the automorphism group of F. Viewing V as the underlying vector space for $\pi = PG(2, q)$, we see that every element of $\Gamma L(3, q)$ induces a collineation of π by permuting row vector representations of points via the action of a field automorphism on each coordinate, followed by matrix multiplication on the right. The center, Z, of $\Gamma L(3, q)$ consists of those semilinear transformations for which θ is the identity and the matrices are scalar multiples of the identity matrix. As scalar multiples of the same matrix will induce the same collineation of π, we see that $\Gamma L(3, q)/Z(\Gamma L(3, q))$ acts faithfully on $PG(2, q)$. This collineation group is called the *projective gamma linear group*, $P\Gamma L(3, q)$. The Fundamental Theorem of Projective Geometry states that every collineation of $\pi = PG(2, q)$ is induced by an element of $\Gamma L(3, q)$, i.e. $P\Gamma L(3, q) \cong \mathrm{Aut}(\pi)$.

We restate that the center of $GL(3, q)$ consists of scalar multiples of the identity matrix and we define the *projective general linear group* as $PGL(3, q) = GL(3, q)/Z(GL(3, q))$. Of course, $PGL(3, q)$ also acts faithfully on $\pi = PG(2, q)$. One immediately sees that $PGL(3, q) \triangleleft P\Gamma L(3, q)$. It is also well-known that all perspectivities of π are elements of $PGL(3, q)$; in fact, these perspectivities generate $PGL(3, q)$. One usually refers to a product of perspectivities as a *projectivity*. Hence $PGL(3, q)$ is often called the *projective group* of π. We will also refer to any subgroup of $PGL(3, q)$ as a *linear* collineation group of π.

Suppose π is any affine plane with Π its projective completion and with l being the line at infinity. A collineation of π is called a *dilatation* if it is a perspectivity with axis l when considered as a collineation of Π. A *translation* of π is a dilatation which is an elation with axis l when considered as a collineation of Π. Thus a nonidentity translation preserves the parallel classes and fixes the lines of exactly one parallel class of π. Moreover it fixes no points of π. An affine plane π is called a *translation plane* if the group of all translations of π is transitive on the points of π. A projective plane Π is called a *translation plane with respect to* *the line* l if Π^l is an affine translation plane. The translation group of $AG(2,q)$ consists of the q^2 maps of the form $T_w : v \mapsto v + w$ for each $w \in W$ (the underlying two-dimensional vector space). It is then clear that $PG(2,q)$ is a translation plane with respect to any line l.

A *correlation* of a projective plane Π is a bijection mapping points to lines and lines to points which reverses inclusion. That is to say, if δ is a correlation of Π and P and l are a point and line of Π, respectively, then $P \in l$ if and only if $l^\delta \in P^\delta$. A point P (line l) is called an *absolute* point (line) of a correlation δ if $P \in P^\delta$ ($l^\delta \in l$). A *polarity* is a correlation of order two. Although not all projective planes admit polarities, every classical projective plane admits one or both of two polarities which we will proceed to describe.

Let V be the three-dimensional vector space over $F = GF(q)$ associated with $PG(2,q)$, and let θ be a field automorphism of F. A *sesquilinear form* s *with associated field automorphism* θ is a mapping from $V \times V$ into F for which

(i) $s(u+v,w) = s(u,w) + s(v,w)$ and $s(u,v+w) = s(u,v) + s(u,w)$;

(ii) $s(ku,v) = ks(u,v)$ and $s(u,kv) = k^\theta s(u,v)$,

for all $u,v,w \in V$ and for all $k \in F$. If θ is the identity, then s is called a *bilinear form.* If in addition, $s(u,v) = s(v,u)$ for all $u,v \in V$, then s is a *symmetric bilinear form.* If θ has order two and $s(u,v) = s(v,u)^\theta$ for all $u,v \in V$, then s is called a *hermitian form.* We define the *radical* of V with respect to a sesquilinear form s to be

$$V^\perp = \{u \in V : s(u,v) = 0 \text{ for all } v \in V\}.$$

A sesquilinear form is *nondegenerate* if $V^\perp = \{0\}$.

For a given sesquilinear form s, it is clear that the map $\delta : W \to W^\perp = \{v \in V : s(v,w) = 0 \text{ for all } w \in W\}$, for $W < V$ and $W \neq \{0\}$, interchanges points and lines and reverses inclusion. If s is nondegenerate, it can be shown that δ is a bijection, and hence a correlation, of $PG(2,q)$ [6]. Conversely, if δ is any correlation of $PG(2,q)$, then there exists a nondegenerate sesquilinear form s on V which induces δ in the manner given above [6]. Moreover, if the sesquilinear form s induces a correlation which is a polarity, then s is either symmetric bilinear or hermitian [6]. The polarities corresponding to these forms are called *orthogonal* and *unitary*, respectively. It should be noted that unitary polarities only exist in square-order fields, in which case the involution θ is uniquely determined. With $o(F)$ denoting the order of F, if $o(F) = q = d^2$, then the automorphism θ acts via $x \mapsto x^d$, for $x \in F$. For the sake of completeness, we note that projective spaces of odd dimension may admit a third type of sesquilinear form and its induced polarity, namely, the *skew symmetric bilinear form* which induces a *symplectic* or *null* polarity.

A *quadratic form* is a mapping Q from V to F satisfying

(i) $Q(ku) = k^2 Q(u)$ for all $u \in V$ and $k \in F$;

(ii) $Q(u+v) - Q(u) - Q(v)$ is a symmetric bilinear form.

If F has odd characteristic, a quadratic form is called *nondegenerate* if its associated symmetric bilinear form is nondegenerate. In this case, a symmetric bilinear form s uniquely determines a quadratic form via $Q(v) = \frac{1}{2}s(v,v)$. If F has even characteristic, Q is called *nondegenerate* if $Q(v) \neq 0$ for all nonzero $v \in V^{\perp}$. From elementary linear algebra, we know that for any symmetric bilinear form s over V, there exists a unique (with respect to a given basis), symmetric 3×3 matrix A over F such that $s(u,v) = uAv^t$. If F has odd characteristic, then s is nondegenerate if and only if the associated matrix A is nonsingular. Therefore, for every quadratic form Q, there exists a symmetric 3×3 matrix A over F such that $Q(v) = vAv^t$, when q is odd. Moreover, this matrix is unique, with respect to a given basis.

A matrix H over a square-order field F is said to be *hermitian* if $H^{(\theta)} = H^t$, where $H^{(\theta)}$ is the matrix obtained by acting on each entry of H with the unique, involutory, field automorphism θ. Then for any hermitian form s over V there exists a hermitian 3×3 matrix H over F such that $s(u,v) = uHv^{(\theta)t}$. Here again, if F

has odd characteristic, then s is nondegenerate if and only if H is nonsingular. Due to lack of better terminology, we will refer to the map $h : V \to F$ via $h(v) = s(v, v)$ as a hermitian form as well. Thus, there exists a hermitian matrix H such that $h(v) = vHv^{(\theta)t}$.

We make one final note before proceeding with applications of these concepts. Let $v \in V$ be a nonzero vector representing a point of $PG(2, q)$. Then v is an absolute point of an orthogonal polarity if and only if $v \in \langle v \rangle^\perp$, where $\perp$ is taken with respect to the associated symmetric bilinear form s. But this occurs if and only if $s(v, v) = 0$. Thus, for q odd, we speak of a point as being an absolute point of a quadratic form (meaning $Q(v) = 0$) with the understanding that we are really referring to the action of the polarity induced by the associated symmetric bilinear form. For any prime power q, we similarly refer to the absolute points of a hermitian form (meaning $h(v) = 0$) with the understanding that these points are absolute points of the unitary polarity induced by the associated hermitian form. When q is an even prime power, the "zeroes" of a nondegenerate quadratic form do not correspond to the absolute points of any orthogonal polarity, but we will still refer to such points as absolute points of the form.

1.3 Conics

It is natural to study those points of $PG(2, q)$ which lie on some algebraic curve. One may choose to study such a set of points in a purely combinatorial setting or the setting of algebraic geometry, as well as studying the automorphism groups of these structures. Of course, linking these viewpoints is highly desirable. One curve of particular intersect is the *conic*, the set of absolute points of a nondegenerate quadratic form. A detailed description of conics in $PG(2, q)$, for q an odd prime power, will be given. This information will also prove to be helpful in Chapter 4. A brief discussion of the even case is also included.

Let V be the underlying three-dimensional vector space over $F = GF(q)$ for $\pi = PG(2, q)$, where q is an odd prime power. It can be shown that any two conics in π are projectively equivalent, i.e. there exists a collineation in $PGL(3, q)$ which maps any conic to any other conic. It is then sufficient to study the properties of only one particular conic. It is our desire to work with the conic described by the quadratic form Q given by $Q(x, y, z) = xz - y^2$, for $(x, y, z) \in V$. We see that the matrix associated with this quadratic form is

$$\begin{pmatrix} 0 & 0 & 1/2 \\ 0 & -1 & 0 \\ 1/2 & 0 & 0 \end{pmatrix}. \tag{1.1}$$

Note that Q is nondegenerate as this matrix is nonsingular. Letting $\mathcal{C}$ denote this conic, we see that

$$\mathcal{C} = \{(x, y, z) : xz - y^2 = 0\}. \tag{1.2}$$

If $(x, y, z) \in \mathcal{C}$ with $x = 0$, then we must have $y = 0$. This gives $(0, 0, 1)$ as the only point of $\mathcal{C}$ for which $x = 0$. If $(x, y, z) \in \mathcal{C}$ with $x \neq 0$, we normalize by setting $x = 1$. This gives q points of C of the form $(1, y, y^2)$ for $y \in F$. Therefore a conic consists of $q + 1$ points. In particular,

$$\mathcal{C} = \{(1, y, y^2) : y \in F\} \cup \{(0, 0, 1)\}. \tag{1.3}$$

A line $[A, B, C]$ of π contains the point $(0, 0, 1)$ if and only if $C = 0$. A line $[A, B, C]$ contains a point $(1, y, y^2)$, for $y \in F$, if and only if

$$A + By + Cy^2 = 0. \tag{1.4}$$

It is evident that no more than two points of $\mathcal{C}$ may lie on a line of π. Lines of π which meet $\mathcal{C}$ in 0, 1, or 2 points will be called *passants*, *tangents*, or *secants*, respectively. For a given point $P \in \mathcal{C}$, we see that of the $q + 1$ lines through P, a distinct line is required to join P to each of the other q points of $\mathcal{C}$. Thus q of the lines through P are secant to $\mathcal{C}$, leaving a unique tangent line to $\mathcal{C}$ at the point P. From a combinatorial point of view, we then count $q+1$ tangents and $\binom{q+1}{2}$ secants to $\mathcal{C}$. The remaining $\binom{q}{2}$ of the q^2+q+1 lines of π are necessarily passants to $\mathcal{C}$. Algebraically, it is not difficult to check whether the line $[A, B, C]$ is tangent, secant, or passant to the particular conic $\mathcal{C}$. One simply checks that the discriminant B^2-4AC (from Equation 1.4) is 0, contained in F_S, or contained in F_N, respectively, where F_S denotes the non-zero squares of F and F_N the non-squares.

Let us now consider the case when q is an even prime power. It may again be shown that all conics are projectively equivalent and that $xz-y^2$ is a nondegenerate quadratic form. Thus, we may again define a conic $\mathcal{C}$ as in 1.3. One may count the same numbers of tangents, secants, and passants for q even as one has for q odd. The even and odd case do differ, however, on an issue concerning tangent lines to the conic. If q is odd, it may be shown without difficulty that every point not on $\mathcal{C}$ lies on exactly two tangent lines to $\mathcal{C}$. If q is even, one may easily show that all of the tangent lines to $\mathcal{C}$ pass through a common point. This point is called the *knot* or the *nucleus* of the conic. The knot of $\mathcal{C}$ is the point $(0, 1, 0)$.

The subgroup of $PGL(3, q)$, for any prime power q, leaving $\mathcal{C}$ invariant is known to act triply transitive on the points of $\mathcal{C}$ and to be isomorphic to $PGL(2, q)$. The elements of this so called *projective orthogonal group* are induced by matrices of the form

$$\begin{pmatrix} a^2 & ac & c^2 \\ 2ab & ad+bc & 2cd \\ b^2 & bd & d^2 \end{pmatrix}, ad-bc \neq 0, \tag{1.5}$$

as in [39].

A set of points in a projective plane for which no three points are collinear is called an *arc*. It has been shown (see [14]) that the maximal size of an arc in a plane of order n is $n+1$ if n is odd and $n+2$ if n is even. An *oval* in a plane of order n is defined to be an arc of cardinality $n+1$. A *hyperoval* in a plane of order n

(for n even) is an arc of cardinality $n+2$. We see that every conic in $\pi = PG(2,q)$ is an oval and that, if q is even, a hyperoval is formed by a conic with its knot. The famous theorem of Segre [57] addresses the converse; in doing so, it reflects the essence of linking classical projective geometry with combinatorics. The theorem states that any oval in $PG(2,q)$, for q odd, is necessarily a conic. Thus, for q odd, a combinatorial structure such as an oval may be completely characterized in terms of analytic geometry. One should note that when q is even there are many families of ovals which are not conics, as well as families of hyperovals which are not formed by a conic with its knot (see [21]).

Finally, we will refer to the set of absolute points of a degenerate quadratic form as a *degenerate conic*. A degenerate conic may come in any of three forms: a single point, a single line, or a pair of intersecting lines. These degenerate conics will prove to be important when developing various characterization results in later chapters.

1.4 Unitals

Our primary interest in this thesis concerns another type of algebraic curve. As with conics, we will investigate its combinatorial and geometric properties with hopes of achieving a characterization of the object. In $\pi = PG(2,q^2)$, the classical projective plane of order q^2, a *hermitian curve* is the set of absolute points of a nondegenerate hermitian form. It may be shown that any two hermitian curves are projectively equivalent and thus the associated hermitian matrix may be taken to be the identity matrix. A point (x,y,z) is then absolute if and only if $x^{q+1} + y^{q+1} + z^{q+1} = 0$. Thus we see that every hermitian curve in $PG(2,q^2)$ is projectively equivalent to

$$\mathcal{U} = \{(x,y,z) : x^{q+1} + y^{q+1} + z^{q+1} = 0\}. \tag{1.6}$$

Notice that if δ is the unitary polarity associated with this form, then we have $(x,y,z)^\delta = [x^q, y^q, z^q]$ and $[x,y,z]^\delta = (x^q, y^q, z^q)$. We also point out that the subgroup of $PGL(3,q^2)$ leaving $\mathcal{U}$ invariant is the well-known *projective unitary group*, $PGU(3,q^2)$. It acts two-transitively on points of $\mathcal{U}$ and has order $(q^3+1)q^3(q^2-1)$.

Let us directly count the number of points of π contained in $\mathcal{U}$. If $(x,y,z) \in \mathcal{U}$ with $x = 0$, we find $y^{q+1} + z^{q+1} = 0$. Notice that $y \neq 0$ else $x = y = z = 0$. Thus we may left-normalize and take $y = 1$. This gives $z^{q+1} = -1$, for which there are $q+1$ solutions for z in $F = GF(q^2)$. Therefore, there are $q+1$ points of $\mathcal{U}$ for which $x = 0$. Similarly, there are $q+1$ points of $\mathcal{U}$ for each of the cases when $y = 0$ and $z = 0$. Hence, if $(x,y,z) \in \mathcal{U}$ with all non-zero coordinates, we may take $x = 1$, giving $z^{q+1} = -1 - y^{q+1}$. As $y^{q+1} \neq -1$, we have $-1 - y^{q+1} \in F^* = F \setminus \{0\}$. Thus, for fixed y, there are $q+1$ choices for z. Notice that y^{q+1} can take on $q-2$ values and for fixed y^{q+1} there are $q+1$ choices for y. Therefore, there are $(q-2)(q+1)^2$ points of $\mathcal{U}$ with all non-zero coordinates. The cardinality of $\mathcal{U}$ is seen to be $(q-2)(q+1)^2 + 3(q+1) = q^3+1$.

To see how lines of π meet $\mathcal{U}$, suppose l is an absolute line of the associated hermitian form. Then $l^\delta \in l$, where we note that $l^\delta \in \mathcal{U}$. By way of contradiction, suppose there exists a point $P \neq l^\delta$ belonging to $l \cap \mathcal{U}$. As P is absolute, we have $P \in P^\delta$, giving $P \in P^\delta \cap l$. But $P \in l$ implies $l^\delta \in P^\delta$, thus $l^\delta \in P^\delta \cap l$. As P^δ and l share two distinct points, we must have $P^\delta = l$. Therefore, $P = l^\delta$, a contradiction. Hence every absolute line meets $\mathcal{U}$ in exactly one point. Such lines will be called *tangent*.

Since a line $[x,y,z]$ is absolute if and only if $x^{q+1} + y^{q+1} + z^{q+1} = 0$, we see that $[0,0,1]$ is a nonabsolute line of the hermitian form. We also see that this line contains $q+1$ points of $\mathcal{U}$, namely, the points of the form $(1,y,0)$ such that $y^{q+1} = -1$. By the two-transitivity of $PGU(3,q^2)$ we see that any line containing more than one point of $\mathcal{U}$ must contain exactly $q+1$ points of $\mathcal{U}$. Such lines will be called *secant*. We count

$$\frac{\binom{q^3+1}{2}}{\binom{q+1}{2}} = q^4 - q^3 + q^2$$

distinct secant lines of $\mathcal{U}$. Thus, the $q^4 - q^3 + q^2$ secants and $q^3 + 1$ tangents to $\mathcal{U}$ account for all of the $q^4 + q^2 + 1$ lines of π. They are precisely the nonabsolute and absolute lines of the hermitian form, respectively.

It is here that we see an important example of the interplay between finite geometry and design theory. A t-(v, k, λ)-*design* is an incidence structure consisting of v objects, called *varieties*, and subsets of varieties of cardinality k, called *blocks*, for which any subset of t varieties lies in precisely λ blocks. The *order* n of a t-(v, k, λ)-design is defined to be $n = k - \lambda$. As $\mathcal{U}$ consists of $q^3 + 1$ points and meets every line in 1 or $q + 1$ points, a 2-$(q^3 + 1, q + 1, 1)$ design is obtained by taking the points of $\mathcal{U}$ as varieties and the intersections of nonabsolute lines with $\mathcal{U}$ as blocks. We see that the order of this design is q. Any 2-$(n^3 + 1, n + 1, 1)$ design is called a *unital* of *order* n. We note that the only known unital whose order is not a power of a prime was first found by Mathon [47], in which case $n = 6$. An arbitrary unital of order q embedded in $\pi = PG(2, q^2)$ is often called a *hermitian arc*. Hereafter, we will refer to a hermitian curve, such as $\mathcal{U}$, as a *classical unital*. It should be noted that there exists unitals which are embeddable in nonclassical projective planes, as well as unitals of prime power order q which are not embeddable in any plane of order q^2. In addition to referencing these examples, we will refer to work which demonstrates that the same unital may be embeddable in two non-isomorphic projective planes.

Several combinatorial facts may be easily derived for an arbitrary unital U of order n embedded in any finite projective plane Π of order n^2. Elementary design theory shows that any 2-$(n^3 + 1, n + 1, 1)$ design consists of $n^4 - n^3 + n^2$ blocks and each variety lies in n^2 blocks. Hence, through any point $P \in U$, there pass n^2 lines of Π which are secant to U, leaving a unique tangent to U at P. Suppose a point P is not in U and let t and s denote the number of tangents and secants, respectively, through P. As the lines through P must cover all the points of U, we find that $t + s(n+1) = n^3 + 1$. Since there are $n^2 + 1$ lines of Π through P, we have $t + s = n^2 + 1$. Solving these equations gives $n + 1$ tangent lines through any point $P \notin U$. The corresponding $n + 1$ points of U lying on these tangent lines will be called the *feet* of P. We note that the feet of any point P lying off a classical unital $\mathcal{U}$ are necessarily collinear, as they lie on the image of P under the associated unitary polarity.

In general, there is not a great deal known about unitals embedded in finite projective planes. The classical projective plane has certainly been well studied. As we have seen, the classical unital is embeddable in $PG(2, q^2)$ for every prime power q. In addition, Buekenhout [18] presented two methods for constructing unitals. The first method may be accomplished in any "two-dimensional" translation plane and produces unitals which meet the line at infinity in one point. Such unitals are often called *parabolic*. The second method requires that the translation plane be derivable and produces unitals which meet the line at infinity in $q + 1$ points. These unitals are often called *hyperbolic*. Metz [48] then used Buekenhout's parabolic method to construct a nonclassical unital in $PG(2, q^2)$. These so-called Buekenhout-Metz unitals will be presented in great detail in a subsequent chapter. Barwick [11] has recently shown that any unital obtained from Buekenhout's hyperbolic method in $PG(2, q^2)$ is necessarily a classical unital. We note that every known unital which is embeddable in $PG(2, q^2)$ is obtainable by Buekenhout's construction.

Using a computer, Brouwer [15] has studied unitals on 28 points and the embedding of such unitals in various projective planes of order 9. His findings provide examples of unitals which are not embeddable in any projective plane of order 9, as well as unitals which embed in more than one projective plane. The latter was generalized in the work of Grüning [30], who constructed a unital which embeds in both the Hall and the Dual Hall planes of order q, for every prime power

q. His method used Buekenhout's hyperbolic construction, where we note that the Hall plane is a derivable translation plane.

In [56], Rosati constructed a unital in the Hughes plane of order q, for any odd prime power q. Kestenband [42] generalized this construction to a class of unitals, all of which are projectively equivalent for a given q to Rosati's unital. As the Hughes planes are not translation planes, these unitals do not arise from Buekenhout's construction. Kestenband [42] also showed that the Rosati unital is non-isomorphic, as a design, to the classical unital. The linear automorphism group of this unital was found by Abatangelo and Larato [2]. In addition, they embedded the unital in the derived Hughes plane (Hughes-Rosati plane) and determine its automorphism group, when $q \equiv 3 \pmod 4$. Unitals embedded in the Hughes plane will be analyzed in a subsequent chapter.

Other known unitals may be summarized as follows. A unital arising from a unitary polarity has been found in the Figueroa planes of order q^6, q any odd prime power, by de Resmini and Hamilton [23]. Barlotti and Lunardon [10] have demonstrated the existence of a unital in the Bose-Barlotti Δ-planes. Finally, Lüneberg [46] has exhibited unitals of order $q = 3^{2r+1}$ arising from the Ree groups which are not embeddable in any projective plane of order q^2.

Having the enumeration of unitals embedded in known finite projective planes as an overall motivation, we seek to address two specific issues. The first arises in the setting of the classical projective plane, where we have noted that all known unitals are obtainable from Buekenhout's construction. With hopes of contributing to a future result which declares that all unitals embedded in $PG(2, q^2)$ do indeed arise from Buekenhout construction, we seek to characterize certain properties which force a unital embedded in $PG(2, q^2)$ to be Buekenhout-Metz. To this end, we have been quite successful in characterizing Buekenhout-Metz unitals in terms of the collineation group which leaves the unital invariant. In addition, we have attempted to obtain a geometric characterization of Buekenhout-Metz unitals based on knowledge of the patterns formed by the feet. Although a characterization has not yet been obtained, we have classified these patterns.

The second issue concerns the existence, classification, and characterization of unitals embedded in nonclassical projective planes. To make progress in this undertaking, it is natural to start with projective planes which share many similarities with the classical plane. The Hughes plane is one such plane in which we have made notable accomplishments. Along with several helpful results in interpreting the incidence relation in the Hughes plane, we prove new properties of the only previously known unital embedded in the Hughes plane, the unital attributed to Rosati. Of a more exciting nature, we show that the Rosati unital is a member of a whole family of unitals in the Hughes plane. Moreover, the members of this new family are analogs to certain Buekenhout-Metz unitals in $PG(2, q^2)$, in the same way that the Rosati unital is analgous to the classical unital. Several key properties of these unitals are obtained as well. We assess these contributions more fully and outline the questions which remain unanswered in the Conclusion.

Chapter 2

DESCRIPTION OF BUEKENHOUT-METZ UNITALS

In this chapter, we describe Buekenhout-Metz unitals. Before giving Buekenhout's construction, it is necessary to describe a model for $PG(2, q^2)$ in projective 4-space. Recall that the classical projective plane was defined by taking the one and two-dimensional subspaces of a three-dimensional vector space as the points and lines, respectively. Similarly, one can define *projective n-space over the field F*. Points, lines, planes, and hyperplanes, are defined to be one-dimensional, two-dimensional, three-dimensional, and n-dimensional subspaces, respectively, of a vector space of dimension $n+1$ over F. Of course, we will only concern ourselves with projective spaces over the finite field $F = GF(q)$. Projective spaces, which are so defined, are "classical" in that they are coordinatized by a field. One can synthetically define a projective n-space, but a remarkable result of Veblen and Young [62] states that any projective n-space for $n > 2$ is classical, hence coordinatized by a field. We denote projective n-space over the field $F = GF(q)$ by $PG(n, q)$.

For use throughout this chapter, we now define the analog of a conic in projective n-space. A *quadric* in $PG(n, q)$ is the set of absolute points of a nondegenerate quadratic form defined over the underlying $(n+1)$-dimensional vector space. If the projective dimension n is even, then there is a unique projective equivalence class of nondegenerate quadrics in $PG(n, q)$ (see Section 5.2 of [33]). Such quadrics are known as *parabolic* quadrics. When n is odd, there are two projectively distinct nondegenerate quadrics in $PG(n, q)$ (see Section 5.2 of [33]). They are distinguished by the maximum dimension of the projective subspaces which lie on the quadric. This maximum dimension is either $(n-1)/2$ and the quadric is called *elliptic* or $(n-3)/2$ and the quadric is called *hyperbolic*. One may similarly define the analog of an oval in projective n-space. An *ovoid* is a set of points of $PG(n,q)$, no three of which are collinear, for which the union of all lines "tangent" to a given point on the ovoid forms a hyperplane. It is not difficult to discern that an ovoid consists of $q^{n-1}+1$ points. It is further known that if $PG(n,q)$ contains an ovoid then $n \leq 3$ (see [24]). When $n = 3$, a direct analog of the theorem of Segre holds. It was shown by Barlotti [9] and Pannella [50] that every ovoid in $PG(3,q)$ is necessarily an elliptic quadric, when q is an odd prime power. This result does not hold for even prime powers $q \geq 8$, as demonstrated by the Tits ovoid [60], which is not an elliptic quadric.

2.1 Buekenhout's Construction

We begin our work in projective 3-space. A *spread* of $\Sigma = PG(3,q)$ is any collection of q^2+1 pairwise disjoint lines of Σ. Since Σ has q^3+q^2+q+1 points and each line contains $q+1$ points, the lines of a spread partition the points of Σ. A *regulus* of Σ is a collection of $q+1$ pairwise disjoint lines in Σ such that any line of Σ which meets three lines of the regulus meets all lines of the regulus. The points on the lines of a regulus form a hyperbolic quadric (also known as a *doubly-ruled* quadric) in $PG(3,q)$. It can be shown that any three pairwise disjoint lines of Σ determine a unique regulus containing them. A spread is called *regular* if the regulus determined by any three lines of the spread is entirely contained in the spread. It is well-known that regular spreads exist in $PG(3,q)$ for every prime power q. We note that the notion of a spread may be generalized to higher dimensions. A *t-spread* in $PG(2t+1,q)$ is a collection of $q^{t+1}+1$ pairwise disjoint projective t-spaces which necessarily partition the points of $PG(2t+1,q)$.

We now describe the method of André [5] or Bose [17] for representing translation planes. We give only the simplest version of this representation, as this will be sufficient for our purposes. Let $\Sigma^* = PG(4, q)$, with $\Sigma = PG(3, q)$ viewed as a hyperplane of Σ^*, and let $\mathcal{S}$ be a spread of Σ. We define a new incidence structure, $\pi(\mathcal{S})$, where "points" are the q^4 points of $\Sigma^* \setminus \Sigma$, "lines" are the planes of Σ^* which meet Σ in a line of $\mathcal{S}$, and incidence is set containment. Using the dimension theorem for vector subspaces, one sees that the line of Σ^* determined by any two "points" of $\pi(\mathcal{S})$ must intersect Σ in a point of a line of $\mathcal{S}$. These intersecting lines of Σ^* span a unique "line" of $\pi(\mathcal{S})$. For a "point" P and "line" l of $\pi(\mathcal{S})$, with $P \notin l$, we see that the span of P and the spread line of S associated with l is a "line" of $\pi(\mathcal{S})$. This "line" contains P but shares no "points" of $\pi(\mathcal{S})$ with l. Thus $\pi(\mathcal{S})$ is an affine plane of order q^2. One may complete $\pi(\mathcal{S})$ to a projective plane $\Pi(\mathcal{S})$ by adding the lines of $\mathcal{S}$ as "points" at infinity and $\mathcal{S}$ as the "line" at infinity. It can be shown that $\pi(\mathcal{S})$ (and $\Pi(\mathcal{S})$) is a translation plane. Moreover, $\Pi(\mathcal{S})$ is classical if and only if $\mathcal{S}$ is a regular spread [17]. In the general situation, one constructs translation planes from t-spreads of $PG(2t + 1, q)$ embedded in $PG(2t + 2, q)$. It turns out (see [17]) that every finite translation plane arises from a t-spread for some appropriate t. The translation planes arising from nonregular spreads of $PG(3, q)$ are called *two-dimensional*. These planes may be coordinatized by algebraic structures called quasifields which are two-dimensional over their kernels (see [31, 32]).

Let $\Pi = \Pi(\mathcal{S})$, as in the above two-dimensional case. Buekenhout's method of obtaining a parabolic unital in Π starts with a three-dimensional ovoid $\mathcal{O}$ which meets Σ in a single point P. Let Q be any point, other than P, of the unique spread line of $\mathcal{S}$ containing P. The *cone* Λ over $\mathcal{O}$ with vertex Q is the union of the *ruling* lines joining Q to the points of $\mathcal{O}$. Buekenhout [18] showed that Λ corresponds to a unital in Π. We proceed to outline the proof that this construction does indeed yield a unital when Π is classical and $\mathcal{O}$ is an elliptic quadric.

Suppose $\mathcal{S}$ is regular, hence $\Pi(\mathcal{S})$ is $\pi = PG(2,q^2)$. Suppose $\mathcal{O}$ is an elliptic quadric contained in a copy of $PG(3,q)$, denoted by Σ_0, such that $\mathcal{O} \cap \Sigma = \{P\}$. Suppose Λ is formed as above and let U denote the set of points of π which correspond to Λ. We first note that Λ is the union of q^2+1 distinct lines of Σ^* through Q, since any line through Q which contains more than one point of $\mathcal{O}$ would necessarily lie in Σ_0. Thus U consists of q^3+1 "points" of π, where we note that the spread line PQ corresponds to one "point" at infinity in π. We denote this special "point" by P_∞. One may count q^2 planes of Σ^* which pass through the spread line PQ and do not lie in Σ. That is, each plane is the span of PQ with another ruling line of Λ. As such planes may contain only one ruling line other than PQ, these planes meet Λ in exactly the $q+1$ points of that ruling line. Thus every "line" of π through P_∞ meets U in $q+1$ "points", with the exception of the "line" at infinity which meets U in the single "point" P_∞.

Let π' be a plane of Σ^*, not in Σ, which meets Σ in a spread line l' of $\mathcal{S}$ other than PQ, i.e., π' determines a "line" of $PG(2,q^2)$ which does not contain P_∞. Let Σ' be the three-space spanned by π' and Q. Now Σ' either meets Λ in a quadratic cone with vertex Q (i.e., the union of all lines joining Q to the points of a conic) or in a ruling line of Λ. The latter choice for Σ' is called a "tangent" hyperplane to Λ and it is uniquely determined by l'. In this case, π' meets Λ in a single point; hence, π' corresponds to a tangent "line" of U in $PG(2,q^2)$. If $\Sigma' \cap \Lambda$ is a quadratic cone, then $\pi' \cap \Lambda$ is a conic, as π' does not pass through Q. Hence, $\pi' \cap \Lambda$ has cardinality $q+1$, which shows that π' corresponds to a secant "line" of U in $PG(2,q^2)$. Therefore, it has been shown that U is a 2-$(q^3+1, q+1, 1)$ design, i.e. a unital.

Metz showed that one may construct a nonclassical unital in $PG(2,q^2)$, for any $q > 2$, by choosing an appropriate elliptic quadric $\mathcal{O}$. Thus we define a *Buekenhout-Metz unital* (or *BM-unital*, for brevity) to be a parabolic unital in $PG(2,q^2)$ obtained via Buekenhout's construction when $\mathcal{O}$ is any elliptic quadric.

When q is odd, it has been noted that every ovoid is an elliptic quadric. For q even, we note that Buekenhout's construction yields a nonclassical unital when $\mathcal{O}$ is a Tits ovoid. This unital, however, will not be considered a BM-unital. It should also be noted that the classical unital is considered a BM-unital, since one may obtain the classical unital by an appropriate choice of an elliptic quadric (for q even or odd).

Buekenhout's hyperbolic method for constructing unitals requires that the spread $\mathcal{S}$ associated with the translation plane $\Pi(\mathcal{S})$ contain a regulus. A unital is then obtained from a four-dimensional nondegenerate quadric surface in Σ^* which meets Σ in a doubly-ruled (hyperbolic) quadric, for which the lines of the required regulus are one family of ruling lines. We again note that Barwick [11] has recently shown that any unital of $PG(2, q^2)$ obtained from this construction is a classical unital.

2.2 Contributions of Baker and Ebert to the study of BM-unitals

This section is based on the findings of Baker and Ebert [8], for the case when q is odd, and Ebert [26], when q is even. The reader should assume that the results may be found in these sources unless otherwise stated.

We establish homogeneous coordinates for $\Sigma^* = PG(4, q)$ using vectors of the form (x_1, x_2, y_1, y_2, z), for $x_1, x_2, y_1, y_2, z \in K = GF(q)$, where $z = 0$ is the equation of the hyperplane Σ at infinity. Let (x, y, z), $x, y, z \in F = GF(q^2)$, denote homogeneous coordinates for $\pi = PG(2, q^2)$ where $z = 0$ is the equation of the line at infinity. Throughout this chapter, we will normalize point coordinates from the right. Thus normalized representatives for points of π will have their z-coordinate in the subfield K. By picking $\epsilon \in F \setminus K$ and considering $\{1, \epsilon\}$ as a basis for F over K, we may identify $x = x_1 + x_2\epsilon$ and $y = y_1 + y_2\epsilon$. For q odd, we prefer to select

$$\epsilon = \gamma^{(q+1)/2} \tag{2.1}$$

where γ is a primitive element of F. We see then that $\omega = \epsilon^2$ is a primitive element of the subfield K. If q is even, we choose ϵ to be a root of an irreducible polynomial

$$x^2 + x + \sigma \tag{2.2}$$

for some σ in K. In this case, $\epsilon^q = 1+\epsilon$ and $\epsilon^{q+1} = \sigma$. Throughout this document we will often refer to the "real" and "imaginary" parts of an element $x \in F$, meaning those elements x_1 and $x_2 \in K$, respectively, for which $x = x_1 + x_2\epsilon$.

In Section 17.7 of Hirschfeld [34], it is shown that every BM-unital is equivalent to one whose ovoidal cone is represented by the equation $f(x_1, x_2) + y_2 z = 0$, where f is an irreducible binary form. In this representation, $y_1 = 0$ is the equation of the hyperplane Σ_0 containing the ovoid $\mathcal{O}$, and the vertex Q of the cone has coordinates $(0, 0, 1, 0, 0)$. In [8] and [26], the points of a BM-unital are described explicitly in $\pi = PG(2, q^2)$. The authors show that every BM-unital, for $q \geq 3$, may be written as

$$U_{a,b} = \{(x, ax^2 + bx^{q+1} + r, 1) : x \in F, r \in K\} \cup \{(0, 1, 0)\} \tag{2.3}$$

subject to certain conditions on $a, b \in F$. Let $a = a_1 + a_2\epsilon$ and $b = b_1 + b_2\epsilon$ for $a_1, a_2, b_1, b_2 \in K$. For q odd, one may check that Hirschfeld's form f is then given by

$$-f(x_1, x_2) = a_2(x_1^2 + \omega x_2^2) + b_2(x_1^2 - \omega x_2^2) + 2a_1x_1x_2 \tag{2.4}$$

and that f is irreducible if and only if

$$(b^q - b)^2 + 4a^{q+1} \in K_N. \tag{2.5}$$

For the case when $q = 2^n \geq 4$ we first define the *trace* function of $GF(q)$ over $GF(2)$ by $tr : GF(q) \to GF(2)$ via $x \mapsto x + x^2 + x^4 + \ldots + x^{2^{n-1}}$. We then define $\mathcal{C}_0$ to be $\{x \in GF(q) : tr(x) = 0\}$. For q even, we find that in Hirschfeld's notation

$$f(x_1, x_2) = (a_2 + b_2)x_1^2 + b_2x_1x_2 + (a_1 + a_2 + a_2\sigma + b_2\sigma)x_2^2. \tag{2.6}$$

Lemma 2 of [26] demonstrates that f is irreducible if and only if $a^{q+1}/(b^q+b)^2 \in \mathcal{C}_0$. As $b^q + b = b_2$, we see that $b_2 \neq 0$ and hence $b \notin K = GF(q)$, when q is even.

We note that $U_{a,b}$ is a classical unital if and only if $a = 0$. It is easy to see that in this case $U_{a,b}$ consists of the set of absolute points of the hermitian form $(b^q - b)x^{q+1} + yz^q - y^q z$. When q is odd and $b \in K$ (hence $a \neq 0$), $U_{a,b}$ consists of a partial pencil of q conics, all of which pass through the point $P_\infty = (0,1,0)$. Moreover, Theorem 3 of [8] states that $U_{a,b}$ contains a conic of π if and only if $b \in K$ (i.e. $b^q - b = 0$) and in that case every conic must pass through P_∞, where q is necessarily odd. When q is even, Theorem 3 of [26] shows that no BM-unital contains an oval of π. The Buekenhout-Metz unitals which arise as unions of conics have been studied in [7] and [36], as well.

The collineation groups leaving $U_{a,b}$ invariant have also been determined in [8] and [26]. We state these important results here.

Theorem 2.2.1 *Let U be a nonclassical Buekenhout-Metz unital embedded in $PG(2,q^2)$. Let $G = \mathrm{Aut}(U) \cap PGL(3,q^2)$ be the full linear collineation group stabilizing U. Then G is a semidirect product $S \rtimes \mathbf{Z}_t$, where $S \in \mathrm{Syl}_p(G)$ has order q^3 and $\mathbf{Z}_t$ is a cyclic group of order*

$$t = \begin{cases} 2(q-1) \\ q-1 \end{cases}.$$

The first case for $\mathbf{Z}_t$ occurs if and only if q is odd and U can be expressed as a partial pencil of q conics in $PG(2,q^2)$. Moreover, S is abelian if and only if $t = 2(q-1)$. ■

Theorem 2.2.2 *Let $U_{a,b}$ be a nonclassical Buekenhout-Metz unital and let $G = \mathrm{Aut}(U) \cap PGL(3,q^2)$ as in Theorem 2.2.1. Then G fixes some point P_∞ of U and acts transitively on $U \setminus \{P_\infty\}$ as well as $l_\infty \setminus P_\infty$. G acts transitively on the points of $PG(2,q^2) \setminus (U \cup l_\infty)$ when q is even and when $b \in GF(q)$ for q odd. Otherwise, G has two orbits on the points of $PG(2,q^2) \setminus (U \cup l_\infty)$.* ■

When q is odd and $-(b^q - b)^2/a^{q+1}$ is a nonsquare in some subfield of K, the orbits of $PG(2,q^2)\backslash(U \cup l_\infty)$ mentioned in Theorem 2.2.2 are fused by a semilinear map which leaves $U_{a,b}$ invariant [8]. That is to say, the full collineation group stabilizing such a unital (the stabilizer of the unital in $P\Gamma L(3,q)$) acts transitively on $PG(2,q^2) \setminus (U \cup l_\infty)$. For the classical unital $\mathcal{U} = U_{0,b}$, let G denote the stabilizer of the point P_∞ in $\mathrm{Aut}(\mathcal{U}) \cap PGL(3,q^2)$ (see Section 1.4, page 13). Then G is the semidirect product $S \rtimes \mathbf{Z}_t$, as in Theorem 2.2.1 above, with $t = q^2 - 1$. The orbits of G acting on $\pi = PG(2,q^2)$ are $\{P_\infty\}$, $\mathcal{U} \setminus \{P_\infty\}$, $l_\infty \setminus \{P_\infty\}$, $\pi \setminus (\mathcal{U} \cup l_\infty)$. One should recall that the full linear collineation group stabilizing the classical unital is, in fact, 2-transitive on the points of the unital.

The question of projective equivalence among the $U_{a,b}$'s has also been answered in [8] and [26]. The authors show that $U_{a',b'}$ is projectively equivalent to $U_{a,b}$ if and only if $a' = a^\theta s^2 e$ and $b' = b^\theta s^{q+1} e + g$ for $e \in K^*, g \in K, s \in F^*$, and $\theta \in \mathrm{Aut}(F)$. We point out that the classical unital ($a = 0$) forms one equivalence class. Additionally, when q is odd, we see that there is a unique equivalence class which contains the unitals formed from partial pencils of conics, i.e., for which $b \in GF(q)$. The number of equivalence classes is counted by the following theorem (see [8, 26]).

Theorem 2.2.3 *Let $q = p^n \geq 3$. Then the number of projectively inequivalent Buekenhout-Metz unitals of order q is*

$$\frac{1}{2n}\left[n_0 + \sum_{m|n} \phi\left(\frac{2n}{m}\right) p^m\right],$$

where ϕ is the Euler phi-function and $n_0 = 0$, if $p = 2$, and n_0 is the odd part of n, if $p > 2$. ∎

When q is an odd prime, one obtains $(q+1)/2$ projectively inequivalent BM-unitals in $PG(2,q^2)$ [8]. If $q = 2^p$ for some odd prime p, then the number of projectively inequivalent BM-unitals of order q is $1 + (2^{p-1} - 1)/p$ [26].

2.3 Classification of the Feet of BM-unitals

In the concluding paragraph of [8], it is commented that gaining knowledge of the feet (see Section 1.4, page 15) of points exterior to a Buekenhout-Metz unital "is an important first step toward understanding the embeddability" of BM-unitals in nonclassical translation planes. Without addressing the embeddability issue, we will now describe the configurations formed by the feet of a point lying off a BM-unital. An ultimate goal would be to characterize BM-unitals in terms of the possible configuration patterns assumed by the feet of a unital embedded in $\pi = PG(2, q^2)$. While unable to provide such a characterization at this time, we will state a conjecture regarding this matter.

In Section 1.4, it was shown that the feet of each point lying off a classical unital are collinear. Suppose $U_{a,b}$ is any nonclassical BM-unital. We first demonstrate that the feet of any point on $l_\infty \setminus \{P_\infty\}$ are collinear. First note that l_∞ has line coordinates $[0, 0, 1]$. By Theorem 2.2.2, the automorphism group of $U_{a,b}$ is transitive on $l_\infty \setminus \{P_\infty\}$, hence we need only examine the feet of the point $Q = (1, 0, 0) \in l_\infty \setminus \{P_\infty\}$. Notice that $P_\infty = (0, 1, 0)$ is one of the feet of Q. Also consider the points $(0, s, 1) \in U_{a,b}$, for $s \in K = GF(q)$, which lie on the lines $[0, 1, -s]$, respectively, passing through Q. To see that lines of the form $[0, 1, -s]$, for $s \in K$, are tangent to $U_{a,b}$, note that an affine point $(x, ax^2 + bx^{q+1} + r, 1) \in U_{a,b}$, $x \in F$, $r \in K$, lies on such a line if and only if $ax^2 + bx^{q+1} \in K$. But the "imaginary" part of $ax^2 + bx^{q+1}$ is given by $f(x_1, x_2)$ as in (2.4) or (2.6), depending on q, hence this is equivalent to having $f(x_1, x_2) = 0$. As f is irreducible, we find that $x = 0$ and the lines are indeed tangent. Thus the feet of Q are $\{(0, 1, 0)\} \cup \{(0, s, 1) : s \in K\}$ which all lie on the line $[1, 0, 0]$.

In order to determine the set of feet for points of the set $T = \pi \setminus (U_{a,b} \cup l_\infty)$, we recall from Theorem 2.2.2 that there are either one or two orbits under G for such points. Until further notice, we restrict our consideration to the case when

q is odd. From the proof of Theorem 2.2.2 given in [8], we see that the points $(0, \epsilon, 1), (0, \omega\epsilon, 1) \in T$ lie in different orbits of G when $a \neq 0$ and $b \notin K$. Thus it suffices to describe the pattern of the feet for these representatives of each orbit. We explicitly determine only the feet of the point $(0, \epsilon, 1)$, as the computations for the feet of $(0, \omega\epsilon, 1)$ (when necessary) may be accomplished in a completely similar manner.

First, notice that the lines of π passing through $P = (0, \epsilon, 1)$ are $[1, 0, 0]$ and $[c, 1, -\epsilon]$, for $c \in F$, and that $[1, 0, 0]$ is secant to $U_{a,b}$. As shown in Corollary 2 of Theorem 2 of [8], the unique tangent line to $U_{a,b}$ at the point $(x, ax^2 + bx^{q+1} + r, 1)$ may be represented by line coordinates $[-2ax + (b^q - b)x^q, 1, ax^2 - b^q x^{q+1} - r]$. Comparing these "center-normalized" representatives for lines, we see that a point $(x, ax^2 + bx^{q+1} + r, 1) \in U_{a,b}$ lies on a tangent line through P if and only if

$$ax^2 - b^q x^{q+1} - r = -\epsilon. \tag{2.7}$$

Thus the feet of P have the form

$$(x, 2ax^2 - (b^q - b)x^{q+1} + \epsilon, 1), \tag{2.8}$$

where we have reexpressed $ax^2 + bx^{q+1} + r$ using (2.7). By raising (2.7) to the qth power and subtracting (2.7) from this, we see that

$$a^q x^{2q} + (b^q - b)x^{q+1} - ax^2 - 2\epsilon = 0 \tag{2.9}$$

must also be satisfied. Therefore, the feet of P are precisely those points of the form given in (2.8) for which x satisfies (2.9).

Although it has been shown previously, we have here an immediate proof that the feet of a classical unital of odd order are collinear. Namely, when $a = 0$, we see that the feet of P have the form $(x, -\epsilon, 1)$, where $x^{q+1} = 2\epsilon/(b^q - b)$, and all lie on the line $[0, 1, \epsilon]$. When $b \in K$ (the union of conics case), we see that the feet of P have the form $(x, 2ax^2 + \epsilon, 1)$ where $a^q x^{2q} - ax^2 - 2\epsilon = 0$. Thus the feet are absolute points of the quadratic form $2ax^2 - yz + \epsilon z^2 = 0$. The symmetric bilinear form associated with this quadratic form is represented by the matrix

$$\begin{pmatrix} 2a & 0 & 0 \\ 0 & 0 & -\frac{1}{2} \\ 0 & -\frac{1}{2} & \epsilon \end{pmatrix},$$

which has nonzero determinant (as $a \neq 0$). Therefore, the feet of P lie on a conic of π determined by this nondegenerate quadratic form. That is to say, in the union of conics case, the feet form an arc of cardinality $q+1$ which is a subset of a conic (of cardinality q^2+1). Through extensive computer search of each equivalence class of BM-unitals for every odd prime power less than 100, it has been observed that this arc does not form a subconic in π. (We define a *subconic* to be the intersection of a conic of π with a subplane of π of order q.)

We now proceed to describe the feet of P for $U_{a,b}$ when $a \neq 0$ and $b \notin K$ and q is odd. We first show that (2.9) has exactly $q+1$ solutions for $x \in F$. By writing $x = x_1 + x_2\epsilon$, $a = a_1 + a_2\epsilon$, $b = b_1 + b_2\epsilon$, for $x_1, x_2, a_1, a_2, b_1, b_2 \in K$, (2.9) may be expanded to give

$$(a_2 + b_2)x_1^2 + (a_2 - b_2)\omega x_2^2 + 2a_1x_1x_2 + 1 = 0. \tag{2.10}$$

We may view this as a quadratic form defined on the points of a copy of $PG(2,q)$ with homogeneous coordinates (x_0, x_1, x_2), where $x_0 = 1$ for affine points, i.e.,

$$Q(x_0, x_1, x_2) = (a_2 + b_2)x_1^2 + (a_2 - b_2)\omega x_2^2 + 2a_1x_1x_2 + x_0^2. \tag{2.11}$$

Notice that every absolute point $(1, x_1, x_2)$ of Q may be identified with a solution $x = x_1 + x_2\epsilon$ of (2.9) and vice-versa. The matrix representing the symmetric bilinear form corresponding to Q is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & a_2 + b_2 & a_1 \\ 0 & a_1 & (a_2 - b_2)\omega \end{pmatrix}$$

which has determinant $(a_2^2 - b_2^2)\omega - a_1^2 = -d/4$, where $d = (b^q - b)^2 - 4a^{q+1} \in K_N$ from (2.5). As the determinant is nonzero, Q is nondegenerate. Therefore, there are $q+1$ absolute points to Q (i.e., a conic of $PG(2,q)$), which correspond to $q+1$ solutions to (2.9). One must remember that the copy of $PG(2,q)$ used here is not a subplane of $\pi = PG(2,q^2)$. It is simply an aid in counting the number of solutions to an equation.

The following proposition demonstrates that the feet of P form a $\{0,1,2,4\}$-set, when $a \neq 0$ and $b \notin K$. That is to say, every line of π contains either zero, one, two, or four feet of P.

Proposition 2.3.1 *Let $U_{a,b}$ be a nonclassical BM-unital of odd order. Any line of π which contains more than two feet of $P = (0,\epsilon,1)$ must contain exactly four feet of P.*

Proof: We first note that $l_\infty = [0,0,1]$ contains no feet of P. Also, it is clear that any line of the form $[1,0,g]$, $g \in F$, may contain only one of the feet (as given by (2.8)) of P, since $x + g = 0$ uniquely determines x. Therefore, any line containing more than two feet of P must have the form $[e,1,g]$, $e,g \in F$. The number of feet lying on such a line will correspond to the number of simultaneous solutions for x of (2.9) and

$$ex + 2ax^2 - (b^q - b)x^{q+1} + \epsilon + g = 0, \qquad (2.12)$$

which one obtains from the inner product of $[e,1,f]$ with (2.8). Separating (2.12) into real and imaginary parts, in terms of the basis $\{1,\epsilon\}$, one obtains

$$e_1x_1 + e_2\omega x_2 + 2a_1(x_1^2 + \omega x_2^2) + 4a_2\omega x_1x_2 + g_1 = 0 \qquad (2.13)$$

and

$$e_2x_1 + e_1x_2 + 2a_2(x_1^2 + \omega x_2^2) + 4a_1x_1x_2 + 2b_2(x_1^2 - \omega x_2^2) + 1 + g_2 = 0, \qquad (2.14)$$

respectively. As the x corresponding to each of the feet of P must also satisfy (2.10), we may write (2.14) as

$$e_2x_1 + e_1x_2 - 1 + g_2 = 0. \tag{2.15}$$

We seek simultaneous solutions to (2.13), (2.15), and (2.10), by considering the curves they describe in some copy of $PG(2,q)$ with affine points given by $(1, x_1, x_2)$. We have seen previously that (2.10) is the equation of a nondegenerate conic in $PG(2,q)$. As (2.15) is the equation of a line of $PG(2,q)$, we see that there are at most two simultaneous solutions to (2.10) and (2.15), since a line can meet a conic in at most two points. Thus (2.15) must be identically zero, because our assumption is that $[e, 1, g]$ contains more than two feet. This gives $e_1 = e_2 = 0$ and $g_2 = 1$. Thus any line containing more than two feet of P must have the form $[0, 1, g_1 + \epsilon]$. Hence, (2.13) has the form

$$2a_1(x_1^2 + \omega x_2^2) + 4a_2\omega x_1x_2 + g_1 = 0 \tag{2.16}$$

It remains to determine how the (affine) conics given by (2.10) and (2.16) meet in $PG(2,q)$. If the same locus of $q+1$ points satisfy these equations, then one of these equations is identically zero or one of the quadratic forms is a scalar multiple of the other. (Note that (2.10) is not identically zero.) Suppose (2.16) is a λ-multiple of (2.10), for some $\lambda \in K^*$. Comparing the x_1^2 and x_2^2 terms gives $2a_1 = \lambda(a_2 + b_2)$ and $2a_1 = \lambda(a_2 - b_2)$, respectively. By subtracting these, we find $b_2 = 0$, as $\lambda \neq 0$. But this implies $b^q - b = 0$, which contradicts the assumption that (2.12) has more than two solutions for x. Therefore, (2.16) is identically zero, giving $a_1 = a_2 = 0$. As this contradicts the assumption that $U_{a,b}$ is a nonclassical BM-unital, it must be that (2.10) and (2.16) correspond to distinct conics of $PG(2,q)$. Now, any two distinct conics can meet in at most four points, even if one of them is degenerate (which (2.16) will be precisely when $g_1 = 0$). Furthermore, we see that if $x = x_1 + x_2\epsilon$ corresponds to a simultaneous solution of (2.10) and (2.16), then $-x$ does as well. As $x = 0$ is not such a solution, the number of solutions must be even.

Therefore, there are exactly four solutions to (2.10) and (2.16), which correspond precisely to the feet of P lying on the line $[e, 1, g]$. ■

We summarize our results in the following corollary.

Corollary 2.3.2 *Let $U_{a,b}$ be a nonclassical Buekenhout-Metz unital of odd order. Then, the feet of a point $P \in l_\infty \setminus \{P_\infty\}$ are collinear. The feet of a point $P \notin \pi \setminus (U_{a,b} \cup l_\infty)$ form a $\{0, 1, 2, 4\}$-set. In the special case when $b \in K = GF(q)$, the feet of P form a $(q + 1)$-arc.*

■

The author has studied the patterns formed by the feet of $(0, \epsilon, 1)$ and $(0, \omega\epsilon, 1)$ for all equivalence classes of BM-unitals for every odd prime power $q < 100$, using the software package MAGMA developed at the University of Sydney. It has been observed that there are a variety of possibilities for the configuration which has been described as a $\{0, 1, 2, 4\}$-set. In some instances, the feet actually form a $(q + 1)$-arc, but no example has been seen for which this arc is a subset of a conic when $b \notin K$. If $b \notin K$ then, up to projective equivalence, one may choose $U_{a,b}$ in such a way that b is a primitive element γ of F. We conjecture that the feet of a nonclassical unital $U_{a,b}$, with $b = \gamma$, form an arc if and only if a is a nonsquare of F. Moreover, there is evidence to suggest that such unitals correspond to the case described in [8] for which $-(b^q - b)^2/a^{q+1}$ is a nonsquare in some subfield of K, when $q \equiv 3 \pmod 4$.

From the proof of Proposition 2.3.1, any line of π which contains more than two feet of $P = (0, 1, \epsilon)$ must have the form $[0, 1, g_1 + \epsilon]$, $g_1 \in K$. An analgous result shows that any line containing more than two feet of $P' = (0, 1, \omega\epsilon)$ must have the form $[0, 1, g_1 + \omega\epsilon]$, $g_1 \in K$. Thus, we will only consider these "special" lines through the point $(1, 0, 0) \in l_\infty$ when investigating the intersections of lines with the sets of feet. (Recall that in the classical case it was seen that the feet of $(0, 1, \epsilon)$ are collinear on a line through $(1, 0, 0)$.)

While unable to prove general theorems at this time, there is ample evidence to support the following statements. Consider a BM-unital $U_{a,b}$ with P, P', and "special" lines defined as in the preceding paragraph. When $q \equiv 3 \pmod 4$ and $a \in F_S$, the "special" lines contain zero or four feet of either P or P', while meeting the set of feet of the other in zero, two, or four feet. More specifically, if the "special" lines contain only zero or four points of a set of feet, then the $q+1$ feet are partitioned by the $(q+1)/4$ "special" lines which meet the set in four feet. If the "special" lines meet a set of feet in zero, two, or four points, then all but four of the feet are partitioned by the $(q-3)/4$ "special" lines which meet the set in four feet. The remaining four feet are partitioned by the two "special" lines which meet the set in two feet. When $q \equiv 1 \pmod 4$ and $a \in F_S$, the sets of feet are always partitioned by the $(q-1)/4$ "special" lines which meet the set in four feet and the unique "special" line which meets the set in two feet.

We now turn our attention to the case when q is even. From Theorem 2.2.1, G acts transitively on $T = \pi \setminus (U_{a,b} \cup l_\infty)$ when $a \neq 0$. We choose $(0, \epsilon, 1)$ as the representative of T whose feet we will describe. Each step is identical to the case when q is odd, with appropriate adjustments for fields of characteristic two. We see that lines through $P = (0, \epsilon, 1)$ are $[1, 0, 0]$ and $[c, 1, \epsilon]$, for $c \in F$, and once again $[1, 0, 0]$ is secant to $U_{a,b}$. In Corollary 6 of [26], it was shown that the unique tangent line to $U_{a,b}$ at the point $(x, ax^2 + bx^{q+1} + r, 1)$ may be represented by the vector $[(b^q + b)x^q, 1, ax^2 + b^q x^{q+1} + r]$. Comparing these lines one sees that $(x, ax^2 + bx^{q+1} + r, 1) \in U_{a,b}$ lies on a tangent line through P if and only if

$$ax^2 + b^q x^{q+1} + r = \epsilon. \tag{2.17}$$

Thus, the feet of P must have the form

$$(x, (b^q + b)x^{q+1} + \epsilon, 1). \tag{2.18}$$

By raising (2.17) to the qth power, one obtains $a^q x^{2q} + bx^{q+1} + r = \epsilon + 1$, which when added to (2.17) gives

$$a^q x^{2q} + (b^q + b)x^{q+1} + ax^2 + 1 = 0. \tag{2.19}$$

Therefore, the feet of P are precisely those points of the form given in (2.18) for which x satisfies (2.19).

To see that (2.19) has exactly $q+1$ solutions for x, we expand the equation via the basis $\{1, \epsilon\}$ to obtain

$$(a_2 + b_2)x_1^2 + (a_1 + a_2 + (a_2 + b_2)\sigma)x_2^2 + b_2 x_1 x_2 + 1 = 0. \tag{2.20}$$

As before, we view this as a quadratic form Q defined on the points of a copy of $PG(2,q)$. For points $u = (u_0, u_1, u_2)$ and $v = (v_0, v_1, v_2)$, the symmetric bilinear form associated with Q is

$$s(u,v) = Q(u+v) + Q(u) + Q(v) = b_2(u_1 v_2 + u_2 v_1). \tag{2.21}$$

We see that if v is in the radical with respect to s, then $b_2(u_1v_2 + u_2v_1) = 0$ for all $u_1, u_2 \in K$, where we note that $b_2 \neq 0$. This gives $v_1 = v_2 = 0$ and $v = (0,0,1)$. Finally, $Q(0,0,1) = 1$, hence Q is nondegenerate. Therefore, Q defines a conic in $PG(2,q)$, giving $q+1$ solutions to (2.19).

When $a \neq 0$, we show that the feet of P form a $(q+1)$-arc.

Proposition 2.3.3 *Let $U_{a,b}$ be a nonclassical BM-unital of even order. Any line of π contains at most two feet of $P = (0, \epsilon, 1)$.*

Proof: Suppose by way of contradiction that some line of $\pi = PG(2, q^2)$ contains more than two feet of P. As in Proposition 2.3.1, this line must have the form $[e, 1, g]$, for $e, g \in F$. Using $b_2 = b^q + b$, we see that the number of feet lying on such a line will correspond to the number of simultaneous solutions of (2.19) and

$$ex + b_2 x^{q+1} + \epsilon + g = 0. \tag{2.22}$$

With the identities $\epsilon^q = 1 + \epsilon$, $\epsilon^{q+1} = \sigma$, and $\epsilon^2 = \epsilon + \sigma$, (2.22) may be expanded into real and imaginary parts to obtain

$$e_1 x_1 + e_2 \sigma x_2 + b_2(x_1^2 + x_1 x_2 + \sigma x_2^2) + g_1 = 0 \tag{2.23}$$

and

$$e_2 x_1 + e_1 x_2 + 1 + g_2 = 0, \tag{2.24}$$

respectively. As we seek simultaneous solutions to (2.20), (2.23), and (2.24), we notice that the line given by (2.24) and the nondegenerate conic given by (2.20) can meet in at most two points of $PG(2, q)$. Thus (2.24) must be identically zero, i.e., $e_1 = e_2 = 0$ and $g_2 = 1$. This gives (2.23) the form

$$b_2(x_1^2 + x_1 x_2 + \sigma x_2^2) + g_1 = 0. \tag{2.25}$$

Using this fact in (2.20) gives

$$a_2 x_1^2 + (a_1 + a_2 + a_2\sigma)x_2^2 + 1 + g_1 = 0 \tag{2.26}$$

which is a degenerate quadratic form whose absolute points are those of the line in $PG(2, q)$ with equation $\sqrt{a_1}x_1 + \sqrt{a_1 + a_2(1+\sigma)}x_2 + \sqrt{1 + g_1} = 0$. (Recall that every element of F may be written as a square, since F has even characteristic.) If (2.20) and (2.26) share the same locus of $q + 1$ points, then (2.26) must be identically zero since the conic determined by (2.20) is nondegenerate. This would give $a_1 = a_2 = 0$. As $a \neq 0$ for nonclassical BM-unitals, we see that the line of (2.26) and the conic of (2.20) can meet in at most two points. Thus the line $[e, 1, g]$ of π can contain at most two feet of P, our final contradiction. ■

Computer-generated data appear to indicate that the $(q + 1)$-arc formed by these feet is not a subset of a conic of π.

The following corollary summarizes the results when q is even.

Corollary 2.3.4 *Let $U_{a,b}$ be a nonclassical Buekenhout-Metz unital of even order. Then, the feet of a point $P \in l_\infty \setminus \{P_\infty\}$ are collinear. The feet of a point $P \notin \pi \setminus (U_{a,b} \cup l_\infty)$ form a $(q + 1)$-arc.*

Thas [59] has shown that a unital U in $\pi = PG(2, q^2)$ is classical if and only if the feet of every point off U are collinear. It seems reasonable to make the following conjecture which, if true, would provide a characterization of Buekenhout-Metz unitals in terms of the feet.

Let U be a unital embedded in $PG(2, q^2)$ having a special point P_∞, with l_∞ the tangent line at the point P_∞. Suppose

(i) the feet of any point on $l_\infty \setminus \{P_\infty\}$ are collinear, and

(ii) the feet of any point off $U \cup l_\infty$ are collinear or form a $\{0, 1, 2, 4\}$-set.

Then U is a Buekenhout-Metz unital.

The next chapter will discuss in detail various characterizations of Buekenhout-Metz unitals, as well as the classical unital.

Chapter 3

A GROUP THEORETIC CHARACTERIZATION OF BUEKENHOUT-METZ UNITALS

3.1 Characterizations of Unitals Embedded in $PG(2, q^2)$

As one studies the properties of a particular configuration, such as a unital, the immediate question is to ask which of these properties are unique to that configuration. In other words, given an arbitrary unital, what list of properties is needed to declare that the unital is of a certain type? As with most configurations embedded in a finite projective plane, one may characterize unitals by a variety of criteria. Known characterizations have focused on geometric and combinatorial properties, as well as the collineation group which leaves the unital invariant. We attempt to record most known characterizations of classical and Buekenhout-Metz unitals in $\pi = PG(2, q^2)$.

As the classical unital has been long and well-studied, a rich variety of characterizations exist, many of which represent recent work. Thas [59] has provided a combinatorial characterization for unitals embedded in π based on the feet being collinear, as was noted in the previous chapter. A unital U in π is called *reciprocal* if for any four points $P_1, P_2, P_3, P_4 \in U$, with no three collinear and with tangents l_1, l_2, l_3, l_4, respectively, $l_1 \cap l_2 \in P_3P_4$ implies $l_3 \cap l_4 \in P_1P_2$. Tallini-Scafati (see [33]) has shown that a reciprocal unital embedded in $PG(2, q^2)$ must be classical. Piper [52] has conjectured that a unital which contains no O'Nan configurations (four blocks for which any two blocks meet in a unique point and any three blocks have empty intersection) must necessarily be classical. Wilbrink [63] showed that a unital with no O'Nan configurations which satisfies certain other geometric conditions must be a classical unital.

More geometrically, it was shown independently by Lefèvre-Percsy [45] and Faina and Korchmáros [27] that a unital embedded in π is classical if each secant line of π meets the unital in a Baer subline. We note that a *Baer subline* is defined to be the nontrivial intersection of a line of π with some subplane of order q embedded in π. Hirschfeld, Storme, Thas, and Voloch [35] have shown that any algebraic curve of degree $q+1$ in π, $q>2$, without linear components, and which contains at least q^3+1 points, must be a classical unital.

If a unital is embedded in a projective plane of order m^2 and is left invariant by a collineation group isomorphic to $PSU(3,m^2)$ (the subgroup of $PGU(3,m^2)$ induced by matrices with determinant one), Hoffer [37] has shown that the plane is necessarily classical and the unital is classical. About this time, Kantor [40] showed that if a unital U of order m embedded in a projective plane of order m^2 is preserved by a collineation group G which acts transitively on the flags formed by a point of U and a secant line of U, then the projective plane is classical and U is a classical unital. Moreover, he showed $PSU(3,m^2) \leq G$ [40]. As observed in [13], due to a result of Camina and Gagen [19], one need only assume transitivity on the secant lines of U to obtain the same result. Finally, Biliotti and Korchmáros have proven, in [12] and [13], that a unital U embedded in a projective plane of order m^2 which is left invariant by a collineation group which acts primitively on the points of U must be classical and the plane is classical.

One purely geometric characterization of Buekenhout-Metz unitals is due to Lefèvre-Percsy [44]. It states that if U is a unital in π with l a tangent line to U for which the intersection of U with any Baer subline meeting l has 0, 1, 2, or $q+1$ points, then U is Buekenhout-Metz. Larato [43] showed that if U is a unital embedded in a translation plane of odd square order such that l_∞ is tangent to U, then U is Buekenhout-Metz if and only if for any two affine lines l_1 and l_2 meeting in the point $U \cap l_\infty$, there is an affine Baer subplane Π_0 such that

$$\Pi_0 \cap U = (l_1 \cap U) \cup (l_2 \cap U).$$

Casse, O'Keefe, and Pentilla [20], for $q = 3$ and q even, and Casse and Quinn [53], for $q > 3$, have also provided a geometric characterization of BM-unitals. They showed that a unital is Buekenhout-Metz if and only if there exists a point T on U such that the points of U on each of the q^2 secant lines to U through T form a Baer subline.

Abatangelo and Larato [3] proved the following group theoretic characterization.

Theorem 3.1.1 *Let U be a unital in $\pi = PG(2, q^2)$ for q odd. Then U is a Buekenhout-Metz unital which is a union of conics if and only if there is a point $P \in U$ and a linear collineation group Γ of U such that Γ is transitive on $U \setminus \{P\}$, the stabilizer in Γ of a point in $U \setminus \{P\}$ is cyclic of order $2(q-1)$, and Γ is the semidirect product of a normal abelian subgroup of order q^3 by a cyclic subgroup of order $2(q-1)$.*

For the even case, Abatangelo [1] showed the following.

Theorem 3.1.2 *Let U be a unital in $\pi = PG(2, q^2)$ for q even. Suppose there is a point $P \in U$ and a linear collineation group Γ of U such that Γ fixes P, and has a normal subgroup which is sharply transitive on $U \setminus \{P\}$, and for any $Q \in U \setminus \{P\}$, the point stabilizer Γ_Q has order $q-1$. Then U is a Buekenhout-Metz unital.*

In the following section, a concise group theoretic characterization of BM-unitals will be proven. Its method owes much to the work of Abatangelo and Larato [1, 3], yet it is wider in scope and unifies the even and odd cases into essentially one argument. The main theorem verifies the conjecture stated in the closing remarks of [26].

3.2 A Group Theoretic Characterization

Suppose U is any unital embedded in $\pi = PG(2, q^2)$ which admits a linear collineation group $\Gamma = S \rtimes R$ which is a semidirect product of a subgroup S of order q^3 by a subgroup R of order $q-1$. We proceed to show that U is necessarily a Buekenhout-Metz unital by a sequence of lemmas. The strategy closely resembles that used by Abatangelo in [1].

Lemma 3.2.1 *Γ fixes some point Y_∞ of U, and S acts regularly on $U \setminus \{Y_\infty\}$. Moreover, the translation subgroup T of S has order q and consists of elations with center Y_∞.*

Proof: Let S act on the q^3+1 points of U. By a decomposition of the orbits of U under S, we see

$$|U| = \sum \frac{|S|}{|S_P|}, \tag{3.1}$$

where the sum is taken over representatives, P, of distinct orbits and S_P denotes the stabilizer of a point P in the group S. If no point of U is fixed by S, then for every $P \in U$, $S_P < S$, and $|S|/|S_P|$ is a nonzero power of the prime p for which $q = p^n$, for some integer n. This forces p to divide the right side of (3.1), contradicting $|U| \equiv 1 \pmod p$. Thus, S must fix some point Y_∞ of U. Let $Q \in U \setminus \{Y_\infty\}$, and suppose there is some nonidentity element $s \in S$ that fixes Q. Then s leaves invariant the block $b = Y_\infty Q \cap U$. Let the cyclic subgroup $\langle s \rangle$ act on the $q+1$ points of b, and write $|b| = q+1$ as the sum of the cardinalities of the orbits of $\langle s \rangle$. As the orbits corresponding to Q and Y_∞ each have size one, $\langle s \rangle$ must fix a third point of $b \setminus \{Y_\infty, Q\}$, else one would have $1 \equiv 2 \pmod p$. Hence s fixes three distinct points of the line $Y_\infty Q$ and thus fixes every point of $Y_\infty Q$, as s is linear. Thus, s is a perspectivity of π. Now s must fix the unique tangent line to U at each point of b, and hence fix the intersection of any two such tangents. Since s fixes at most one point not lying on its axis $Y_\infty Q$, the above tangents must all be concurrent at the center of s and s must be an homology. In particular, this means $o(s)|(q^2-1)$, contradicting the fact that s is a nonidentity element of a group with order q^3. Therefore S acts semiregularly, and hence regularly, on the points of $U \setminus \{Y_\infty\}$. As Γ acts transitively on $U \setminus \{Y_\infty\}$, Γ either fixes Y_∞ or acts transitively on U. In the latter case,

$$q^3(q-1) = |\Gamma| = |\Gamma_{Y_\infty}||Y_\infty^\Gamma| = |\Gamma_{Y_\infty}|(q^3+1).$$

But $S \leq \Gamma_{Y_\infty}$ and S has order q^3. Therefore, Γ must also fix Y_∞.

Since S is a p-group, any perspectivity in S must be an elation. Moreover, the axis of any perspectivity in S must be a tangent line to U as previously argued. Since every element of S fixes Y_∞, any perspectivity in S must be an elation with axis l_∞, where l_∞ is the tangent line to U at Y_∞. We call the subgroup of all such elations, together with the identity element, the *translation subgroup* T of S.

We next observe that any nonidentity element θ of T must have center Y_∞. Namely, if the center were $C \neq Y_\infty$, then θ would leave invariant the $q+1$ tangent lines through C and hence fix the corresponding $q+1$ points of tangency, contradicting the fact that θ is an elation with axis l_∞. Thus, since T must act semiregularly on the q points of $U \setminus \{Y_\infty\}$ that lie on any line through Y_∞, the order of T is at most q. To show that T actually has order q we let S act on the q^2 secants through Y_∞. This action is transitive as S acts regularly on $U \setminus \{Y_\infty\}$. If l is any such line, then the stabilizer S_l of l under this action has order $|S|/|l^S| = q$. Letting S_l act on the q^2-1 secant lines through Y_∞ other than l, we see by an orbit decomposition argument that S_l must fix some secant $m \neq l$ through Y_∞. Hence any nonidentity element of S_l fixes the three lines l_∞, l, and m through Y_∞, and therefore fixes all lines through Y_∞. That is, $S_l \leq T$ and T consists of q elations with center Y_∞. ■

If A is any point of $U \setminus \{Y_\infty\}$, we may coordinatize π so that A is the origin, AY_∞ is the y-axis, the x-axis is the tangent line to U at A, and the line at infinity is the tangent line l_∞ to U at Y_∞. Let X_∞ be the intersection of l_∞ and the x-axis.

Lemma 3.2.2 *The stabilizer Γ_A of A in Γ is cyclic of order $q-1$. It consists of (affine) transformations of the form*

$$h_\alpha : (x, y) \to (\alpha x, \beta(\alpha) y),$$

where α varies over K^* and β is a mapping from K^* into K^*. Moreover, β is a bijection when q is even, while the range of β is K_S when q is odd.

Proof: Since Γ acts transitively on $U \setminus \{Y_\infty\}$, Γ_A has order $q-1$. Since Γ_A fixes A and Y_∞, it leaves invariant the unique tangent lines to U at A and Y_∞, and hence fixes their intersection X_∞. In particular, Γ_A leaves invariant the x-axis, y-axis, and l_∞. Thus the $q-1$ elements of Γ_A may be expressed affinely as maps of the form

$$h_{\alpha,\beta} : (x, y) \to (\alpha x, \beta y)$$

for certain choices of $\alpha, \beta \in F$. Suppose first that Γ_A has two distinct elements with the same "α-subscripts", say h_{α,β_1} and h_{α,β_2} with $\beta_1 \neq \beta_2$. Then $h = h^{-1}_{\alpha,\beta_1} h_{\alpha,\beta_2} : (x, y) \mapsto (x, \beta_1^{-1}\beta_2 y)$ is easily seen to be a nontrivial homology whose axis is the x-axis and whose center is Y_∞. Let the cyclic subgroup $\langle h \rangle$ act on the $q+1$ points of some block b containing Y_∞, other than the y–axis. As b contains no point on the x-axis, no point of $b \setminus \{Y_\infty\}$ is fixed by any of the nontrivial homologies of $\langle h \rangle$. Thus, $o(h) = |P^{\langle h \rangle}|$ for each $P \in b \setminus \{Y_\infty\}$, giving $o(h)|q$. But $h \in \Gamma_A$, giving $o(h)|(q-1)$. Therefore, $o(h)|gcd(q, q-1)$, contradicting the fact that $h \neq id$. Hence, if $\mathcal{A} = \{\alpha \in F^* : h_{\alpha,\beta} \in \Gamma_A \text{ for some } \beta \in F^*\}$, then $\mathcal{A}$ is a multiplicative subgroup of F^* of order $q-1$, and hence $\mathcal{A} = K^*$. In particular, this implies that Γ_A is cyclic and $\beta = \beta(\alpha)$ is a function of α.

Next suppose that two distinct elements of Γ_A have the same "β–subscripts", say $h_{\alpha_1,\beta}$ and $h_{\alpha_2,\beta}$ with $\alpha_1 \neq \alpha_2$. Then $h = h^{-1}_{\alpha_1,\beta} h_{\alpha_2,\beta}$ is a nontrivial homology whose axis is the y-axis and whose center is X_∞. The $q+1$ tangent lines to U through X_∞ must meet U in the $q+1$ points of the block $U \cap AY_\infty$ since these points of tangency must be fixed by h. Thus any one of the q^2-q secants to U through X_∞ must meet U in a block b consisting of $q+1$ points, none of which lie on the y-axis. Letting $\langle h\rangle$ act on the $q+1$ points of any such block b, we see that this action is semiregular. Therefore, $o(h)=|P^{\langle h\rangle}|$ for all $P\in b$, thereby showing that $o(h)|(q+1)$. Thus

$$o(h)|gcd(q+1,\ q-1). \tag{3.2}$$

If q is even, then $gcd(q+1,\ q-1)=1$ and we contradict the fact that $h\neq id$. That is, for q even the β-subscripts on elements of Γ_A are all distinct and $\mathcal{B}=\{\beta\in F^*: h_{\alpha,\beta}\in\Gamma_A \text{ for some } \alpha\in K^*\}$ is a multiplicative subgroup of F^* of order $q-1$, and hence $\mathcal{B}=F^*$. In this case, we have shown that β is a bijection on K^*.

Suppose now that q is odd and thus $o(h)=2$ from (3.2). From the first paragraph of this proof, we see that $h_{1,-1}\notin\Gamma_A$ as $h_{1,1}=id\in\Gamma_A$. By way of contradiction, suppose $h_{-1,-1}\in\Gamma_A$. Let $\langle h_{-1,-1}\rangle$ act on a block b through Y_∞ different from the y-axis and note that $h_{-1,-1}$ fixes no points of $U\setminus\{Y_\infty\}$ other than the origin A. By an oft repeated argument, we see that $o(h_{-1,-1})|q$, contradicting the fact that $o(h_{-1,-1})=2$ when q is odd. Hence, the unique element of order two in the cyclic group Γ_A must be $h_{-1,1}$. That is, $h=h_{-1,1}$ above and $h_{\alpha_2,\beta}=h_{\alpha_1,\beta}h_{-1,1}=h_{-\alpha_1,\beta}$, implying that $\alpha_2=-\alpha_1$. Moreover, if $h_{\alpha,\beta}\in\Gamma_A$ is arbitrary, then $h_{-1,1}h_{\alpha,\beta}=h_{-\alpha,\beta}\in\Gamma_A$ as well. We see that elements of Γ_A share the same "β-subscripts" if and only if the "α-subscripts" are negatives of each other. Thus $\mathcal{B}=\{\beta\in F^*: h_{\alpha,\beta}\in\Gamma_A \text{ for some } \alpha\in K^*\}$ is a multiplicative subgroup of order $(q-1)/2$ in F^*, and hence $\mathcal{B}=S_q$ when q is odd. ■

Eventually, we will show that $\beta=\beta(\alpha)=\alpha^2$ for all $\alpha\in K^*$, using the notation of Lemma 3.2.2. First we return to our coordinatization of π. So far we have only specified coordinates for A, Y_∞, and X_∞. We now pick a fourth point for our frame in such a way so that the affine point $(0,1)$ lies on U. Recall from Lemma 3.2.1 that the translation subgroup T of S consists of q elations, including the identity, with axis l_∞ and center Y_∞. As shown in the proof of Lemma 3.2.1, these are the only perspectivities in S.

Lemma 3.2.3 *The elements of T, treated as affine maps, have the form*

$$\theta_t : (x, y) \to (x, y + t),$$

where t ranges over K.

Proof: As the elements of T have center Y_∞, for any affine point of U, the x-coordinate is fixed and the y-coordinate is shifted by such translations. Thus elements of T have the form θ_t, as above, for $t \in F$. Moreover, t must vary over some additive subgroup H of order q in F. Writing Γ as the semidirect product of S by Γ_A, we see that Γ_A normalizes the translation subgroup T of S. Using the notation established above and in Lemma 3.2.2, we obtain $h_\alpha \theta_t h_\alpha^{-1} \in T$ for all $\alpha \in K^*$ and for all $t \in H$. This implies that $\beta(\alpha)t \in H$ for all $\beta(\alpha) \in \mathcal{B}$ and $t \in H$. Recall that the range $\mathcal{B}$ of the function β is K^* for q even and is S_q for q odd. Since each nonsquare in K, q odd, may be written as a sum of squares (see Lemma 5.1.4 of [33], for instance), we immediately see that H is a vector subspace of F over K. As shown in the proof of Lemma 3.2.1, T acts transitively on the affine points of the block $AY_\infty \cap U$. Since $(0, 1) \in AY_\infty \cap U$, there must be some translation in T sending A to $(0, 1)$. Thus $1 \in H$ and $H = (K, +)$. ∎

We now attempt to explicitly determine the form of all transformations in the subgroup S as was done in [1] and [3]. In fact, the notation closely follows that used in [1] and [3]. As S fixes Y_∞ and acts regularly on $U \setminus \{Y_\infty\}$, Lemma 3.2.3 implies that the elements of S, treated as affine maps, have the form

$$s_{(a,t)} : (x, y) \to (x + a,\ \phi(a)x + \delta(a)y + \psi(a) + t), \tag{3.3}$$

where a ranges over F, t ranges over K, and ϕ, δ, ψ are certain functions from F into F. For the remainder of this paper each element x of F will be expressed uniquely as $x_1 + x_2\epsilon$ for some $x_1,\ x_2 \in K$, where $\{1, \epsilon\}$ is the basis for F over K described in Section 2.2. In particular, we may assume without loss of generality that $\psi(a)$ is a K-multiple of ϵ, the scalar obviously depending upon a.

Lemma 3.2.4 *Using the above notation,*

(i) $\phi(0) = 0$ *and* $\psi(0) = 0$*,*

(ii) $\delta(a) = 1$ *for all* $a \in F$*,*

(iii) There exist constants $c \in K$ *and* $d \in F$ *such that* $\phi(a) = da - ca_2$ *for all* $a \in F$*, where* a *is uniquely expressed as* $a_1 + a_2\epsilon$ *for some* $a_1, a_2 \in K$*, and*

(iv) $\psi(a + b) - \psi(a) - \psi(b) - \phi(b)a \in K$ *for all* $a, b \in F$*.*

Proof: For $s_{(a,t_1)},\ s_{(b,t_2)} \in S$, the map $s_{(a,t_1)} \circ s_{(b,t_2)}$, whose rule is

$$(x, y) \to (x+a+b, [\phi(a)+\delta(a)\phi(b)]x+\delta(a)\delta(b)y+\phi(b)a+\delta(a)\psi(b)+\psi(a)+\delta(a)t_2+t_1), \tag{3.4}$$

must be in S for all $a, b \in F$ and for all $t_1, t_2 \in K$. Moreover, $s_{(a,t_1)} \circ s_{(b,t_2)} = s_{(a+b,t)}$ for some $t \in K$. By analyzing the x and y coefficients of the second coordinate, we obtain

$$\phi(a + b) = \phi(a) + \delta(a)\phi(b) \tag{3.5}$$

$$\delta(a + b) = \delta(a)\delta(b) \tag{3.6}$$

for all $a, b \in F$. Since $s_{(0,0)}$ clearly serves as the identity map in S, we must have $\phi(0) = 0,\ \delta(0) = 1$ and $\psi(0) = 0$. If p denotes the characteristic of K, from (3.6) we obtain $1 = \delta(0) = \delta(pa) = (\delta(a))^p$ and hence $\delta(a) = 1$ for all $a \in F$. We have thus proven parts (i) and (ii) of the lemma.

By examining the constant term of the second coordinate of $s_{(a+b,t)}$ as given by (3.4), we further obtain

$$\psi(a + b) - \psi(a) - \psi(b) - \phi(b)a \in K \tag{3.7}$$

for all $a, b \in F$, thus proving part (iv). Interchanging the roles of a and b in (3.7) and then subtracting, we see that

$$\phi(b)a - \phi(a)b \in K \tag{3.8}$$

for all $a, b \in F$. In particular, with $b = 1$ we have $\phi(1)a - \phi(a) \in K$ for all $a \in F$.

If we now define a new function

$$\lambda : F \to K \text{ via } \lambda(a) = \phi(1)a - \phi(a), \tag{3.9}$$

then (3.5), (ii), and (3.8) imply that

$$\lambda(a + b) = \lambda(a) + \lambda(b) \tag{3.10}$$

$$\lambda(a)b - \lambda(b)a \in K \tag{3.11}$$

for all $a, b \in F$. Picking $a \in K$ and $b \in F \setminus K$, we see that $\lambda(a)b \in K$ from (3.11) and thus $\lambda(a) = 0$ for all $a \in K$. If an arbitrary element a of F is expressed uniquely as $a = a_1 + a_2\epsilon$ for some $a_1, a_2 \in K$, then (3.10) and the above observations imply

$$\lambda(a) = \lambda(a_1) + \lambda(a_2\epsilon) = \lambda(a_2\epsilon). \tag{3.12}$$

On the other hand, choosing $a = a_2\epsilon$ and $b = b_2\epsilon$ in (3.11), where $a_2, b_2 \in K$, we obtain $\lambda(a_2\epsilon)b_2 - \lambda(b_2\epsilon)a_2 = 0$. That is, $\frac{\lambda(a_2\epsilon)}{a_2} = \frac{\lambda(b_2\epsilon)}{b_2}$ whenever a_2 and b_2 are nonzero elements of K, and we may define c to be the constant in K given by

$$c := \frac{\lambda(a_2\epsilon)}{a_2} \text{ for any } a_2 \in K^*. \tag{3.13}$$

Thus, for any $a \in F$, (3.12) gives

$$\lambda(a) = ca_2. \tag{3.14}$$

Finally, if we define d to be the constant $\phi(1)$ in F, (3.9) and (3.14) imply that $\phi(a) = da - ca_2$ for all $a = a_1 + a_2\epsilon$ in F, proving (iii) of the lemma. ■

Lemma 3.2.5 *Using the notation from Lemma 3.2.2, $\beta = \beta(\alpha) = \alpha^2$ for all $\alpha \in K^*$.*

Proof: As Γ_A normalizes S, we see that $h_\alpha s_{(a,t)} h_\alpha^{-1} \in S$ for all $a \in F$, $t \in K$, and $\alpha \in K^*$, where

$$h_\alpha s_{(a,t)} h_\alpha^{-1} : (x, y) \to (x + \alpha a, \alpha^{-1}\beta\phi(a)x + y + \beta(\psi(a) + t)), \tag{3.15}$$

using our previously established notation. Thus $h_\alpha s_{(a,t)} h_\alpha^{-1} = s_{(\alpha a, t')}$ for some $t' \in K$. Examining the x coefficient of the second coordinate, we see that

$$\phi(\alpha a) = \alpha^{-1}\beta\phi(a) \text{ for all } a \in F \text{ and } \alpha \in K^*. \tag{3.16}$$

Expressing $a = a_1 + a_2\epsilon$ for some $a_1, a_2 \in K$, part (iii) of Lemma 3.2.4 implies $\phi(\alpha a) = \alpha\phi(a)$ and hence $\alpha^2\phi(a) = \alpha\phi(\alpha a) = \beta\phi(a)$. Since the translation subgroup of S has order q by Lemma 3.2.1, $\phi(a) \neq 0$ whenever $a \neq 0$. The result now follows by cancellation. ■

Theorem 3.2.6 *Let U be a unital embedded in π which admits a linear collineation group $\Gamma = S \rtimes R$ that is a semidirect product of a subgroup S of order q^3 by a subgroup R of order $q - 1$. Then U is a Buekenhout-Metz unital.*

Proof: We freely use all the notation previously established. Using $\beta = \alpha^2$, analyzing the constant term of (3.15) shows that $\psi(\alpha a) - \alpha^2\psi(a) \in K$. By assumption, ψ maps F to the coset $K\epsilon$, hence

$$\psi(\alpha a) = \alpha^2\psi(a), \tag{3.17}$$

for all $a \in F$ and $\alpha \in K^*$. Let a be an arbitrary element of F, and express a as $a_1 + a_2\epsilon$ for some $a_1, a_2 \in K$. Using part (iii) of Lemma 3.2.4 and (3.17) in part (iv) of Lemma 3.2.4, we obtain

$$\psi(a_1 + a_2\epsilon) - a_1^2\psi(1) - a_2^2\psi(\epsilon) - a_1a_2d_1\epsilon - a_1a_2d_2\epsilon^2 + a_1a_2c \in K \tag{3.18}$$

where we have also expressed the constant $d \in F$ as $d_1 + d_2\epsilon$ for some $d_1, d_2 \in K$.

If q is even, then parts (i) and (iv) of Lemma 3.2.4 with $a = b = 1$ imply that $\phi(1) = d \in K$ and hence $d_2 = 0$. With $a = b = \epsilon$, we see $\phi(\epsilon)\epsilon \in K$, which gives $(d\epsilon - c)\epsilon \in K$, from (iii) of Lemma 3.2.4. Using (2.2), we find that $d_1 = c$ and hence

$$\phi(a) = ca^q. \tag{3.19}$$

If q is odd, then $\epsilon^2 = w \in K$. In either case, $c \in K$ and (3.18) reduces to

$$\psi(a_1 + a_2\epsilon) - a_1^2\psi(1) - a_2^2\psi(\epsilon) - a_1a_2d_1\epsilon \in K.$$

Since $\psi(a)$ is a K-scalar multiple of ϵ, this implies that

$$\begin{aligned} \psi(a) = \psi(a_1 + a_2\epsilon) &= a_1^2\psi(1) + a_2^2\psi(\epsilon) + a_1a_2d_1\epsilon \\ &= (a_1^2k_1 + a_2^2k_2 + a_1a_2d_1)\epsilon, \end{aligned} \tag{3.20}$$

where k_1, k_2, and d_1 are fixed constants in K.

Now Lemma 3.2.4 implies that the q^3 elements of S have affine representations of the form

$$s_{(a,t)} : (x, y) \to (x + a, (da - ca_2)x + y + t + \psi(a))$$

as a ranges over F and t ranges over K, where $c \in K$ and $d \in F$ are constants and ψ is given by (3.20). Since S acts regularly on $U \setminus \{Y_\infty\}$, we see that $U \setminus \{Y_\infty\}$ is the orbit of $A = (0, 0)$ under S and hence $U \setminus \{Y_\infty\} = \{(a, t + \psi(a) : a \in F, t \in K\}$. It should be noted that $\psi(a) \neq 0$ whenever $a \neq 0$ since the x-axis is tangent to U at $A = (0, 0)$.

Modeling $PG(2, q^2)$ in $PG(4, q)$ as described in Section 2.2, we thus have the q^3 affine points of U represented as

$$\{(a_1, a_2, t, k_1a_1^2 + k_2a_2^2 + d_1a_1a_2, 1) : a_1, a_2, t \in K\},$$

where we have right normalized vectors to get a unique representation for points in $PG(4, q)$. Thinking in terms of homogeneous coordinates (x_1, x_2, y_1, y_2, z) for

$PG(4,q)$, where $z = 0$ is the hyperplane at infinity, this set is described by the equation $y_2 z - f(x_1,x_2) = 0$, where $f(x_1,x_2) = k_1x_1^2 + k_2x_2^2 + d_1x_1x_2$. Moreover, f is an irreducible binary form since $\psi(a) \neq 0$ whenever $a \neq 0$ as stated above. Hence this equation represents the cone of an elliptic quadric (see [34] page 14), with vertex $(0,0,1,0,0)$. Therefore U is a Buekenhout-Metz unital by definition. ■

We note that when q is an odd prime p the normality of S in Γ is not needed in the hypotheses of Theorem 3.2.6. That is to say, if U is a unital embedded in $PG(2,p^2)$, for p an odd prime, which admits a linear collineation group Γ of order $p^3(p-1)$ with a subgroup S of order p^3 and subgroup R of order $p-1$, then by Sylow's Theorem $S \triangleleft \Gamma$, which proves $\Gamma = S \rtimes R$. One may reasonably question whether the assumption of the normality of S is needed in general. We note that this assumption was not used until Lemma 3.2.5 and was used thereafter only at the beginning of the proof of Theorem 3.2.6.

Group theory may also be used to characterize certain BM-unitals within the class of BM-unitals.

Corollary 3.2.7 *Assume the hypotheses of Theorem 3.2.6. If S is abelian, then S is elementary abelian and U is a Buekenhout-Metz unital consisting of a union of conics. Moreover, q is necessarily odd in this case.*

Proof: It is well known (see [8] and [26], for instance) that a Sylow p-subgroup of the full linear collineation group stabilizing a classical unital has order q^3 and is nonabelian. Hence, if the subgroup S is abelian, U is necessarily nonclassical. It then follows from Theorem 2.2.1 that q is odd and U is a union of conics.

We now offer a direct proof of these assertions and prove that S is necessarily elementary abelian in the process. We use the notation developed throughout this section. For $s_{(a,t_1)}$ and $s_{(b,t_2)} \in S$, for $a,b \in F$ and $t_1,t_2 \in K$, the composition $s_{(a,t_1)} \circ s_{(b,t_2)}$ is given by (3.4). Comparing the y-coordinates of $s_{(a,t_1)} \circ s_{(b,t_2)}$ and

$s_{(b,t_2)} \circ s_{(a,t_1)}$, we find that S is abelian if and only if $ca_2b = cab_2$ for all $a, b \in F$, where c is defined by (3.13). Substituting, $a = 1$ and $b = \epsilon$, shows $c = 0$.

By way of contradiction, suppose q is even. We have seen that $d_1 = c$ in this case. Therefore, S is abelian if and only if $d_1 = 0$, which implies that the quadratic form associated with ψ (as in (3.20)) is reducible. This contradiction forces q to be odd.

When q is odd, with $c = 0$, S may easily be shown to be elementary abelian by observing that $s^p_{(a,t)} : (x, y) \to (x + pa,\ pdax + y + pt + p\psi(a) + \frac{p(p-1)}{2}da^2) = (x, y)$ for any $s_{(a,t)} \in S$, since p is odd.

To explicitly describe the conics forming this unital, we consider (iv) of Lemma 3.2.4 with $c = 0$, to obtain $\psi(a+b) - \psi(a) - \psi(b) - dab \in K$ for all $a, b \in F$. Using this with (3.20), we then compute that $(2k_1 - d_2)a_1b_1 + (2k_2 - d_2\omega)a_2b_2 = 0$, for all $a, b \in F$. With $a = b = 1$ and $a = b = \epsilon$, this gives $2k_1 - d_2 = 0$ and $2k_2 - d_2\omega = 0$, respectively, hence $k_2 = k_1\omega$. Thinking in terms of the description found in (2.3), we define $a := \frac{d_1}{2} + k_1\epsilon$. Let $C_s = \{(x, ax^2 + s, 1) : x \in F\} \cup \{(0, 1, 0)\}$ and notice that C_s is a nondegenerate conic in $PG(2, q^2)$ for each $s \in K$. Furthermore, $C_s \cap C_{s'} = \{(0, 1, 0)\}$, for $s \neq s'$, hence $\left|\bigcup_{s\in K} C_s\right| = q^3 + 1$. To see that $C_s \subset U$, fix $s \in K$ and let $P = (x, ax^2 + s, 1) \in C_s$, for some $x \in F$. Then, writing $x = x_1 + x_2\epsilon$, for $x_1, x_2 \in K$, we see

$$P = (x, (k_1x_1^2 + d_1x_1x_2 + k_1\omega x_2^2)\epsilon + \frac{d_1}{2}(x_1^2 + \omega x_2^2) + 2k_1\omega x_1x_2 + s, 1) \in U,$$

where $\frac{d_1}{2}(x_1^2 + \omega x_2^2) + 2k_1\omega x_1x_2 + s$ is some element $t \in K$. Thus $U = \bigcup_{s\in K} C_s$. ■

Using the techniques demonstrated in this section, we also obtain a new group theoretic characterization of the classical unital.

Corollary 3.2.8 *Let U be a unital embedded in π which admits a linear collineation group $\Gamma = S \rtimes R$ that is a semidirect product of a subgroup S of order q^3 by a subgroup R of order $q^2 - 1$. Then U is classical.*

Proof: Exactly as in the lemmas leading up to the proof of Theorem 3.2.6, one shows that Γ fixes some point Y_∞ of U, S acts regularly on $U \setminus \{Y_\infty\}$, and $|\Gamma_A| = q^2 - 1$ for any point $A \in U \setminus \{Y_\infty\}$. Using the same argument given in the proof of Lemma 3.2.2, we find $\mathcal{A} = \{\alpha : h_{\alpha,\beta} \in \Gamma_A\} = F^*$, hence Γ_A is cyclic. Therefore, Γ_A has a subgroup R_0 of order $q - 1$, and the semidirect product $S \rtimes R_0$ is a linear collineation group leaving U invariant. Thus, U is a Buekenhout-Metz unital by Theorem 3.2.6 and therefore classical using Theorem 2.2.1.

We now provide a direct proof that U is the set of absolute points of a hermitian form without relying on Theorem 2.2.1. We have observed that Lemma 3.2.1 may be readily adapted to the case when Γ_A has order $q^2 - 1$ and that elements of Γ_A have the form $h_{\alpha,\beta}$ as in Lemma 3.2.2 with the exception that α ranges over F. To complete the analog of Lemma 3.2.2, we show that the range of the function β is K^*. As Γ_A is cyclic of order $q^2 - 1$, it has an element $h = h_{\alpha,\beta}$ of order $q + 1$, where we note that $\alpha \neq 1$. By way of contradiction, suppose $\beta \neq 1$ and let $\langle h \rangle$ act on a block b through Y_∞ different from the y-axis. As $\langle h \rangle$ fixes no points of $b \setminus \{Y_\infty\}$, we see $o(h) = |P^{\langle h \rangle}|$ for all $P \in b \setminus \{Y_\infty\}$, hence $o(h)|q$. From this contradiction, we determine that elements of $\langle h \rangle$ have the form $h_{\alpha,1}$ for α in the subgroup of F^* defined by $\mathcal{A}_1 = \{\alpha \in F^* : \alpha^{q+1} = 1\}$. Suppose $h_{\alpha_1,\beta}, h_{\alpha_2,\beta} \in \Gamma_A$, for $\alpha_1 \neq \alpha_2$, share the same "β-subscripts". Using the counting argument given in Lemma 3.2.2, we see that $o(h^{-1}_{\alpha_1,\beta} h_{\alpha_2,\beta})|(q+1)$, i.e. $h^{-1}_{\alpha_1,\beta} h_{\alpha_2,\beta} = h_{\alpha,1}$ for some $\alpha \in \mathcal{A}_1$. Therefore, $h_{\alpha_1,\beta}$ and $h_{\alpha_2,\beta}$ share the same "β-subscript" if and only if $\alpha_1 = \alpha_2\alpha$ for some $\alpha \in \mathcal{A}_1$. Hence β is a $(q + 1)$-to-1 map and $\mathcal{B} = \{\beta : h_{\alpha,\beta} \in \Gamma_A \text{ for some } \alpha \in \mathcal{A}\} \leq F^*$ has order $q - 1$, giving $\mathcal{B} = K^*$.

One may prove the analogs of Lemmas 3.2.3 and 3.2.4 with very few changes required. Notice that the analog of (3.16) would be that

$$\phi(\alpha a) = \alpha^{-1}\beta\phi(a) \text{ for all } a \in F \text{ and } \alpha \in F^*. \tag{3.21}$$

If q is even, using (3.18) in (3.21) gives $\alpha^q a^q c = \alpha^{-1}\beta a^q c$. Substituting $a = 1$ and noting that $c \neq 0$, we see that $\beta = \alpha^{q+1}$. If q is odd, using (iii) of the analog to Lemma 3.2.4 in (3.21) with $a = 1$ and $a = \epsilon$, one finds that $d\alpha - c\alpha_2 = \alpha^{-1}\beta d$ and $d\alpha\epsilon - c\alpha_1 = \alpha^{-1}\beta(d\epsilon - c)$, respectively, where $\alpha = \alpha_1 + \alpha_2\epsilon$ for $\alpha_1, \alpha_2 \in K$. Notice from either of these equations that $c \neq 0$ else $\beta = \alpha^2$ for all $\alpha \in F^*$ (as $d \neq 0$), where α^2 may take on values in $F \setminus K^*$. These equations may then be solved to obtain $\beta = \alpha^{q+1}$. Using this in (3.21) and substituting $\alpha = \epsilon$ and $a = 1$, we see that $2d\epsilon - c = 0$, hence $d_1 = 0$, when q is odd.

The analog of (3.17) stems from the fact that $\psi(\alpha a) - \beta\psi(a) \in K$ for all $\alpha \in F^*$ and $a \in F$. Thus

$$\psi(\alpha a) - \alpha^{q+1}\psi(a) = 0, \tag{3.22}$$

as $\alpha^{q+1} \in K^*$ and the range of ψ is $K\epsilon$. Notice that $\alpha^{q+1} = \alpha^2$ for all $\alpha \in K^*$ thus ψ may be written as in (3.20). If q is even, by representing ψ as in (3.20) and using (3.22) with $\alpha = \epsilon$ and $a = 1$, one obtains $k_2 = \sigma k_1$. Similarly, by substituting $\alpha = 1 + \epsilon$ and $a = 1$, one learns that $\psi(1 + \epsilon) = \sigma k_1$. But $\psi(1 + \epsilon) = k_1 + d_1 + k_2$ directly from (3.20), thus $k_1 = d_1$. Therefore $\psi(x) = k_1(x_1^2 + x_1x_2 + \sigma x_2^2)\epsilon = k_1 x^{q+1}\epsilon$. If q is odd, with $\alpha = \epsilon$ and $a = 1$ in (3.22), we find that $k_2 = -\omega k_1$. Therefore, recalling $d_1 = 0$, $\psi(x) = k_1(x_1^2 - \omega x_2^2)\epsilon = k_1 x^{q+1}\epsilon$.

For both the even and odd cases, we see that

$$U = \{(x, k_1 x^{q+1}\epsilon + t, 1) : x \in F, t \in K\} \cup \{(0, 1, 0)\}.$$

Thus the points of U are absolute points of the hermitian form represented by the nonsingular matrix

$$\begin{pmatrix} k_1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

if q is even, and

$$\begin{pmatrix} 2k_1 & 0 & 0 \\ 0 & 0 & -\epsilon^{-1} \\ 0 & \epsilon^{-1} & 0 \end{pmatrix},$$

if q is odd. ■

Chapter 4

UNITALS EMBEDDED IN THE HUGHES PLANE

We have thus far endeavored to add to the already substantial body of available knowledge regarding unitals embedded in the classical projective plane. It has been noted that all known examples of such unitals are obtainable from Buekenhout's parabolic construction, but it is still an open question as to whether other unitals embedded in $PG(2, q^2)$ exist. Moreover, Buekenhout's parabolic method enables us to construct unitals in all two-dimensional translation planes. Since far less is known about unitals embedded in non-translation planes, it seems that this nonclassical setting would provide fertile ground in which to labor. We have found the Hughes plane to be a particularly hospitable setting in which to work. As noted earlier, the first finite example of a nonclassical projective plane (found by Veblen and Wedderburn [61]) belongs to the class of Hughes planes.

The Hughes plane offers the advantage of preserving several important aspects of the classical plane, while providing a straightforward analog of others. For instance, points and lines of the Hughes plane are represented by certain equivalence classes of "vectors" over a nearfield of order q^2, where the operations of the nearfield are a slight perturbation of the operations of the field $GF(q^2)$. In addition, one may define incidence in the Hughes plane as a modification of incidence in the classical plane. Furthermore, in a manner similar to the classical plane, the full collineation group of the Hughes plane is the semidirect product of a group induced by matrices with the automorphism group of the nearfield.

4.1 Description of the Hughes Plane

A *nearfield* is an algebraic structure $(N, +, \cdot)$ for which $+$ and $\cdot$ are associative binary operations on N, $(N, +)$ and $(N \setminus \{0\}, \cdot)$ are groups, and

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$

for all $a, b, c \in N$. The *kernel* of a nearfield N is the set of elements $c \in N$ for which

$$(a + b) \cdot c = a \cdot c + b \cdot c \text{ for all } a, b \in N.$$

Let F be a finite field of odd order q^2 with K its subfield of order q and with F_S and F_N the squares and nonsquares of F, respectively. Multiplication in F will be denoted by juxtaposition. We define a nearfield N by taking the elements of F with $+$ defined as in F and $\cdot$ defined as follows:

$$a \cdot b = \begin{cases} ab & \text{if} \quad a \in F_S \\ ab^q & \text{if} \quad a \in F_N \\ 0 & \text{if} \quad a = 0 \end{cases} . \tag{4.1}$$

Notice that K is the kernel of N and if $K^* = K \setminus \{0\}$ and $N^* = N \setminus \{0\}$, then $(K^*, \cdot)$ is the center of $(N^*, \cdot)$. Also notice that the Frobenius automorphism σ of F, $\sigma : x \mapsto x^q$, leaves F_S and F_N invariant since q is odd. Thus the Frobenius automorphism preserves $\cdot$, hence is also an automorphism of N.

Let V be a three-dimensional vector space over F. We consider the vectors of $V^* = V \setminus \{(0, 0, 0)\}$ as three-tuples over N, as well. Using the notation of Rosati [56], we define an equivalence relation ρ on V^* by

$$P \rho Q \text{ if and only if } Q = a \cdot P \text{ for some } a \in N^*. \tag{4.2}$$

Here, the notation $a \cdot P$ means $(a \cdot x, a \cdot y, a \cdot z)$, where $P = (x, y, z) \in V^*$. Thus V^* may be partitioned into $q^4 + q^2 + 1$ ρ-equivalence classes each of size $q^2 - 1$. Moreover, one may choose a unique left-normalized representative from each of these classes in the following way. First note that if $a \in F^*$ then a, $1/a$, a^q, and $1/a^q$ share the same quadratic character, as q is odd. If $a \in F_S$, then $a \cdot \frac{1}{a} = a\frac{1}{a} = 1$ and $\frac{1}{a} \cdot a = \frac{1}{a}a = 1$. If $a \in F_N$, then $a \cdot \frac{1}{a^q} = a(\frac{1}{a^q})^q = 1$ and $\frac{1}{a^q} \cdot a = \frac{1}{a^q}a^q = 1$. Thus, the inverse of a in N is $1/a^\theta$ where $\theta = 1$ or q, as $a \in F_S$ or F_N, respectively. Therefore, when $x \neq 0$, we see that $\frac{1}{x^\theta} \cdot (x, y, z) = (1, (\frac{y}{x})^\theta, (\frac{z}{x})^\theta)$, where $\theta = 1$ or q, as $x \in F_S$ or F_N, respectively. Hence, $(x, y, z)\rho(1, (\frac{y}{x})^\theta, (\frac{z}{x})^\theta)$. One can similarly find a left-normalized representative when x is 0, as well as find a right-normalized representative for every ρ-equivalence class. It is clear that such representatives will be unique.

We now define an incidence relation J on V^* as in [56]. For fixed $t \in F \setminus K$, the set $\{1, t\}$ forms a basis for F over K. If $P = (x, y, z)$ and $Q = (u, v, w)$ are contained in V^* such that $u = u_1 + u_2 t$, $v = v_1 + v_2 t$, and $w = w_1 + w_2 t$, for $u_1, u_2, v_1, v_2, w_1, w_2 \in K$, then we define

$$PJQ \text{ if and only if } xu_1 + yv_1 + zw_1 + (xu_2 + yv_2 + zw_2) \cdot t = 0. \tag{4.3}$$

Rosati [55] has shown that J is symmetric and if PJQ then $(a \cdot P)J(b \cdot Q)$ for all $a, b \in N^*$. Thus J induces an incidence relation on the ρ-equivalence classes of V^*.

Consider an incidence structure where "points" and "lines" are defined to be equivalence classes of ρ with incidence given by J. This structure is a projective plane of order q^2 (see [55]) known as the *Hughes plane*. It should be noted that different choices of $t \in F \setminus K$ generate isomorphic Hughes planes. We denote a Hughes plane of order q^2 by $\mathcal{H}(q^2)$. The plane was first constructed by Hughes [38], who used a different method of construction than that given here. The special case when $q = 3$ was studied by Veblen and Wedderburn [61]. It may be helpful to contrast the construction of the Hughes plane with that of the classical plane given in Section 1.1. Recall that for the classical projective plane, the equivalence classes are one-dimensional subspaces (with the zero vector removed) and incidence is the standard inner product. As in the classical case, we will represent points and lines of the Hughes plane with vectors in V^*, with point coordinates in parentheses and line coordinates in square brackets. We also freely identify a point (or line) of $\mathcal{H}(q^2)$ with any of its representatives in V^*.

It will be helpful to view the incidence relation J in a manner which more closely resembles the standard inner product. As q is odd, we select $t = \epsilon$ for use in (4.3), where ϵ is defined as in (2.1), i.e. $\epsilon = \gamma^{(q+1)/2}$ for γ a primitive element of F. Note that for $x = x_1 + x_2\epsilon$, with $x_1, x_2 \in K$, we have $x^q = x_1 - x_2\epsilon$. Suppose (x, y, z) is a left-normalized representative of a point P and $[u, v, w]$ is a right-normalized representative of a line Q of $\mathcal{H}(q^2)$. We then define $d_{PQ} = xu_2 + yv_2 + zw_2$. Notice first that since $d_{P^qQ} = (d_{PQ})^q$, we see that d_{P^qQ} and d_{PQ} have the same quadratic character. Also notice that $d_{PQ^q} = -d_{PQ}$, hence d_{PQ} and d_{PQ^q} have the same quadratic character in F. If $d_{PQ} \in F_S$ then $(xu_2+yv_2+zw_2)\cdot\epsilon = xu_2\epsilon+yv_2\epsilon+zw_2\epsilon$. Hence, in this case, (4.3) takes the form

$$PJQ \iff xu + yv + zw = x(u_1 + u_2\epsilon) + y(v_1 + v_2\epsilon) + z(w_1 + w_2\epsilon) = 0. \quad (4.4)$$

If $d_{PQ} \in F_N$ then $(xu_2 + yv_2 + zw_2)\cdot\epsilon = (xu_2 + yv_2 + zw_2)\epsilon^q = -(xu_2 + yv_2 + zw_2)\epsilon$. In this case, (4.3) looks like

$$PJQ \iff xu^q + yv^q + zw^q = x(u_1 - u_2\epsilon) + y(v_1 - v_2\epsilon) + z(w_1 - w_2\epsilon) = 0. \quad (4.5)$$

If $d_{PQ} = 0$, we see that both forms (4.4) and (4.5) of (4.3) hold true. Notice that in either case PJQ if and only if P^qJQ^q, where P^q denotes raising each coordinate to the qth power. Therefore, the Frobenius field automorphism induces a collineation of $\mathcal{H}(q^2)$. Also note that $PJQ^q \iff P^qJQ$, and the "discriminants" d_{P^qQ}, d_{PQ^q}, and d_{PQ} all have the same quadratic character in $F = GF(q^2)$. We record these observations in the form of a proposition for frequent reference. The notation $P{\cdot}Q$ denotes the usual dot product.

Proposition 4.1.1 *Let (x, y, z) be a left-normalized representative of a point P and let $[u, v, w]$ be a right-normalized representative of a line Q. Let $d_{PQ} = xu_2 + yv_2 + zw_2$ as above.*

(i) Suppose $d_{PQ} \in F_S$*. Then* $PJQ \iff P^{\bullet}Q = 0$*, and* $PJQ^q \iff P^qJQ \iff P^{\bullet}Q^q = 0 \iff P^{q\bullet}Q = 0$*.*

(ii) Suppose $d_{PQ} \in F_N$*. Then* $PJQ \iff P^{\bullet}Q^q = 0 \iff P^{q\bullet}Q = 0$ *and* $PJQ^q \iff P^qJQ \iff P^{\bullet}Q = 0$*.*

(iii) Suppose $d_{PQ} = 0$*. Then the following are all equivalent:* PJQ*,* PJQ^q*,* P^qJQ*,* $P^{\bullet}Q = 0$*,* $P^{\bullet}Q^q = 0$*, and* $P^{q\bullet}Q = 0$*.*

■

Consider the points and lines of $\mathcal{H}(q^2)$ which have a normalized representative in V^* whose coordinates all lie in K. We show that these points and lines form a copy of $PG(2,q)$. For instance, if $(x,y,z) \in V^*$ with $x,y,z \in K$, then for any $a \in F$ we have $a \cdot (x,y,z) = a(x,y,z)$. Thus, $(x,y,z)\rho(xa,ya,za)$ for all $a \in F^*$. This shows that the ρ-equivalence class associated with such a point (or line) is actually a vector subspace of V (with $(0,0,0)$ removed). Moreover, if $P = (x,y,z)$ and $Q = [u,v,w]$ are in V^*, for $x,y,z,u,v,w \in K$, then $d_{PQ} = xu_2 + yv_2 + zw_2 = 0$. Thus PJQ if and only if $ux + vy + wz = 0$. Therefore, these points and lines form an isomorphic copy of $PG(2,q)$ embedded in $\mathcal{H}(q^2)$. We denote this subplane by π_0 and note that it is a *Baer subplane*, i.e. every line of $\mathcal{H}(q^2)$ must meet π_0 and dually, every point of $\mathcal{H}(q^2)$ must lie on a line of π_0. We additionally note that for an arbitrary point $P \in \mathcal{H}(q^2)$ and line Q of π_0, the discussion given above shows that PJQ if and only if $xu + yv + zw = 0$. Similarly, the dual statement also holds. Thus, where points and lines of π_0 are concerned, incidence in the Hughes plane is identical to incidence in the classical plane.

The following proposition regarding incidence in the Hughes plane will also prove to be helpful.

Proposition 4.1.2 *Let* $P = (x,y,z)$ *and* $Q = [u,v,w]$ *be a point and line of* $\mathcal{H}(q^2)$*, respectively. If* PJQ *and* PJQ^q *then either* P *or* Q *(or both) belong to* π_0*.*

Proof: If PJQ and PJQ^q then the equations on the right-hand side of both (4.4) and (4.5) are satisfied (again recalling that d_{PQ} and d_{PQ^q} have the same quadratic character in F). By adding these equations, we see that $d_{PQ} = xu_2 + yv_2 + zw_2 = 0$ and $xu_1 + yv_1 + zw_1 = 0$. Consider the vectors $[u_1, v_1, w_1]$ and $[u_2, v_2, w_2]$, noting that at least one is nonzero as $[u, v, w]$ is nonzero. If one vector is the zero vector, then $[u, v, w] = [u_1, v_1, w_1]$ or $[u, v, w] = [u_2\epsilon, v_2\epsilon, w_2\epsilon] = \epsilon \cdot [u_2, v_2, w_2]$, where $\epsilon \cdot [u_2, v_2, w_2]\rho[u_2, v_2, w_2]$. Hence, $Q = [u, v, w]$ is a line of π_0 in this case. If both $[u_1, v_1, w_1]$ and $[u_2, v_2, w_2]$ are nonzero, then they represent lines of π_0. If P is not a point of π_0, then it may lie on at most one line of the Baer subplane π_0. Thus if $P \notin \pi_0$, $[u_1, v_1, w_1]$ and $[u_2, v_2, w_2]$ represent the same line of π_0, since $PJ[u_1, v_1, w_1]$ and $PJ[u_2, v_2, w_2]$. Hence $[u_1, v_1, w_1] = \lambda[u_2, v_2, w_2]$ for some $\lambda \in K^*$. Therefore, $Q = [u, v, w] = [u_2(\lambda + \epsilon), v_2(\lambda + \epsilon), w_2(\lambda + \epsilon)] = (\lambda + \epsilon) \cdot [u_2, v_2, w_2]$, which is ρ-equivalent to $[u_2, v_2, w_2]$, is in π_0. ■

Notice that we obtain the same conclusion if PJQ and P^qJQ, since PJQ^q if and only if P^qJQ.

We now consider an element $A = (a_{i,j})$ of $GL(3, q)$ and define the analog of matrix multiplication on vectors in V^* when such vectors are viewed as three-tuples over N. For $(x, y, z) \in V^*$, we define a mapping, also denoted by A, from V^* to V^* via the rule

$$A : (x, y, z) \mapsto (a_{1,1}x + a_{2,1}y + a_{3,1}z, a_{1,2}x + a_{2,2}y + a_{3,2}z, a_{1,3}x + a_{2,3}y + a_{3,3}z).$$

Since all the entries of A are from K, all nearfield multiplication reduces to the usual field multiplication, thus we have no need of the operator $\cdot$ in this definition. We will freely denote the action of A on three-tuples over N by usual notation for matrix multiplication on the right. Since multiplication in N is associative and left-distributive, with center K, we see that $(a \cdot (x, y, z))A = a \cdot ((x, y, z)A)$ for all $a \in N$ and $(x, y, z) \in V^*$. Therefore, every element of $GL(3, q)$ induces a permutation of the points of $\mathcal{H}(q^2)$. Using Proposition 4.1.1, it is not difficult to see that elements of $GL(3,q)$ preserve the incidence relation J as well. Thus $GL(3,q)$ induces a collineation group of $\mathcal{H}(q^2)$, i.e. $PGL(3,q)$ is a collineation group of $\mathcal{H}(q^2)$. Collineations of $\mathcal{H}(q^2)$ which are induced by elements of $GL(3,q)$ will be called *linear*. Notice that every linear collineation of $\mathcal{H}(q^2)$ leaves the points and lines of π_0 invariant.

It is known that the full collineation group of $\mathcal{H}(q^2)$ is isomorphic to $PGL(3,q) \rtimes \mathrm{Aut}(N)$, where $\mathrm{Aut}(N)$ is the automorphism group of the nearfield N [55, 64]. It is also known that every perspectivity of π_0 may be extended to a perspectivity of $\mathcal{H}(q^2)$ [55, 64]. If $q = p^n$, for odd prime $p > 3$, the automorphism group of N was shown by Zassenhaus [65] (see also Section 17 of Foulser [28]) to be cyclic of order $2n$ with generator $\alpha : x \mapsto x^p$. As every element of $\mathrm{Aut}(N)$ is also a field automorphism of $GF(q^2)$, such elements must leave $GF(q)$ invariant (the unique subfield of order q). Thus, the collineations induced by $\mathrm{Aut}(N)$ leave the points and lines of π_0 invariant. Finally, notice that the Frobenius automorphism σ is the unique element of order two in $\mathrm{Aut}(N)$. We will use σ to denote the collineation of $\mathcal{H}(q^2)$ induced by the Frobenius automorphism, as well.

We emphasize that the left-normalized (right-normalized) vectors in V^* serve as representatives for points (lines) in both the classical plane and the Hughes plane. A version of the following lemma was proven by Kestenband [42] under restrictive hypotheses, although his method of proof is valid in a more general setting. We present the general result with a concise argument based on Propositions 4.1.1 and 4.1.2.

Lemma 4.1.3 *Let S be a set of left-normalized vectors which represent points in both $PG(2,q^2)$ and $\mathcal{H}(q^2)$ such that S is invariant under the Frobenius collineation σ. Let l be any right-normalized vector representing a line of both $PG(2,q^2)$ and $\mathcal{H}(q^2)$. Then $l \cap S$ has the same cardinality independent of the plane in which the points and line are viewed.*

Proof: If l is a line of π_0 then, as noted earlier, incidence with l is identical in the Hughes and classical plane.

Suppose l is not a line of π_0 and let $(x,y,z) \in S$. Then, by hypotheses, $(x^q, y^q, z^q) \in S$. Let $l = [u,v,w]$. From Proposition 4.1.1, $(x,y,z)J[u,v,w]$ implies that either $xu + yv + zw = 0$ or $xu^q + yv^q + zw^q = 0$ according to the discriminant condition found in that proposition. Thus either (x,y,z) or (x^q,y^q,z^q) lies on l in $PG(2,q^2)$. Notice that if both (x,y,z) and (x^q,y^q,z^q) lie on l in $PG(2,q^2)$, then by Proposition 4.1.1 (recall $d_{P^qQ} = (d_{PQ})^q$) we see that $(x,y,z)Jl$ and $(x^q,y^q,z^q)Jl$. Hence, by Proposition 4.1.2, $(x,y,z) \in \pi_0$, as $l \notin \pi_0$. Therefore, $(x^q,y^q,z^q) = (x,y,z)$, which shows that for each point of S incident with l in $\mathcal{H}(q^2)$, there corresponds a unique point of S incident with l in $PG(2,q^2)$.

Conversely, if (x,y,z) lies on l in $PG(2,q^2)$, i.e. $xu + yv + zw = 0$, then by Proposition 4.1.1 we see that either $(x,y,z)Jl$ or $(x^q,y^q,z^q)Jl$. If both (x,y,z) and (x^q,y^q,z^q) are incident with l in $\mathcal{H}(q^2)$, then by Proposition 4.1.2, $(x,y,z) \in \pi_0$, as $l \notin \pi_0$. Hence, $(x^q,y^q,z^q) = (x,y,z)$ and we conclude that for each point on l in $PG(2,q^2)$ there corresponds a unique point on l in $\mathcal{H}(q^2)$. Therefore,

$$|\{(x,y,z) \in S : (x,y,z)J[u,v,w]\}| = |\{(x,y,z) \in S : xu + yv + zw = 0\}|.$$

$\blacksquare$

There are certain configurations embedded in finite projective planes which are identifiable solely on the basis of the intersection sizes of the lines of the plane with the set of points comprising the configuration. Two such configurations of which we are interested are arcs (specifically ovals) and unitals. Lemma 4.1.3 gives the following immediate result.

Theorem 4.1.4 *Suppose the Frobenius automorphism leaves a set S of left-normalized vectors invariant. Then S represents an arc or a unital in the Hughes plane if and only if S represents an arc or a unital in the classical plane, respectively.*

$\blacksquare$

4.2 Known Unitals in the Hughes Plane

In answering the question of the presence of unitals in the Hughes plane, we note that the Hughes plane does not admit a unitary polarity (see [51, 54]). In the case $q = 3$, Brouwer [15] used a computational method involving coding theory to discover four unitals embedded in $\mathcal{H}(9)$. As yet, no one has generalized his findings to arbitrary odd prime powers, though Brouwer has subsequently provided a group theoretic description for one of the unitals, labelled E.8, as the union of certain orbits of a particular subgroup of $\mathrm{Aut}(\mathcal{H}(9))$ [16]. While we have attempted, and plan to continue to attempt, to find an infinite family containing the E.8 unital, there is reason to believe that the presence of this unital is merely an anomaly due to the "relatively" large automorphism group (the symmetric group on three letters) of the exceptional nearfield of order nine.

The techniques of Brouwer were not exhaustive, however, even for the case of $\mathcal{H}(9)$. Absent from his original list is the unital obtained by Rosati [56], which has provided the only known infinite family of unitals in $\mathcal{H}(q^2)$. Rosati's idea was to take the equation of a classical unital in $PG(2, q^2)$ and show that the points of $\mathcal{H}(q^2)$ satisfying that equation must form a unital in the Hughes plane. In particular, he showed that

$$U_R = \{(x, y, z) : x^{q+1} + y^{q+1} + z^{q+1} = 0\} \tag{4.6}$$

defines a unital in $\mathcal{H}(q^2)$ [56]. Notice that the equation defining U_R is that of the hermitian form associated with the identity matrix, as with the unital given by (1.6). Kestenband [42] has studied a class of projectively equivalent unitals in $\mathcal{H}(q^2)$, one of which is the Rosati unital. These unitals consist of the absolute (Hughes) points of hermitian forms associated with symmetric matrices over $K = GF(q)$. Kestenband's method of proof is a straight forward application of his version of Theorem 4.1.3, as such sets of points are left invariant by the Frobenius collineation. Kestenband [42] also showed that these unitals are non-isomorphic as designs to the classical unital embedded in the classical plane. We refer to any unital from this projective equivalence class as a *classical-Rosati* unital.

Abatangelo and Larato [2] have determined the linear collineation group leaving the Rosati unital invariant. As every linear collineation leaves π_0 invariant, they point out that a linear collineation stabilizing U_R must leave the set $C = \pi_0 \cap U_R$ invariant as well. We see that $C = \{(x, y, z) \in \pi_0 : x^2 + y^2 + z^2 = 0\}$. Notice that C is the set of absolute points of the nondegenerate quadratic form associated with the symmetric bilinear form represented by the identity matrix; i.e., C is a conic of π_0. The linear collineation group of U_R must then be isomorphic to a subgroup of $PGL(2, q)$ (see Section 1.3). Abatangelo and Larato show that every linear collineation of π_0 leaving C invariant may be extended to a collineation of $\mathcal{H}(q^2)$ leaving U_R invariant [2]. Therefore, the linear collineation group of any classical-Rosati unital is isomorphic to $PGL(2, q)$, hence has order $q(q^2 - 1)$.

We now describe the orbit structure of the classical-Rosati unitals under the linear collineation group isomorphic to $PGL(2, q)$, as well as the orbit structure under the collineation group isomorphic to $PGL(2, q) \times \langle\sigma\rangle$, where σ is the Frobenius collineation. In the proof, we represent a classical-Rosati unital as the absolute points of a different (but equivalent) hermitian form. In doing so, we hope to demonstrate the advantage of having explicit coordinates with which to describe the unital. The proof is rather lengthy and quite technical. In addition, the results of Section 4.3 will provide a helpful base on which to build. Therefore, the proof of Theorem 4.2.1 will be reserved for the appendix.

Theorem 4.2.1 *Let U be a classical-Rosati unital and let C be the conic $U \cap \pi_0$. Let G be the linear collineation group leaving U invariant; i.e., $G \cong PGL(2, q)$. For $q \equiv 1 \pmod 4$, U consists of three orbits under G, namely the points of C, the $q(q^2-1)/2$ points off C which lie on secant lines to C, and the remaining $q(q^2-1)/2$ points which do not lie on secant lines to C.*

For $q \equiv 3 \pmod 4$, U consists of four orbits under G. The points of C and the points off C which lie on secant lines to C are again orbits of G. The points which do not lie on secants to C are split into two orbits, each of size $q(q^2-1)/4$. Moreover, these latter two orbits are joined by the Frobenius collineation σ, giving one orbit of size $q(q^2-1)/2$ for the group $G \times \langle\sigma\rangle$.

■

There are certain advantages to working with a classical-Rosati unital in the form described by Rosati as in (4.6). One advantage is the way in which incidence in the Hughes plane relates directly to the issue of satisfying the equation $x^{q+1} + y^{q+1} + z^{q+1} = 0$. We will capitalize on this relationship in determining the patterns formed by the feet of points off U_R. In order to do so, we first note that in the discussion preceding Proposition 4.1.1 it was required that (x, y, z) be a left-normalized representative of the point P and $[u, v, w]$ be a right-normalized representative of the line Q. Notice that these requirements had no bearing on the proofs of Propositions 4.1.1 and 4.1.2, but merely served to make d_{PQ} well-defined. One could require that the representatives of both P and Q be left-normalized and obtain the same results. Throughout the remainder of this section, we use this alternative method of normalization, and freely make reference to Proposition 4.1.1 and Proposition 4.1.2. Of interest in this discussion will be the set

$$O = \{(x, y, z) \in \mathcal{H}(q^2) : x^2 + y^2 + z^2 = 0\}. \tag{4.7}$$

As the set of points satisfying $x^2 + y^2 + z^2 = 0$ in $PG(2, q^2)$ form a conic and the Frobenius collineation leaves this set invariant, we see that O is an oval in $\mathcal{H}(q^2)$. We note that $O \cap \pi_0 = C$.

Lemma 4.2.2 *Consider a left-normalized vector $P = (x, y, z) = [x, y, z]$ representing both a point and a line of $\mathcal{H}(q^2)$. Let $d_P = d_{PP} = xx_2 + yy_2 + zz_2$ as defined in Lemma 4.1.1.*

(i) Suppose $d_P \in F_S$. Then $PJP \iff P \in O$, and $PJP^q \iff P^qJP \iff P \in U_R$.

(ii) Suppose $d_P \in F_N$. Then $PJP \iff P \in U_R$, and $PJP^q \iff P^qJP \iff P \in O$.

(iii) Suppose $d_P = 0$. Then the following are all equivalent: PJP, PJP^q, P^qJP, $P \in U_R$, and $P \in O$. If one (and hence all) of these conditions hold in this case, then $P \in \pi_0$. Moreover, $PJP \iff P \in C$ in this case.

Proof: Parts (i), (ii), and the first statement in (iii) follow directly from Proposition 4.1.1. The second statement in (iii) follows directly from Proposition 4.1.2. The final statement in (iii) then follows from the previous statement and the fact that $C = \pi_0 \cap O$. ■

Corollary 4.2.3 *Assume the same notation as given in Lemma 4.2.2.*

(1) $U_R \cap O = C$.

(2) Suppose $P \in O \setminus C$. Then $d_P \neq 0$. In fact, $d_P \in F_S \iff q \equiv 3 \pmod 4$, and $d_P \in F_N \iff q \equiv 1 \pmod 4$.

(3) Suppose $P \in C$. Then $d_P = 0$.

Proof: (1) Clearly, $C \subseteq U_R \cap O$. The reverse inclusion is easily shown as a consequence of Lemma 4.2.2, and the fact that $\pi_0 \cap O = C$.

(2) Using the fact that $x_2 = \frac{x - x^q}{2\epsilon}$ and similarly for y_2 and z_2, one sees immediately that $2\epsilon d_P = P{\cdot}P - P{\cdot}P^q$, where again $\cdot$ denotes the usual dot product. Suppose now that $P \in O \setminus C$. Then $P{\cdot}P = 0$, but $P{\cdot}P^q \neq 0$ as $P \notin U_R$ from part (1). Hence $2\epsilon d_P \neq 0$, implying $d_P \neq 0$. In fact, since $P{\cdot}P^q = x^{q+1} + y^{q+1} + z^{q+1} \in K \setminus \{0\}$, we see that $P{\cdot}P^q \in F_S$ and hence $2\epsilon d_P \in F_S$. Thus ϵ and d_P have the same quadratic character in F. The result now follows since $\epsilon = \gamma^{(q+1)/2}$, where γ is a primitive element of F.

(3) We again use the fact that $2\epsilon d_P = P^{\bullet}P - P^{\bullet}P^q$. If $P \in C$, then $P^{\bullet}P = 0$ and $P^{\bullet}P^q = P^{\bullet}P = 0$, thereby implying $2\epsilon d_P = 0$. Since $2\epsilon \neq 0$, we have $d_P = 0$.

■

Using Lemma 4.1.3, we see that if $(x, y, z) \in U_R$, then $[x, y, z]$ represents a tangent line to U_R in $\mathcal{H}(q^2)$ since the line represented by this vector in $PG(2, q^2)$ is clearly a tangent line to $\mathcal{U}$ (see Section 1.4). This implies that $[x^q, y^q, z^q]$ is also a tangent line to U_R in $\mathcal{H}(q^2)$ as the Frobenius collineation σ is an automorphism of $\mathcal{H}(q^2)$ leaving U_R invariant. Similarly, if $(x, y, z) \in O$, then $[x, y, z]$ and $[x^q, y^q, z^q]$ represent tangent lines to O in $\mathcal{H}(q^2)$. The following lemma sorts out the points of tangency for these tangent lines.

Lemma 4.2.4 *Let P be a point represented by a left-normalized vector (x, y, z), and let d_P be defined as in Lemma 4.2.2.*
(i) Suppose $P \in C$. Then the unique tangent line to C at the point P is $[x, y, z] = [x^q, y^q, z^q]$. In fact, $[x, y, z]$ is also the unique tangent line to O at P and the unique tangent line to U_R at P.
(ii) Suppose $P \in O \setminus C$. Then the unique tangent line to O at P is $[x^q, y^q, z^q]$ or $[x, y, z]$, accordingly as q is congruent to 1 or $3 \pmod 4$.
(iii) If $P \in U_R \setminus C$. Then the unique tangent line to U_R at P is $[x^q, y^q, z^q]$ or $[x, y, z]$, accordingly as $d_P \in F_S$ or $d_P \in F_N$.

Proof: These results follow immediately from the above discussion, Lemma 4.2.2, and Corollary 4.2.3. Note that $d_P \neq 0$ for any point $P \in (U_R \setminus C) \cup (O \setminus C)$ from Corollary 4.2.3 and the fact that $2\epsilon d_P = P^{\bullet}P - P^{\bullet}P^q$. ■

We are now ready to show that feet of any point off U_R in $\mathcal{H}(q^2)$ lie on a pair of lines.

Theorem 4.2.5 *Let (a, b, c) be a left-normalized representative of a point of $\mathcal{H}(q^2) \setminus U_R$. Then the feet of (a, b, c) lie on the lines $[a, b, c]$ and $[a^q, b^q, c^q]$. The feet of points of $\pi_0 \setminus U_R$ are thus collinear. Moreover, if $(a, b, c) \in \mathcal{H}(q^2) \setminus (\pi_0 \cup U_R)$ and (x, y, z) is* *one of the feet of* (a,b,c)*, then* (x,y,z) *lies on the line* $[a,b,c]$ *if and only if* $[x,y,z]$ *is the tangent line to* U_R *at* (x,y,z)*.*

Proof: Let (x,y,z) be one of the feet of (a,b,c), i.e., the tangent line at (x,y,z) passes through (a,b,c). From Lemma 4.2.4, this says that either $(a,b,c)J[x,y,z]$ or $(a,b,c)J[x^q,y^q,z^q]$. By the symmetry of J and since the Frobenius automorphism preserves the incidence J, we find that either $(x,y,z)J[a,b,c]$ or $(x,y,z)J[a^q,b^q,c^q]$, respectively. If (a,b,c) represents a point of $\pi_0 \setminus U_R$, then $a,b,c \in K$. Thus $[a,b,c] = [a^q,b^q,c^q]$ and the feet are collinear.

Suppose $(a,b,c) \in \mathcal{H}(q^2) \setminus (\pi_0 \cup U_R)$. If (x,y,z) is one of the feet of (a,b,c) lying on $[a,b,c]$, then by symmetry $(a,b,c)J[x,y,z]$. To see that $[x,y,z]$ is tangent to the unital at (x,y,z), suppose that $[x^q,y^q,z^q]$ is the tangent at (x,y,z), giving $(a,b,c)J[x^q,y^q,z^q]$. From Proposition 4.1.2, we see that either (a,b,c) or $[x,y,z]$ belongs to π_0. As the former is contradictory, we see that $[x,y,z] \in \pi_0$; hence $[x^q,y^q,z^q] = [x,y,z]$. Therefore, $[x,y,z]$ is the unique tangent to U_R at (x,y,z).

One similarly shows that if (x,y,z) lies on $[a^q,b^q,c^q]$, then $[x^q,y^q,z^q]$ is the unique tangent to U_R at (x,y,z). ■

We note that if (u,v,w) is the intersection point of $[a,b,c]$ and $[a^q,b^q,c^q]$, then by Proposition 4.1.2 (u,v,w) is a point of π_0.

The points of π_0 are not the only points off U_R which have collinear feet. As additional evidence that the oval O shares a special relationship with U_R, we now show that the points of $O \setminus C$ have this property.

Corollary 4.2.6 *Let* (a,b,c) *be a left-normalized representative of a point of* $O \setminus C$*. The feet of* (a,b,c) *are collinear on*

$$\begin{cases} [a,b,c] & \textit{for} \quad q \equiv 1 \pmod 4 \\ [a^q,b^q,c^q] & \textit{for} \quad q \equiv 3 \pmod 4 \end{cases}.$$

That is to say, the feet of (a,b,c) *lie on the* q*th power of the* O*-tangent at* (a,b,c)*.*

Proof: From Lemma 4.2.4 we saw that the tangent line to O at a point $(a,b,c) \in O$ is either $[a,b,c]$ or $[a^q,b^q,c^q]$, depending on the parity of q. Moreover, from Theorem 4.2.5 the feet of a point off U_R lie on the union of the lines $[a,b,c]$ and $[a^q,b^q,c^q]$. We first consider the case when $q \equiv 3 \pmod 4$; i.e., $[a,b,c]$ is the line tangent to O at the point $(a,b,c) \in O \setminus C$. Suppose (x,y,z) is one of the feet of (a,b,c) and $(x,y,z)J[a,b,c]$. From Theorem 4.2.5, we see that the unique tangent to U_R at the point (x,y,z) is $[x,y,z]$, i.e., $(a,b,c)J[x,y,z]$. But the line joining (x,y,z) to (a,b,c) is unique; hence, $[a,b,c]\rho[x,y,z]$. This implies $(a,b,c)\rho(x,y,z)$, where $(a,b,c) \in O \setminus C$ and $(x,y,z) \in U_R$. As $O \cap U_R = C$, one has a contradiction. Thus the feet of (a,b,c) must all lie on the line $[a^q,b^q,c^q]$.

Similarly, if $q \equiv 1 \pmod 4$, i.e., $[a^q,b^q,c^q]$ is the line tangent to O at the point (a,b,c), then the feet of (a,b,c) are collinear on the line $[a,b,c]$. ■

4.3 A New Class of Unitals in the Hughes Plane

In the previous section we saw that the points in the Hughes plane which satisfy the "standard" equation of a classical unital in $PG(2,q^2)$ also form a unital in $\mathcal{H}(q^2)$, based on the work of Rosati [56] and Kestenband [42]. In this section we construct a class of unitals in the Hughes plane which are analogs of the Buekenhout-Metz unitals in $PG(2,q^2)$ in the sense that the points may be described in a manner similar to (2.3) as found in [8]. As with the BM-unitals in the classical plane, we will find a classical-Rosati unital represented as a particularly "nice" member of this new class of unitals.

As in the case of the classical-Rosati unital, we restrict our consideration to those unitals which are left invariant by the Frobenius automorphism. That is to say, we rely on Theorem 4.1.4 to show that certain known unitals in $PG(2,q^2)$ correspond to unitals in $\mathcal{H}(q^2)$. We begin by considering sets of points in $PG(2,q^2)$ of a form quite similar to that of (2.3), namely

$$\{(1,y,ay^2+by^{q+1}+t\eta) : y \in F = GF(q^2), t \in K = GF(q)\} \cup \{(0,0,1)\}, \quad (4.8)$$

where a, b, and η are fixed elements of F, with $\eta \neq 0$. If such a set is left invariant by the Frobenius automorphism, we find that $(1, y, ay^2 + by^{q+1} + t\eta)^q = (1, y^q, a^q y^{2q} + b^q y^{q+1} + t\eta^q)$ must be some point $(1, y', a(y')^2 + b(y')^{q+1} + t'\eta)$, for some $y' \in F$ and some $t' \in K$. Comparing the second coordinates gives $y' = y^q$, hence comparing the third coordinates gives

$$(a^q - a)y^{2q} + (b^q - b)y^{q+1} + t\eta^q - t'\eta = 0. \tag{4.9}$$

By multiplying (4.9) by η^q and subtracting the qth power of the resulting equation, one obtains

$$(a^q - a)(y^{2q}\eta^q + y^2\eta) + (b^q - b)y^{q+1}(\eta^q + \eta) + t(\eta^{2q} - \eta^2) = 0.$$

As this equation must hold for all $y \in F$ and $t \in K$, by substituting $y = 0$ and $t = 1$ we find that $\eta^{2q} - \eta^2 = 0$. Thus,

$$(a^q - a)(y^{2q}\eta^q + y^2\eta) + (b^q - b)y^{q+1}(\eta^q + \eta) = 0, \tag{4.10}$$

for all $y \in F$, where either $\eta^q - \eta = 0$ or $\eta^q + \eta = 0$. Suppose $\eta^q - \eta = 0$; i.e., $\eta \in K$ and hence (4.8) is of a form equivalent to (2.3). By substituting $y = 1$ and $y = \epsilon$ in (4.10), one obtains two equations which when solved give $a^q - a = 0$ and $b^q - b = 0$. Therefore, $a, b \in K$. Bearing in mind that our primary concern is to obtain a unital, we note that the discriminant condition in (2.5) cannot be satisfied if both a and b are elements of $K = GF(q)$. Therefore, one cannot obtain (the "affine" points of) a BM-unital which is invariant under the Frobenius automorphism from the point set (4.8) in the case when $\eta^q - \eta = 0$. We now suppose that $\eta^q + \eta = 0$; i.e., η belongs to the multiplicative coset $K\epsilon$. Additionally, without loss of generality, we may take $\eta = \epsilon$ in (4.8). From (4.10), it is immediate that $a^q - a = 0$, since $y^{2q}\eta^q + y^2\eta = (y^2 - y^{2q})\epsilon$ is nonzero for some choice of y in F. We establish the notation

$$U_{(a,b)} = \{(1, y, ay^2 + by^{q+1} + t\epsilon) : y \in F, t \in K\} \cup \{(0, 0, 1)\}, \tag{4.11}$$

for fixed $a \in K$ and $b \in F$, in order to distinguish these sets from those described in (2.3).

One may show that $U_{(a,b)}$ is indeed a Buekenhout-Metz unital subject to certain restrictions on a and b. Namely, by writing $b = b_1 + b_2\epsilon$ and $y = y_1 + y_2\epsilon$ for $b_1, b_2, y_1, y_2 \in K$ and using $a \in K$, we see that the "real" part of $ay^2 + by^{q+1} + t\epsilon$ is a binary form in y_1 and y_2 given by

$$(a + b_1)y_1^2 + (a - b_1)\omega y_2^2. \tag{4.12}$$

(Recall that $\omega = \epsilon^2$.) Thus a point (x, y, z) belongs to $U_{(a,b)}$ if and only if

$$xz_1 = (a + b_1)y_1^2 + (a - b_1)\omega y_2^2, \tag{4.13}$$

where $z = z_1 + z_2\epsilon$ for $z_1, z_2 \in K$. Therefore, in a copy of $PG(4, q)$ with homogeneous coordinates (x, y_1, y_2, z_1, z_2), where $x = 0$ is the equation of the hyperplane at infinity, the set $U_{(a,b)}$ corresponds to a cone over a quadric whose points are determined by (4.13). Now $U_{(a,b)}$ is a BM-unital if and only if the binary form in (4.12) is irreducible, which occurs if and only if $4\omega(b_1^2 - a^2) \in K_N$. As $b_1 = (b^q + b)/2$, we are left with a discriminant condition quite similar to that given in (2.5). In fact, the discriminant condition can be obtained from (2.5) by considering the transformation which maps $U_{(a,b)}$ to $U_{(a/\epsilon, b/\epsilon)}$, for $a \in K$, by dividing the third coordinate by ϵ and permuting the coordinates. Finally, as ω is a nonsquare in K, $U_{(a,b)}$ is a Buekenhout-Metz unital if and only if $b_1^2 - a^2 \in K_S$, for $b = b_1 + b_2\epsilon$, $b_1, b_2 \in K$. It should be remarked that we originally showed that (4.11) was a BM-unital using the group theoretic characterization that was proved in Section 3.2. This involved first showing that $U_{(a,b)}$ was a unital and then determining the linear collineation group which leaves it invariant in a manner which mimics the work of Baker and Ebert in Section 3 of [8].

From Theorem 4.1.4, we find that $U_{(a,b)}$, for $b = b_1 + b_2\epsilon \in F$, $a, b_1, b_2 \in K$, with $b_1^2 - a^2 \in K_S$, is a unital in $\mathcal{H}(q^2)$ as well. Notice that the third coordinate of an "affine" point in $U_{(a,b)}$ has the form $ay^2 + by^{q+1} + t\epsilon$, for some $y \in F$ and $t \in K$, which may be expressed as

$$ay^2 + b_1 y^{q+1} + (b_2 y^{q+1} + t)\epsilon.$$

Further note that $b_2 y^{q+1} + t$ ranges over K as y ranges over F and t ranges over K. Therefore, the set $U_{(a,b)}$ contains the same q^3+1 points as the set $U_{(a,b_1)}$. Without loss of generality, we will henceforth consider unitals of the form $U_{(a,b)}$ for $a, b \in K$ for which $b^2 - a^2 \in K_S$. We immediately see that with $a = 0$, and $b \in K$, the points of $U_{(a,b)}$ satisfy the hermitian form $xz^q + x^q z - 2by^{q+1} = 0$. Thus, $U_{(0,b)}$ is a classical-Rosati unital for any $b \in K^*$.

In order to determine the linear collineation group of $\mathcal{H}(q^2)$ which leaves $U_{(a,b)}$ invariant, we first note that $U_{(a,b)} \cap \pi_0$ is the set $\{(x,y,z) \in \pi_0 : xz - (a+b)y^2 = 0\}$. This set clearly forms a conic in π_0 (as $a + b \neq 0$) which we denote by $C_{a,b}$.

Theorem 4.3.1 *Let G be the subgroup of $Aut(\mathcal{H}(q^2))$ which consists of linear collineations leaving the unital $U_{(a,b)}$ invariant. Then,* $o(G) = \begin{cases} q(q^2-1) & \text{if} \quad a = 0 \\ q(q-1) & \text{if} \quad a \neq 0 \end{cases}$. *Moreover, if $a \neq 0$ then G fixes the point $P_\infty = (0,0,1)$.*

Proof: As G leaves π_0 invariant, it must leave invariant the conic $C_{a,b} = \{(x,y,z) \in \pi_0 : xz - (a+b)y^2 = 0\}$. Thus G is isomorphic to a subgroup of $PGL(2,q)$ (see Section 1.3). Therefore, the elements of G have a form similar to that given in (1.5), namely,

$$\begin{pmatrix} c^2 & cd & d^2(a+b) \\ 2ce & cf+ed & 2df(a+b) \\ \frac{e^2}{a+b} & \frac{ef}{a+b} & f^2 \end{pmatrix}, \text{ where } c,d,e,f \in K, \ cf - de \neq 0. \qquad (4.14)$$

When $a = 0$, it has been shown above that $U_{(a,b)}$ is a classical-Rosati unital. By the work of Abatangelo and Larato [2], G is isomorphic to $PGL(2,q)$, hence the result holds.

If $a \neq 0$, we proceed to demonstrate that G must fix the point $P_\infty = (0,0,1)$. By way of contradiction, suppose that g is an element of G, represented by a matrix of the form shown above, such that $P_\infty^g \neq P_\infty$. We see immediately that e in (4.14) is nonzero. We then set $e = 1$ in order to obtain a unique matrix representative of g. Consider a point $P \in U_{(a,b)}$ of the form $P = (1, y, (a+b)y^2 + (a+b)\epsilon)$ for some $y \in K$, $y \neq -c$. We see that

$$P^g = ((y+c)^2 + \epsilon, (y+c)(fy+d) + f\epsilon, (a+b)[(fy+d)^2 + f^2\epsilon]).$$

Let $A = y + c$ and $B = fy + d$ for ease of computation, noting that $A, B \in K$ and $A \neq 0$. Then, from the definition of ρ-equivalence, P^g may be represented by the normalized vector

$$\left(1, \frac{AB + f\epsilon^\theta}{A^2 + \epsilon^\theta}, \frac{(a+b)[B^2 + f^2\epsilon^\theta]}{A^2 + \epsilon^\theta}\right),$$

where $\theta = 1$ or q depending on whether $A^2 + \epsilon$ is in F_S or F_N, respectively. We demonstrate only the case when $\theta = 1$, as the case $\theta = q$ is obtained by replacing ϵ with $-\epsilon$ in the following tedious computation.

As $P^g \in U_{(a,b)}$, it must also have the form $(1, y', a(y')^2 + b(y')^{q+1} + s\epsilon)$ for some $y' \in F$ and $s \in K$. Notice that $y' = \frac{AB + f\epsilon^\theta}{A^2 + \epsilon^\theta}$. Comparing the third coordinates of these left-normalized representatives of P^g, we obtain

$$a\left(\frac{AB + f\epsilon^\theta}{A^2 + \epsilon^\theta}\right)^2 + b\left(\frac{AB + f\epsilon^\theta}{A^2 + \epsilon^\theta}\right)^{q+1} + s\epsilon - \frac{(a+b)[B^2 + f^2\epsilon^\theta]}{A^2 + \epsilon^\theta} = 0.$$

Multiplying through by $(A^2 + \epsilon)(A^2 + \epsilon)^{q+1} = (A^2 + \epsilon)^2(A^2 - \epsilon)$, dividing by ϵ, and grouping like terms gives

$$-a(B - fA)^2(A^2 - \epsilon) + b(B^2 - f^2A^2)(A^2 + \epsilon) + s(A^4 - \omega)(A^2 + \epsilon) = 0.$$

(Recall $\epsilon^2 = \omega$.) Noting that $\{A^2, \epsilon\}$ forms a basis for F over K, we separate this equation in terms of this basis:

$$-a(B - fA)^2 + b(B^2 - f^2A^2) + s(A^4 - \omega) = 0$$

$$a(B - fA)^2 + b(B^2 - f^2A^2) + s(A^4 - \omega) = 0.$$

Subtracting these gives $a(B - fA)^2 = 0$. Since $a \neq 0$, we have

$$0 = B - fA = (fy + d) - f(y + c) = d - fc.$$

But a matrix described by (4.14) must have $cf - de \neq 0$, a contradiction.

Thus every element of G must fix P_∞, hence is representable by a matrix of the form given in (4.14) with $e = 0$, $c \neq 0$, and $f \neq 0$. Taking $c = 1$ to obtain a unique representative for each element of G, there are $q - 1$ choices for f and q choices for d, giving $q(q-1)$ possible collineations in G. For such a collineation g, we see that for $y \in F$ and $t \in K$

$$(1, y, ay^2 + by^{q+1} + t\epsilon)^g = (1, d + fy, a(d + fy)^2 + b(d + fy)^{q+1} + bdf(y - y^q) + f^2t\epsilon),$$

where $bdf(y - y^q) \in K\epsilon$. Therefore every element of G leaves $U_{(a,b)}$ invariant, giving $o(G) = q(q-1)$. ∎

As in the case of Buekenhout-Metz unitals in $PG(2, q^2)$, the linear collineation group leaving $U_{(a,b)}$ invariant and fixing P_∞ may be described in terms of a Sylow p-subgroup and a cyclic subgroup.

Theorem 4.3.2 *Let G_0 be the stabilizer of the point P_∞ in the group G leaving $U_{(a,b)}$ invariant, as in Theorem 4.3.1. Then, $G_0 = S \rtimes M$ where S is an elementary abelian group of order q and M is cyclic of order $q - 1$.*

The orbits of G_0 acting on $U_{(a,b)}$ are $\{P_\infty\}$, $C_{a,b} \setminus \{P_\infty\}$, $\{(1, y, (a+b)y^2 + s\epsilon) : y \in K, s \in K_S\}$, $\{(1, y, (a+b)y^2 + t\epsilon) : y \in K, t \in K_N\}$, and O_t for all $t \in K$, where O_t is the orbit $(1, \gamma, a\gamma^2 + b\omega + t\epsilon)^{G_0}$ for γ a primitive element of F.

Proof: We have seen that elements of G_0 may be written in the form

$$\begin{pmatrix} 1 & d & d^2(a+b) \\ 0 & f & 2df(a+b) \\ 0 & 0 & f^2 \end{pmatrix},$$

for $d, f \in K$, $f \neq 0$. Let S denote those elements of G_0 for which $f = 1$, i.e., $S = \{\psi_d : d \in K\}$, where

$$\psi_d = \begin{pmatrix} 1 & d & d^2(a+b) \\ 0 & 1 & 2d(a+b) \\ 0 & 0 & 1 \end{pmatrix}.$$

Notice that $\psi_d \psi_{d'} = \psi_{d+d'} = \psi_{d'} \psi_d$ and $|S| = q = p^n$. Thus S is the Sylow p-subgroup of G_0 and S is abelian. As $(\psi_d)^p = \psi_{pd} = \psi_0$ is the identity, for any $d \in K$, S is elementary abelian.

Let $M = \{\mu_f \in G_0 : f \in K^*\}$, where

$$\mu_f = \begin{pmatrix} 1 & 0 & 0 \\ 0 & f & 0 \\ 0 & 0 & f^2 \end{pmatrix}.$$

Notice that M is a cyclic group of order $q-1$ and $M \cap S = \{Id\}$. Moreover, as $\mu_f^{-1} \psi_d \mu_f = \psi_{fd}$, we see that M normalizes S. Hence $G_0 = S \rtimes M$, by an order argument.

As $PGL(2,q)$ acts triply-transitively on the points of a conic in $PG(2,q)$, G_0 has $C_{a,b} \setminus \{P_\infty\}$ as one of its orbits. The orbit of G_0 containing $(1,0,\epsilon)$ is the set $\{(1, d, (a+b)d^2 + f^2\epsilon) : d, f \in K, f \neq 0\}$ and that of $(1, 0, \omega\epsilon)$ is $\{(1, d, (a+b)d^2 + f^2\omega\epsilon) : d, f \in K, f \neq 0\}$. Notice that these two orbits are distinct, each having size $q(q-1)/2$, and their union consists of all points of $U_{(a,b)}$ which lie on lines that are secant to $C_{a,b}$ and pass through the point P_∞. The orbits are distinguished by the imaginary part of the third coordinate being a square or nonsquare in K.

For each $t \in K$, we define $P_t = (1, \gamma, a\gamma^2 + b\omega + t\epsilon)$ where γ is a primitive element of F. (Recall that $\omega = \gamma^{q+1}$.) Let O_t be the orbit of P_t under G_0, for each $t \in K$. Notice that

$$O_t = \{(1, d + f\gamma, a(d+f\gamma)^2 + b(d+f\gamma)^{q+1} + bdf(\gamma - \gamma^q) + f^2 t\epsilon) : d, f \in K, f \neq 0\},$$

where $bdf(\gamma - \gamma^q) + f^2 t\epsilon \in K\epsilon$. We see that O_t consists of $q(q-1)$ distinct points since $d + f\gamma$ takes on $q(q-1)$ distinct values in F, as $\{1, \gamma\}$ forms a basis of F over K. By way of contradiction suppose that $O_t \cap O_s$ is nonempty for $t \neq s$. Any point in this intersection may be written as both

$$(1, d + f\gamma, a(d + f\gamma)^2 + b(d + f\gamma)^{q+1} + bdf(\gamma - \gamma^q) + f^2 t\epsilon)$$

and

$$(1, d' + f'\gamma, a(d' + f'\gamma)^2 + b(d' + f'\gamma)^{q+1} + bd'f'(\gamma - \gamma^q) + (f')^2 s\epsilon),$$

for some choices of $d, d' \in K$ and $f, f' \in K^*$. Notice that $d + f\gamma = d' + f'\gamma$, which implies that $d = d'$ and $f = f'$ by a basis argument. Comparing the third component then gives the contradiction that $t = s$, as $f \neq 0$. Therefore, the O_t's partition the remaining $q^2(q-1)$ points of $U_{(a,b)}$ into q orbits of size $q(q-1)$. ■

We turn now to the subject of projective equivalence among unitals in $\mathcal{H}(q^2)$ described by $U_{(a,b)}$. Recall that the collineation group of $\mathcal{H}(q^2)$ is isomorphic to $PGL(3,q) \rtimes \mathrm{Aut}(N)$, where elements of $\mathrm{Aut}(N)$ have the form $\varrho : x \to x^{p^i}$ for $i \in \{1, \ldots 2n\}$, if $q = p^n$. It has been noted that $U_{(0,b)}$, for any $b \in K^*$, is a classical-Rosati unital; hence, all such unitals are projectively equivalent by Kestenband [42]. Notice that $U_{(0,b)}$ cannot be projectively equivalent to $U_{(a',b')}$ with $a' \neq 0$, since the linear automorphism group of the latter must fix P_∞ while that of the former does not.

Suppose ψ is a collineation in $PGL(3,q) \rtimes \mathrm{Aut}(N)$ which maps the unital $U_{(a,b)}$ to the unital $U_{(a',b')}$, where a and a' are nonzero. In order to see that ψ must fix $P_\infty = (0,0,1)$, let G be the linear automorphism group of $U_{(a,b)}$ and G' that of $U_{(a',b')}$. Notice that the conjugate $\psi^{-1}G\psi$ leaves $U_{(a',b')}$ invariant and fixes P_∞^ψ. In particular, $\psi^{-1}G\psi \leq G'$. By Theorem 4.3.1, $o(G) = o(G')$; hence $o(G') = o(\psi^{-1}G\psi)$. Therefore, $\psi^{-1}G\psi = G'$. As G' has P_∞ as its only fixed point, $P_\infty^\psi = P_\infty$. Moreover, the unique tangent line to $U_{(a,b)}$ (and $U_{(a',b')}$) at P_∞ must be left invariant by ψ. Notice that this line has coordinates $[1,0,0]$.

One may also assume that ψ fixes the point $(1,0,0) \in C_{a,b} \cap C_{a',b'}$, by the following reasoning. Since G' is transitive on $C_{a',b'} \setminus \{P_\infty\}$, there exists an element $\psi' \in G'$ mapping $(1,0,0)^\psi$ to $(1,0,0)$. One may then take $\psi\psi'$ as the collineation from $U_{(a,b)}$ to $U_{(a',b')}$, where $\psi\psi'$ fixes the point $(1,0,0)$. Therefore, without loss of generality, ψ acts according to the rule

$$(x,y,z)^\psi = (x^\varrho, y^\varrho, z^\varrho)\begin{pmatrix} 1 & 0 & 0 \\ 0 & e & h \\ 0 & 0 & f \end{pmatrix}, \text{ where } \varrho \in \ \mathrm{Aut}(N) \text{ and } e,f,h \in K,\ ef \neq 0.$$

For a point $P = (1, y, ay^2 + by^{q+1} + t\epsilon) \in U_{(a,b)}$, we see that

$$P^\psi = (1, ey^\varrho, a^\varrho f y^{2\varrho} + b^\varrho f (y^\varrho)^{q+1} + hy^\varrho + ft^\varrho \epsilon^\varrho).$$

As P^ψ must be representable as $(1, y', a'(y')^2 + b'(y')^{q+1} + s\epsilon)$, we see first that $y' = ey^\varrho$. Hence,

$$(b'e^2 - b^\varrho f)(y^\varrho)^{q+1} + (a'e^2 - a^\varrho f)y^{2\varrho} - hy^\varrho + (s - ft^\varrho)\epsilon^\varrho = 0. \tag{4.15}$$

Substituting $y = 0$ gives $s = ft^\varrho$. By adding and subtracting the equations obtained by substituting $y^\varrho = 1$ and $y^\varrho = -1$, we obtain $b'e^2 - b^\varrho f + a'e^2 - a^\varrho f = 0$ and $h = 0$, respectively. Thus (4.15) has the form $(b'e^2 - b^\varrho f)((y^\varrho)^{q+1} - y^{2\varrho}) = 0$. When $y^\varrho = \epsilon$, $(y^\varrho)^{q+1} - y^{2\varrho}$ is nonzero. Therefore,

$$b'e^2 - b^\varrho f = 0, \tag{4.16}$$

which gives

$$a'e^2 - a^\varrho f = 0. \tag{4.17}$$

Thus, $U_{(a,b)}$ is projectively equivalent to $U_{(fa^\varrho/e^2, fb^\varrho/e^2)}$ for any choice of e and f in K^*. As we are considering the case when $a \neq 0$, take $e = f = a^\varrho$. We see that $U_{(a,b)} \sim U_{(1,(b/a)^\varrho)}$. By letting $c = (b/a)^\varrho$ and recalling that $b^2 - a^2 \in K_S$, we find that $U_{(a,b)} \sim U_{(1,c)}$ for some $c \in K$ such that $c^2 - 1 \in K_S$.

The following lemma will be helpful in counting the number of projective equivalence classes of unitals of the form $U_{(a,b)}$.

Lemma 4.3.3 *Suppose $c, c' \in K$ such that $c^2-1, c'^2-1 \in K_S$. Then, $U_{(1,c)} \sim U_{(1,c')}$ if and only if there exists $\varrho \in \mathrm{Aut}(N)$ such that $c' = c^{\varrho}$.*

Proof: The proof is immediate after repeating the argument in the previous paragraph with $a = a' = 1$, $b = c$, and $b' = c'$. From the analog of (4.17), one learns that $f = e^2$. Hence, $U_{(1,c)} \sim U_{(1,c')}$ implies $c' = c^{\varrho}$ for some $\varrho \in \mathrm{Aut}(N)$ using the analog of (4.16). ■

It is then natural to define an equivalence relation $\sim$ on the set $\boldsymbol{C} = \{c \in K : c^2 - 1 \in K_S\}$ via $c \sim c'$ if and only if there exists $\varrho \in \mathrm{Aut}(N)$ such that $c' = c^{\varrho}$. We see that the number of equivalence classes of $\boldsymbol{C}$ is precisely the number of projective equivalence classes of unitals of the form $U_{(1,c)}$. In Theorem 2, Section 4 of Baker and Ebert [8], the number of equivalence classes of $\boldsymbol{C}$ is computed indirectly. Specifically, the authors count the number of equivalence classes of $\Delta = \{\delta \in K : \delta(\delta+1) \in K_S\}$ under the relation $\sim$ defined above. Using $c = 2\delta + 1$, it is evident that for every $\delta \in \Delta$ there corresponds a unique $c \in \boldsymbol{C}$, and vice-versa. It is shown that if $q = p^n$ then the number of equivalence classes of Δ (hence $\boldsymbol{C}$) is

$$\frac{1}{2n}\left[n_0 + \sum_{m|n} \phi\left(\frac{2n}{m}\right) p^m\right] - 2,$$

where ϕ is the Euler phi-function and $n = 2^t n_0$, for n_0 odd [8] (see Theorem 2.2.3). This gives the following theorem regarding unitals of the form $U_{(a,b)}$ in the Hughes plane.

Theorem 4.3.4 *Let $q = p^n$, where $n = 2^t n_0$ for t a nonnegative integer and n_0 odd. The number of projectively inequivalent $U_{(a,b)}$'s is*

$$\frac{1}{2n}\left[n_0 + \sum_{m|n} \phi\left(\frac{2n}{m}\right) p^m\right] - 1,$$

one of which is a classical-Rosati unital.

■

If q is an odd prime, we see that there are $(q-1)/2$ projectively inequivalent $U_{(a,b)}$'s.

We note that when $b = 0$, $U_{(a,b)}$ corresponds to the union of conics unital in $PG(2,q^2)$. While $U_{(a,0)}$ does not appear to be a union of ovals in $\mathcal{H}(q^2)$, it does contain at least one oval of $\mathcal{H}(q^2)$. If we define

$$O_{a,b} = \{(x,y,z) \in \mathcal{H}(q^2) : xz - (a+b)y^2 = 0\},$$

we see that $O_{a,b}$ is an oval (by Lemma 4.1.3) and $C_{a,b} \subseteq O_{a,b} \cap U_{(a,b)}$. Moreover, $O_{a,b} \subset U_{(a,b)}$ if and only if $b = 0$. Finally, notice that this analog of the Buekenhout-Metz union of conics occurs only when $q \equiv 1 \pmod 4$, as -1 must be in K_S.

The *dual* of an arbitrary unital U embedded in a projective plane Π is the unital obtained by taking the tangent lines to U as "varieties" and the points of Π lying off U as "blocks", with incidence given by inclusion. We note that two designs $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ and $\mathcal{D}' = (\mathcal{P}', \mathcal{B}', I')$ are called *design isomorphic* if there exists a mapping ζ that maps the points $\mathcal{P}$ onto $\mathcal{P}'$ bijectively and the blocks $\mathcal{B}$ onto $\mathcal{B}'$ bijectively, such that xIb if and only if $x^\zeta I' b^\zeta$ for all $x \in \mathcal{P}$ and all $b \in \mathcal{B}$. A unital U is called *self-dual* if U and its dual are design isomorphic. It was shown in [8] and [26] that all Buekenhout-Metz unitals in $PG(2,q^2)$ are self-dual. We now determine the duals of the unitals described by $U_{(a,b)}$. It will be shown that the classical-Rosati unital and the unital corresponding to the union of conics unital are both self-dual. To accomplish this task, we proceed to determine the tangent line at each point of $U_{(a,b)}$. It has been noted that $[1,0,0]$ is the tangent at $P_\infty = (0,0,1)$. Furthermore, $[0,0,1]$ is the tangent at $(1,0,0)$, for if any point of the form $(1, y, ay^2 + by^{q+1} + t\epsilon)$ is on this line, it would imply that $ay^2 + by^{q+1} + t\epsilon = 0$. By examining the "real" part of this equation, one learns that $(a+b)y_1^2 + (a-b)\omega y_2^2 = 0$. We then see that $y_1 = y_2 = 0$, else the requirement that $b^2 - a^2 \in K_S$ is contradicted. This implies

$t = 0$ and the tangency is thus shown. The following lemma determines the tangent lines at the other points of $U_{(a,b)}$.

Lemma 4.3.5 *Let* $d = 2y_2(by - ay_2\epsilon) - t$. *Then the unique tangent to* $U_{(a,b)}$ *at the point* $P = (1, y, ay^2 + by^{q+1} + t\epsilon)$ *is*

$$\begin{cases} [ay^2 + by^{q+1} - t\epsilon, -2(ay + by^q), 1] & if \quad d \in F_S \cup \{0\} \\ [ay^{2q} + by^{q+1} + t\epsilon, -2(ay^q + by), 1] & if \quad d \in F_N \end{cases} .$$

Proof: If $Q = [u, v, w] = [ay^2 + by^{q+1} - t\epsilon, -2(ay + by^q), 1]$, then $u_2 = 2ay_1y_2 - t$, $v_2 = -2y_2(a - b)$, and $w_2 = 0$. Thus, as in Proposition 4.1.1, we have $d_{PQ} = 2y_2(by - ay_2\epsilon) - t$. Recall that $d_{PQ^q} = -d_{PQ}$ has the same quadratic character as d_{PQ} in F. Also note that $P^\bullet Q = 0$. From Proposition 4.1.1, we see that

$$(1, y, ay^2 + by^{q+1} + t\epsilon)J[ay^{2\theta} + by^{q+1} - t\epsilon^\theta, -2(ay^\theta + by^{q\theta}), 1]$$

where $\theta = 1$ or q as $d = d_{PQ}$ is in $F_S \cup \{0\}$ or F_N, respectively.

To see that Q is indeed tangent to $U_{(a,b)}$, notice first that $(0, 0, 1)$ does not lie on this line. Suppose a point $(1, y', a(y')^2 + b(y')^{q+1} + s\epsilon)$, $y' \in F$ and $s \in K$, lies on Q. Using Proposition 4.1.1, this implies

$$ay^{2\vartheta} + by^{q+1} - t\epsilon^\vartheta - 2(ay^\vartheta + by^{q\vartheta})y' + a(y')^2 + b(y')^{q+1} + s\epsilon = 0,$$

where $\vartheta = 1$ or q depending on the discriminant condition found in that proposition. This equation may be rewritten as

$$a(y^\vartheta - y')^2 + b(y^\vartheta - y')^{q+1} + b(y^\vartheta(y')^q - y^{q\vartheta}y') - t\epsilon^\vartheta + s\epsilon = 0,$$

where we note that $b(y^\vartheta(y')^q - y^{q\vartheta}y') \in K\epsilon$. Now consider a point $(1, y'', a(y'')^2 + b(y'')^{q+1} + r\epsilon) \in U_{(a,b)}$, where $y'' = y^\vartheta - y'$ and $r \in K$ such that $r\epsilon = b(y^\vartheta(y')^q - y^{q\vartheta}y') - t\epsilon^\vartheta + s\epsilon$. From above, we see that $a(y'')^2 + b(y'')^{q+1} + r\epsilon = 0$. Hence $(1, y'', 0)$ is a point of $U_{(a,b)}$ lying on $[0, 0, 1]$. But it has been shown that $[0, 0, 1]$ is tangent at $(1, 0, 0)$. Thus $y'' = 0$ and hence $r = 0$. Therefore, $y' = y^\vartheta$ and $s\epsilon = t\epsilon^\vartheta$. It is evident that the line Q meets $U_{(a,b)}$ in only the point $(1, y, ay^2 + by^{q+1} + t\epsilon)$ or the point $(1, y^q, ay^{2q} + by^{q+1} - t\epsilon)$, whichever is indicated by the discriminant d. To complete the argument, note that the line Q^q is also tangent to $U_{(a,b)}$ since the Frobenius collineation leaves $U_{(a,b)}$ invariant. ∎

Theorem 4.3.6 *As a design, the dual of $U_{(a,b)}$ is isomorphic to $U_{(a,-b)}$.*

Proof: Let $U = \{(1, -2(ay + by^q), ay^2 + by^{q+1} - t\epsilon) : y \in F, t \in K\} \cup \{(0, 0, 1)\}$. By taking $y' = -2(ay + by^q)$, we see that

$$ay^2 + by^{q+1} = \frac{a}{4(a^2 - b^2)}(y')^2 - \frac{b}{4(a^2 - b^2)}(y')^{q+1}.$$

As $-t$ varies over K as t varies over K, we see that $U = U_{(a/(4(a^2-b^2)), -b/(4(a^2-b^2)))}$. From the earlier discussion regarding projective equivalence, we see that $U \sim U_{(a,-b)}$.

By way of the design isomorphism which changes square brackets to parentheses and permutes first and third coordinates, we see from Lemma 4.3.5 that the dual of $U_{(a,b)}$ is design isomorphic to the unital

$$\begin{aligned} U^* \;=\; & \{(1, -2(ay + by^q), ay^2 + by^{q+1} - t\epsilon) : y \in F, t \in K, d \in F_S \cup \{0\}\} \cup \\ & \{(1, -2(ay^q + by), ay^{2q} + by^{q+1} + t\epsilon) : y \in F, t \in K, d \in F_N\} \cup \{(0, 0, 1)\}. \end{aligned}$$

To see that U^* is a subset of U, we simply note that the points of U^* of the form $(1, -2(ay^q + by), ay^{2q} + by^{q+1} + t\epsilon)$ are contained in U by substituting $y' = y^q$ and $t' = -t$. As U and U^* both have cardinality $q^3 + 1$, the result follows.

∎

If one recalls that all classical-Rosati unitals are projectively equivalent and that this occurs precisely when $a = 0$, then the following corollary is immediate.

Corollary 4.3.7 *If either $a = 0$ or $b = 0$ then $U_{(a,b)}$ is self-dual.*

∎

If $a \neq 0$ and $b \neq 0$ then more work is required to determine whether or not $U_{(a,b)}$ is self-dual. This is equivalent to deciding if $U_{(a,b)}$ is design isomorphic to $U_{(a,-b)}$. In general, to determine if $U_{(1,c)}$ is projectively equivalent to $U_{(1,-c)}$, using Lemma 4.3.3, one must answer the cyclotomic question of determining which elements $c \in K$ simultaneously satisfy $c^2 - 1 \in K_S$ and $c^{p^i} = -c$ for some integer i between 1 and $n-1$, where $q = p^n$. We are unable to answer this question at this time. Of course, even if $U_{(1,c)}$ is not projectively equivalent to $U_{(1,-c)}$, it is still possible that the unitals are design isomorphic. One must either exhibit the isomorphism from one unital to the other, or show that one unital possesses a property (which would be preserved under isomorphism) that the other does not and declare that the unitals are nonisomorphic. We note that Kestenband [42] used the latter to show that the Rosati unital is not design isomorphic to the classical unital in $PG(2,q^2)$.

Besides determining whether $U_{(a,b)}$ is self-dual, there are several other issues which require this type of analysis. One very natural question is that of design isomorphism between a given $U_{(a,b)}$ in $\mathcal{H}(q^2)$ and its corresponding Buekenhout-Metz unital in $PG(2,q^2)$. Moreover, there is very little known about design isomorphism among Buekenhout-Metz unitals themselves. Indeed, it is not conclusively known which nonclassical BM-unitals (if any) are isomorphic as designs to the classical unital.

CONCLUSION

This document has endeavored to contribute to the study of unitals embedded in finite projective planes in two arenas. The first is the well-studied subject of Buekenhout-Metz unitals in the classical plane $PG(2,q^2)$. The second setting is that of the Hughes plane, in which far less is known regarding unitals. In this section, we attempt to outline the achievements recorded in this document, as well as the open questions which will be the focus of future research.

In Chapters 2 and 3, two aspects of Buekenhout-Metz unitals embedded in the classical plane $PG(2,q^2)$ are considered. The first matter of concern is that of the "feet" of BM-unitals. It is well-known that the feet of a classical unital are collinear. For nonclassical BM-unitals, it has been evident to some researchers that the feet of a unital which is a union of conics form an arc, but the patterns of the feet for the remaining BM-unitals have not been previously classified. Although the results of Section 2.3 do not describe the patterns of these feet to the degree of specificity that one may desire, the general pattern of a $\{0,1,2,4\}$-set is shown. One goal is to prove general theorems based on the computer data noted in Section 2.3. Of much greater difficulty and importance is the question of characterizing BM-unitals by the knowledge of the feet. The conjecture given at the conclusion of Chapter 2 seems a likely place to start.

The group theoretic characterization of Buekenhout-Metz unitals given in Chapter 3 represents joint work with G. L. Ebert. It is based heavily on earlier group theoretic characterizations, yet is arguably the most concise and encompassing group theoretic characterization to date. The method used in the proof has the added benefit of producing a new group theoretic characterization of the classical unital. There is some possibility that Theorem 3.2.6 may be strengthened by weakening the hypotheses. A natural hypothesis that one might reasonably weaken is that of the normality of the subgroup S in Γ. One ambitious hope for Theorem 3.2.6 (or a stronger version) is to provide an answer for the difficult question of showing that every unital in $PG(2, q^2)$, q odd, is Buekenhout-Metz. It appears that both of these problems require knowledge of group theory at a level beyond that which is used in this document.

The research regarding unitals in the Hughes plane began as an attempt to obtain a group theoretic characterization of the Rosati unital. While this remains as a pressing open question, we have made an important first step by determining the orbit structure of the points under the group which leaves the classical-Rosati unital invariant. Moreover, the feet of the classical-Rosati unital have been determined, knowledge that may prove beneficial in developing a geometric characterization. Several helpful tools involving incidence in the Hughes plane and its relationship to that of the classical plane were developed in the process.

While examining a certain representative of the classical-Rosati unital, a striking similarity was noted between its form and that of Buekenhout-Metz unitals as described by (2.3). This led to a computer search for unitals in the Hughes plane with a similar form, from which the general form and conditions for the $U_{(a,b)}$'s were deduced. These unitals were previously unknown, hence a new class of infinite families of unitals has been added to the Hughes planes. Although several key properties of these new unitals have been presented, some important questions remain to be answered. First, the patterns formed by the feet of these unitals have not yet been determined. Additionally, the issue of which $U_{(a,b)}$'s, for $a \neq 0$ and $b \neq 0$, are self-dual is not yet resolved. Finally, can one obtain a group theoretic characterization of these unitals, as well as the classical-Rosati unital? In answering this last question, one should consider the possibility of using the group theoretic characterization which was presented in Chapter 3 in some clever way, as the order of the Sylow p-subgroup of the group leaving the unital invariant in the Hughes plane is roughly a factor of q^2 less than that of the corresponding BM-unital in $PG(2, q^2)$.

The general subject of unitals embedded in the Hughes plane is one which bears consideration. Could there be other unitals embedded in the Hughes plane which correspond, in some sense, to Buekenhout-Metz unitals, other than those which are invariant under the Frobenius collineation? Is it possible, for $q > 3$, that all the unitals in $\mathcal{H}(q^2)$ have now been found, as is widely believed regarding unitals in $PG(2, q^2)$? Recall that for $q = 3$ Brouwer has found a unital embedded in $\mathcal{H}(9)$ which he denotes by E.8. In [16], it is shown that the automorphism group of this unital has the same order as that of Rosati's unital but it is nonisomorphic to it. Thus, one may seek to answer the previous question in the negative by generalizing Brouwer's E.8 for arbitrary q.

Although addressed only briefly in Chapter 4, the issue of design isomorphism between the various unitals described in this document is virtually wide open. As noted at the conclusion of Chapter 4, it is of interest to answer the design isomorphism question between: $U_{(a,b)}$'s and BM-unitals, nonclassical BM-unitals and the classical unital, and various BM-unitals.

Finally, one cannot help but wonder whether the general technique which has led to new unitals in the Hughes plane can be repeated in other nonclassical projective planes. The representatives of points (and lines) in such a plane would need to be sufficiently similar to those of the classical plane in order to make a reasonable correspondence. Moreover, the incidence relation of this plane must be sufficiently similar to that of the classical plane in order to declare that the set corresponding to a known unital was indeed a unital in the nonclassical plane.

APPENDIX

The proof of Theorem 4.2.1 will now be given. We remind the reader of its statement.

Theorem 4.2.1 *Let U be a classical-Rosati unital and let C be the conic $U \cap \pi_0$. Let G be the linear collineation group leaving U invariant; i.e., $G \cong PGL(2,q)$. For $q \equiv 1 \pmod 4$, U consists of three orbits under G, namely the points of C, the $q(q^2-1)/2$ points off C which lie on secant lines to C, and the remaining $q(q^2-1)/2$ points which do not lie on secant lines to C. For $q \equiv 3 \pmod 4$, U consists of four orbits under G. The points of C and the points off C which lie on secant lines to C are again orbits of G. The points which do not lie on secants to C are split into two orbits, each of size $q(q^2-1)/4$. Moreover, these latter two orbits are joined by the Frobenius collineation σ, giving one orbit of size $q(q^2-1)/2$ for the group $G \times \langle\sigma\rangle$.*

Using the notation of (4.11), we choose $U = U_{(0,1)}$ as the representative of a classical-Rosati unital for which we will determine the orbit structure. Thus,

$$U = \{(1, y, y^{q+1} + t\epsilon) : y \in F, t \in K\} \cup \{(0,0,1)\}.$$

We remind the reader that G denotes the linear collineation group leaving U invariant. From Theorem 4.3.1, G has order $q(q^2-1)$ and consists of collineations which may be represented by matrices of the form

$$\begin{pmatrix} c^2 & cd & d^2 \\ 2ce & cf+ed & 2df \\ e^2 & ef & f^2 \end{pmatrix}, \text{ where } c,d,e,f \in K,\ cf - de \neq 0. \tag{4.18}$$

Let G_0 denote the stabilizer in G of the point $P_\infty = (0,0,1)$, as in Theorem 4.3.2. In addition, we let C denote the conic formed by the intersection of U with the central subplane π_0. Therefore,

$$C = \{(1, y, y^2) : y \in K\} \cup \{(0,0,1)\},$$

which was described in detail in Section 1.3. Finally, recall that the "discriminant" d (as used in Lemma 4.3.5) takes the form $d_{(P)} = 2yy_2 - t$ for a point $P = (1, y, y^{q+1} + t\epsilon)$ in $U = U_{(0,1)}$. The following lemma will be be useful in the proof of Theorem 4.2.1.

Lemma 4.1 *Let $P = (1, y, y^{q+1} + t\epsilon) \in U \setminus C$. Then P lies on a secant line to C if and only if $d_{(P)} = 2yy_2 - t \in F_S$.*

Proof: As π_0 is a Baer subplane of $\mathcal{H}(q^2)$, every point of $\mathcal{H}(q^2) \setminus \pi_0$ lies on a unique line of π_0 (i.e., a line which may be represented by a vector with all coordinates in K). Dually, every line of $\mathcal{H}(q^2)$ which is not a line of π_0 contains a unique point of π_0. Thus, we see that every line which is secant to C must be a line of π_0. For $P = (1, y, y^{q+1} + t\epsilon) \in U \setminus C$, suppose that $[u, v, w]$ is the unique line of π_0 passing through P, where $u, v, w \in K$. From our discussion, it is clear that P lies on a secant line to C if and only if $[u, v, w]$ is a secant line to C. Moreover, from Section 1.3, we know that the line $[u, v, w]$ is secant to C if and only if $v^2 - 4uw \in K_S$.

As $PJ[u, v, w]$, we have

$$u + v(y_1 + y_2\epsilon) + wy^{q+1} + wt\epsilon = 0,$$

where y has been written in terms of the basis $\{1, \epsilon\}$. Separating this equation into "real" and "imaginary" parts we obtain

$$u + vy_1 + wy^{q+1} = 0 \tag{4.19}$$

and

$$vy_2 + wt = 0, \tag{4.20}$$

respectively.

As $P \notin \pi_0$, either $y \in F \setminus K$ or $t \neq 0$. Equivalently, either $y_2 \neq 0$ or $t \neq 0$. Suppose first $t = 0$, (hence $y_2 \neq 0$) which from (4.20) gives $v = 0$. In this case, w is nonzero; hence, we may normalize the vector by taking $w = 1$. Thus, from (4.19), $[u, v, w] = [-y^{q+1}, 0, 1]$. Therefore, P (with $t = 0$) lies on a line secant to C if and only if $4y^{q+1} \in K_S$, which occurs if and only if $4y^{q+1}y_2^2 \in K_S$. But, $4y^{q+1}y_2^2 = d_{(P)}^{q+1}$ and $d_{(P)} \in F_S$ if and only if $d_{(P)}^{q+1} \in K_S$. Hence, P lies on a C-secant if and only if $d_{(P)} \in F_S$.

Suppose now that $t \neq 0$. Then, (4.20) gives $w = -vy_2/t$. Again, as $v \neq 0$, we set $v = 1$. This gives $u = y_2 y^{q+1}/t - y_1$ and

$$[u, v, w] = \left[\frac{y_2 y^{q+1}}{t} - y_1, 1, \frac{-y_2}{t}\right].$$

Therefore, P lies on a secant line to C if and only if $1 - 4(-y_2/t)(y_2 y^{q+1}/t - y_1) \in K_S$, which occurs if and only if $t^2 + 4y_2(y_2 y^{q+1} - y_1 t) \in K_S$. As $d_{(P)}^{q+1} = t^2 + 4y_2(y_2 y^{q+1} - y_1 t)$, we see again that P lies on a C-secant if and only if $d_{(P)} \in F_S$. ■

Proof of Theorem 4.2.1: From Theorem 4.3.2, the points $(1, 0, \epsilon)$ and $(1, 0, \omega\epsilon)$ of U lie in different orbits under G_0. Taking a matrix of the form given in (4.18) with $c = f = 0$, $d = \omega$, and $e = 1$, we obtain a collineation of G which maps $(1, 0, \epsilon) \in U$ to the point with representative $(\epsilon, 0, \omega^2)$. Suppose $q \equiv 1 \pmod 4$. Then $\epsilon \in F_N$, which implies $(\epsilon, 0, \omega^2)\rho(1, 0, -\omega\epsilon)$. Notice that $-\omega \in K_N$, when $q \equiv 1 \pmod 4$. Therefore, $(1, 0, -\omega\epsilon)$ and $(1, 0, \omega\epsilon)$ lie in the same orbit of G_0. Suppose $q \equiv 3 \pmod 4$. Then $\epsilon \in F_S$ and hence $(\epsilon, 0, \omega^2)\rho(1, 0, \omega\epsilon)$. Therefore, for either choice of q, the orbits of $(1, 0, \epsilon)$ and $(1, 0, \omega\epsilon)$ under G_0 are joined by G. Thus, G acts transitively on the points of U which lie on secant lines to C which pass through P_∞. Since G acts doubly-transitively on C, G is transitive on the secant lines to C. Therefore, G is transitive on the points of $U \setminus C$ which lie on lines secant to C. Also note that since G (and the Frobenius collineation) leave C invariant, points lying on a secant line to C cannot lie in the same orbit as points not lying on a C-secant.

Hence, one orbit of G consists of the $\binom{q+1}{2}(q-1) = q(q^2-1)/2$ points of $U \setminus C$ which lie on lines secant to C.

Case 1: Suppose $q \equiv 1 \pmod 4$ and consider the point $P \in U$ which is represented by $(1, \epsilon, -\omega)$. Notice that $d_{(P)} = -2\epsilon \in F_N$; hence, P does not lie on a secant line to C by the Lemma. We will determine the size of the orbit P^G by computing the stabilizer of P in G. Let g be a collineation of G having the form described in (4.18). We see that

$$P^g = (c^2 - e^2\omega + 2ce\epsilon, cd - ef\omega + (cf + ed)\epsilon, d^2 - f^2\omega + 2df\epsilon). \tag{4.21}$$

Further assume that g fixes P.

Suppose g is a collineation for which $c = 0$; hence $e \neq 0$. This gives $P^g = (-e^2\omega, -ef\omega + ed\epsilon, d^2 - f^2\omega + 2df\epsilon)$, which is equivalent to

$$\left(1, \frac{f}{e} - \frac{d\epsilon}{e\omega}, \frac{d^2 - f^2\omega + 2df\epsilon}{-e^2\omega}\right)$$

as $-e^2\omega \in K* \subset F_S$. Since g fixes P, by comparing second coordinates we see that $\frac{f}{e} - \frac{d\epsilon}{e\omega} = \epsilon$. Using the basis $\{1, \epsilon\}$, this implies $f = 0$. Thus $-\frac{d}{e\omega} = 1$. Setting $e = 1$ to obtain a unique representative, we see that there is at most one element of G, with $c = 0$, that fixes P. Such an element may be represented by the matrix

$$\begin{pmatrix} 0 & 0 & \omega^2 \\ 0 & -\omega & 0 \\ 1 & 0 & 0 \end{pmatrix}. \tag{4.22}$$

It is easy to see that the collineation induced by this matrix does indeed fix P. Therefore, one nonidentity element of the stabilizer G_P has been found.

Consider $g \in G_P$ for which $c \neq 0$ in the representation given in (4.18). One may then choose a unique matrix representation of g by setting $c = 1$. This gives

$$P^g = (1 - e^2\omega + 2e\epsilon, d - ef\omega + (f + ed)\epsilon, d^2 - f^2\omega + 2df\epsilon).$$

We see that P^g may be represented by

$$\left(1, \frac{d - ef\omega + (f + ed)\epsilon^\theta}{1 - e^2\omega + 2e\epsilon^\theta}, \frac{d^2 - f^2\omega + 2df\epsilon^\theta}{1 - e^2\omega + 2e\epsilon^\theta}\right),$$

where $\theta = 1$ or q depending on whether $1 - e^2\omega + 2e\epsilon$ is in F_S or F_N, respectively. As $P^g = P$, we compare the second and third coordinates of these left-normalized representatives to obtain

$$d - ef\omega + (f + ed)\epsilon^\theta = (1 - e^2\omega + 2e\epsilon^\theta)\epsilon \tag{4.23}$$

and

$$d^2 - f^2\omega + 2df\epsilon^\theta = (1 - e^2\omega + 2e\epsilon^\theta)(-\omega), \tag{4.24}$$

respectively. By separating (4.24) in terms of the basis $\{1, \epsilon^\theta\}$, one finds that $e = -df/\omega$ from the "imaginary" part; consequently, $(d^2+\omega)(f^2-1) = 0$ from the "real" part. As $-\omega \in K_N$, for $q \equiv 1 \pmod 4$, we must have either $f = 1$ or $f = -1$. Suppose $\theta = 1$. Then (4.23) yields $d - ef\omega = 2e\omega$ and $de + f = 1 - e^2\omega$ using the basis $\{1, \epsilon\}$. If $f = 1$, we find that $e = -d/\omega$, which from these equations gives $d = e = 0$. Thus, the identity collineation is obtained. If $f = -1$, we find $e = d/\omega$ and one obtains the contradiction that $d^2 = \omega$. Suppose $\theta = q$, in which case (4.23) may be separated using the basis $\{1, \epsilon\}$ to obtain $d - ef\omega = -2e\omega$ and $-(de + f) = 1 - e^2\omega$. If $f = 1$, then $e = -d/\omega$, which gives the contradiction that $d^2 = \omega$. If $f = -1$, then $e = d/\omega$ and we find again that $d = e = 0$. Therefore, G_P consists of two elements, namely the identity and the collineation represented by (4.22). Hence, the orbit of P under G has size $q(q^2-1)/2$, which must be all the points of U which do not lie on a secant line to C.

Case 2: Suppose $q \equiv 3 \pmod 4$ and consider the point $P \in U$ represented by $(1, \gamma\epsilon, -\omega^2)$. (Recall that $\epsilon^2 = \gamma^{q+1} = \omega$.) Notice that $d_{(P)} = -2\gamma\epsilon\mathrm{Im}(\gamma\epsilon)$, where $\mathrm{Im}(\gamma\epsilon)$ denotes the "imaginary" part of $\gamma\epsilon$. As $q \equiv 3 \pmod 4$, we have $\epsilon \in F_S$. Therefore, since $\gamma \in F_N$ and $-2\mathrm{Im}(\gamma\epsilon)\epsilon \in F_S$, we see that $d_{(P)} \in F_N$. Thus P does not lie on any line secant to C by the lemma. To determine G_P, let $g \in G$ having the form of (4.18). We see that

$$P^g = (c^2 - e^2\omega^2 + 2ce\gamma\epsilon, cd - ef\omega^2 + (cf + ed)\gamma\epsilon, d^2 - f^2\omega^2 + 2df\gamma\epsilon). \qquad (4.25)$$

Supposing that $c = 0$ in the matrix representation of g, we see that P^g has normalized representative

$$\left(1, \frac{f}{e} - \frac{d\gamma\epsilon}{e\omega^2}, \frac{d^2 - f^2\omega^2 + 2df\gamma\epsilon}{-e^2\omega^2}\right). \qquad (4.26)$$

If $g \in G_P$, by comparing the second coordinates of these normalized representatives of P one obtains $\frac{f}{e} - \frac{d\gamma\epsilon}{e\omega^2} = \gamma\epsilon$. Using the basis $\{1, \gamma\epsilon\}$ of F over K, we see that $f = 0$ and $d = -e\omega^2$. As the matrix is nonsingular, $e \neq 0$; thus we set $e = 1$ to obtain the collineation

$$\begin{pmatrix} 0 & 0 & \omega^4 \\ 0 & -\omega^2 & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad (4.27)$$

in G_P.

For $g \in G_P$ with $c \neq 0$, we will set $c = 1$ to obtain a unique matrix representation. Similar to the situation above, we see that P^g has as a normalized representative the vector

$$\left(1, \frac{d - ef\omega^2 + (f + ed)\gamma^\theta\epsilon^\theta}{1 - e^2\omega^2 + 2e\gamma^\theta\epsilon^\theta}, \frac{d^2 - f^2\omega^2 + 2df\gamma^\theta\epsilon^\theta}{1 - e^2\omega^2 + 2e\gamma^\theta\epsilon^\theta}\right),$$

where $\theta = 1$ or q depending on whether $1 - e^2\omega^2 + 2e\gamma\epsilon$ is in F_S or F_N, respectively. As $P^g = P$, we compare the second and third coordinates of these left-normalized representatives to obtain

$$d - ef\omega^2 + (f + ed)\gamma^\theta\epsilon^\theta = (1 - e^2\omega^2 + 2e\gamma^\theta\epsilon^\theta)\epsilon \qquad (4.28)$$

and

$$d^2 - f^2\omega^2 + 2df\gamma^\theta\epsilon^\theta = (1 - e^2\omega^2 + 2e\gamma^\theta\epsilon^\theta)(-\omega), \qquad (4.29)$$

respectively. Separating (4.29) in terms of the basis $\{1, \gamma\epsilon\}$ of F over K, we find that $e = -df/\omega^2$ from the "imaginary" part; consequently, $(d^2+\omega^2)(f^2-1) = 0$. As $-\omega^2 \in F_N$, for $q \equiv 3 \pmod 4$, we find that either $f = 1$ or $f = -1$.

Suppose first that $\theta = 1$. Using $e = -df/\omega^2$ and $f^2 = 1$ in (4.28) gives

$$2d + (1 - d^2/\omega^2)f\gamma\epsilon = (1 - d^2/\omega^2)\gamma\epsilon - 2df\gamma^2/\omega. \tag{4.30}$$

If $f = 1$, one finds that $d = -d\gamma^2/\omega$. Then, since $\gamma^2 \neq -\omega$, we must have $d = 0$ and hence $e = 0$. Therefore, if $f = 1$ then g is the identity. If $f = -1$, we see from (4.30) that

$$d\omega\gamma^2 - (d^2 - \omega^2)\gamma\epsilon - d\omega^2 = 0.$$

Thus

$$d = \frac{\omega[(\gamma^2-\omega) \pm (\gamma^2+\omega)]}{2\gamma\epsilon}.$$

By simplifying, we see that $d = \gamma\epsilon$ or $-\omega^2/(\gamma\epsilon)$, neither of which is in K. Hence, there are no solutions for d when $f = -1$.

Suppose now that $\theta = q$. Again using $e = -df/\omega^2$ and $f^2 = 1$ in (4.28) gives

$$2d - (1 - d^2/\omega^2)f\gamma^q\epsilon = (1 - d^2/\omega^2)\gamma\epsilon + 2df, \tag{4.31}$$

where we note that $(\gamma\epsilon)^q = -\gamma^q\epsilon$. If $f = 1$, then (4.31) gives

$$(1 - \frac{d^2}{\omega^2})(\gamma^q + \gamma)\epsilon = 0.$$

As $\gamma + \gamma^q \neq 0$, we find $d = \pm\omega$ which gives $e = \mp 1/\omega$, respectively. Thus, the collineations of G_P represented by matrices for which $f = 1$ and $1 - e^2\omega^2 + 2e\gamma\epsilon \in F_N$ are precisely

$$\begin{pmatrix} 1 & \omega & \omega^2 \\ -2/\omega & 0 & 2\omega \\ 1/\omega^2 & -1/\omega & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & -\omega & \omega^2 \\ 2/\omega & 0 & -2\omega \\ 1/\omega^2 & 1/\omega & 1 \end{pmatrix}.$$

If $f = -1$, then (4.31) gives $4d + (1 - d^2/\omega^2)(\gamma^q - \gamma)\epsilon = 0$. This quadratic in d may be solved and simplified to obtain

$$d = \frac{\omega[2\omega \pm (\gamma^q + \gamma)\epsilon]}{(\gamma^q - \gamma)\epsilon}. \tag{4.32}$$

Notice that $(\gamma^q - \gamma)\epsilon \in K$, but $(\gamma^q + \gamma)\epsilon \notin K$. Hence there are no solutions for d in K when $f = -1$. We conclude that G_P consists of four elements. Therefore, the orbit of P under G has size $q(q^2 - 1)/4$.

Continuing in the case when $q \equiv 3 \pmod 4$, we now consider the collineation group $G \times \langle \sigma \rangle$, where σ is the Frobenious collineation. Notice that if $P = (1, \gamma\epsilon, -\omega^2)$ then $P^\sigma = P^q = (1, -\gamma^q\epsilon, -\omega^2)$. Thus, the orbits of P and P^q under G have the same cardinality. To see that these orbits under G are disjoint, we show directly that no collineation of G maps P to P^q. After having accomplished this, the theorem will be proven.

Suppose by way of contradiction that there exists $g \in G$ for which $P^g = P^q$, where g is of the form given in (4.18). If $c = 0$, then P^g may be represented by (4.26). Comparing third coordinates of P^g and P^q gives $d^2 - f^2\omega^2 + 2df\gamma\epsilon = e^2\omega^4$. Separating this in terms of the basis $\{1, \gamma\epsilon\}$ gives $df = 0$. Now, $d \neq 0$ as the matrix associated with g is nonsingular. Hence, $f = 0$ which gives $d^2 = e^2\omega^4$. Comparing the second coordinates, then gives

$$\frac{d}{e\omega^2}\gamma\epsilon = -\gamma^q\epsilon.$$

Using the fact that $d^2 = e^2\omega^4$, we see that $\gamma = \pm\gamma^q$ which is a contradiction. If $c \neq 0$, we set $c = 1$. Using the same computation as above, we find that (4.29) holds in this situation, by comparing third coordinates. So again, $f^2 = 1$ and $e = -df/\omega^2$. By comparing the second coordinates, one obtains

$$d - ef\omega^2 + (f + ed)\gamma^\theta\epsilon^\theta = (1 - e^2\omega^2 + 2e\gamma^\theta\epsilon^\theta)(-\gamma^q\epsilon) \tag{4.33}$$

(which is analgous to (4.28)). As before, $\theta = 1$ or q depending on whether $1 - e^2\omega^2 + 2e\gamma\epsilon \in F_S$ or F_N, resprectively. Suppose first $\theta = 1$, then (4.33) has the form

$$2d(1 - f) + (1 - d^2/\omega^2)(f\gamma + \gamma^q)\epsilon = 0.$$

When $f = 1$, by separating in terms of the basis $\{1, \epsilon\}$ and noting that $\gamma^q + \gamma \in K$, we see that $d = \omega$ and $e = -1/\omega$. But then, $1 - e^2\omega^2 + 2e\gamma\epsilon = -2\gamma\epsilon/\omega \in F_N$, contradicting that we are in the case when $\theta = 1$. When $f = -1$, (4.33) has the form $4d + (1 - d^2/\omega^2)(\gamma^q - \gamma)\epsilon = 0$. But we have seen that this quadratic has no solutions for d in K (see (4.32)). Suppose now $\theta = q$; hence, (4.33) may be written as

$$2d - (1 - d^2/\omega^2)f\gamma^q\epsilon = -(1 - d^2/\omega^2)\gamma^q\epsilon - 2df\gamma^{2q}/\omega.$$

If $f = 1$ then $d = d\gamma^{2q}/\omega$. As $d \neq 0$ (else g is the identity), we see that $\gamma^{2q} = \omega$, a contradiction. When $f = -1$, we obtain

$$(d^2 - \omega^2)\gamma^q\epsilon + d\gamma^{2q}\omega - d\omega^2$$

which when raised to the qth power gives the same quadratic that has been shown to have no solutions for d in K. Therefore, there is no element of G which maps P to P^q. $\blacksquare$

BIBLIOGRAPHY

[1] V. Abatangelo. On Buekenhout-Metz unitals in $PG(2,q^2)$, q even. *Arch. Math.*, 59:197–203, 1992.

[2] V. Abatangelo and B. Larato. Unitals in the Hughes planes and the Hughes-Rosati planes. Preprint.

[3] V. Abatangelo and B. Larato. A group-theoretical characterization of parabolic Buekenhout-Metz unitals. *Boll. Un. Mat. Ital.*, (7) 5-A:195–206, 1991.

[4] V. Abatangelo, B. Larato, and L.A. Rosati. Unitals in planes derived from the Hughes planes. *J. Comb. Inf. Sys. Sci.*, 15:151–155, 1990.

[5] J. André. Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Zeit.*, 60:156–186, 1954.

[6] R. Baer. *Linear algebra and projective geometry.* Academic Press, New York, 1952.

[7] R.D. Baker and G.L. Ebert. Intersection of unitals in the desarguesian plane. *Cong. Num.*, 70:87–94, 1990.

[8] R.D. Baker and G.L. Ebert. On Buekenhout-Metz unitals of odd order. *J. Combin. Theory, Ser. A*, 60:67–84, 1992.

[9] A. Barlotti. Un'estensione del teorema di Segre-Kustaanheimo. *Boll. Un. Mat. Ital.*, 10:498–506, 1955.

[10] A. Barlotti and G. Lunardon. Una classe di unital nei Δ-piani. *Riv. Mat. Univ. Parma*, 5:781–785, 1979.

[11] S.G. Barwick. A characterization of the classical unital. *Geom. Ded.*, 52:175–180, 1994.

[12] M. Biliotti and G. Korchmàros. Collineations preserving a unital in a projective plane of even order. *Geom. Ded.*, 31:333–344, 1989.

[13] M. Biliotti and G. Korchmàros. Collineations preserving a unital of a projective plane of odd order. *J. Algebra*, 122:130–149, 1989.

[14] R.C. Bose. Mathematical theory of the symmetrical factorial design. *Sankhya*, 8:107–166, 1947.

[15] A.E. Brouwer. Some unitals on 28 points and their embeddings in projective planes of order 9. In *Geometries and Groups*, volume 893 of *Lecture Notes in Mathematics*, pages 183–188, 1981.

[16] A.E. Brouwer. A unital in the Hughes plane of order nine. *Discrete Math.*, 77:55–56, 1989.

[17] R.H. Bruck and R.C. Bose. The construction of translation planes from projective spaces. *J. Algebra*, 1:85–102, 1964.

[18] F. Buekenhout. Existence of unitals in finite translation planes of order q^2 with kernel of order q. *Geom. Ded.*, 5:189–194, 1976.

[19] A.R. Camina and T.M. Gagen. Block transitive automorphism groups and designs. *J. Algebra*, 86:549–554, 1984.

[20] R. Casse, C. O'Keefe, and T. Pentilla. Characterisations of Buekenhout-Metz unitals. *Geom. Ded.* submitted.

[21] W. Cherowitzo. Hyperovals in desarguesian planes: an update. Preprint.

[22] H.S.M. Coxeter. *Projective Geometry.* Springer-Verlag, New York, second edition, 1987.

[23] M. J. de Resmini and N. Hamilton. Hyperovals and unitals in Figueroa planes. Preprint.

[24] P. Dembowski. *Finite geometries.* Springer-Verlag, New York, 1968.

[25] L. Dickson. *Linear groups, with an exposition of the Galois field theory.* Reprint Dover, New York, 1958. 1901.

[26] G.L. Ebert. On Buekenhout-Metz unitals of even order. *Europ. J. Combinatorics*, 13:109–117, 1992.

[27] G. Faina and G. Korchmàros. A graphic representation of hermitian curves. *Annals Discr. Math.*, 18:335–342, 1983.

[28] D. A. Foulser. The flag-transitive collineation groups of the finite Desarguesian affine planes. *Canad. J. Math.*, 16:443–472, 1964.

[29] M.J. Ganley. A class of unitary block designs. *Math. Zeit.*, 128:34–42, 1972.

[30] K. Grüning. A class of unitals of order q which can be embedded in two different planes of order q^2. *J. Geom.*, 29:61–77, 1987.

[31] M. Hall. Projective planes. *Trans. Amer. Math. Soc.*, 54:229–277, 1943.

[32] M. Hall. *The theory of groups.* Macmillan, New York, 1959.

[33] J.W.P. Hirschfeld. *Projective Geometries over Finite Fields.* Oxford University Press, London, 1979.

[34] J.W.P. Hirschfeld. *Finite Projective Spaces of Three Dimensions.* Oxford University Press, London, 1985.

[35] J.W.P. Hirschfeld, L. Storme, J.A. Thas, and J. Voloch. A characterization of hermitian curves. *J. Geom.*, 41:72–77, 1991.

[36] J.W.P. Hirschfeld and T. Szonyi. Sets in a finite plane with few intersection numbers and a distinguished point. *Discrete Math.*, 97:229–242, 1991.

[37] A. Hoffer. On unitary collineation groups. *J. Algebra*, 22:211–218, 1972.

[38] D. Hughes. A class of non-desarguesian projective planes. *Canad. J. Math.*, 9:378–388, 1957.

[39] D. Hughes and F. Piper. *Projective planes*. Springer-Verlag, New York, 1973.

[40] W. M. Kantor. On unitary polarities of finite projective planes. *Canad. J. Math.*, 23:1060–1077, 1971.

[41] B. Kestenband. Unital intersections in finite projective planes. *Geom. Ded.*, 11:107–117, 1981.

[42] B. Kestenband. A family of unitals in the Hughes plane. *Canad. J. Math.*, 42(6):1067–1083, 1990.

[43] B. Larato. Una caratterizzazione degli unitals parabolici di Buekenhout-Metz. *Le Matematiche*, 38:95–98, 1983.

[44] C. Lefèvre-Percsy. Characterization of Buekenhout-Metz unitals. *Arch. Math.*, 36(6):565–568, 1981.

[45] C. Lefèvre-Percsy. Characterization of hermitian curves. *Arch. Math.*, 39(5):476–480, 1982.

[46] H. Lüneburg. Some remarks concerning the Ree groups of type (G_2). *J. Algebra*, 3:256–259, 1966.

[47] R. Mathon. Constructions of cyclic Steiner 2-designs. *Annals. Discr. Math.*, 34:353–362, 1987.

[48] R. Metz. On a class of unitals. *Geom. Ded.*, 8:125–126, 1979.

[49] M. O'Nan. Automorphisms of unitary block designs. *J. Algebra*, 20:495–511, 1972.

[50] G. Panella. Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito. *Boll. Un. Mat. Ital.*, 10:507–513, 1955.

[51] F. Piper. Polarities in the Hughes plane. *Bull. London Math. Soc.*, 2:209–213, 1970.

[52] F. Piper. Unitary block designs. In *Graph Theory and Combinatorics*, volume 34 of *Research Notes in Mathematics*, pages 98–105, 1979.

[53] C. Quinn and R. Casse. Concerning a characterisation of Buekenhout-Metz unitals. *J. Geom.*, 52:159–167, 1995.

[54] T. G. Room. Polarities and ovals in the Hughes plane. *J. Aust. Math. Soc.*, 13:196–204, 1972.

[55] L. A. Rosati. I gruppi di collineazioni dei piani di Hughes. *Boll. Un. Mat. Ital.*, 13:505–513, 1958.

[56] L. A. Rosati. Disegni unitari nei piani di Hughes. *Geom. Ded.*, 27:295–299, 1988.

[57] B. Segre. Ovals in a finite projective plane. *Canad. J. Math.*, 7:414–416, 1955.

[58] J. Smart. *Modern Geometries.* Brook/Cole, Pacific Grove, California, fourth edition, 1994.

[59] J.A. Thas. A combinatorial characterization of hermitian curves. *J. Alg. Combin.*, 1:97–102, 1992.

[60] J. Tits. Les groupes simples de Suzuki et de Ree. *Séminaire Bourbaki*, 3 e année(210), 1960.

[61] O. Veblen and J. H. M. Wedderburn. Non-desarguesian and non-pascalian geometries. *Trans. Amer. Math. Soc.*, 8:379–388, 1907.

[62] O. Veblen and J.W. Young. *Projective geometry.* Ginn, Boston, 1910.

[63] H. Wilbrink. A characterization of the classical unitals. In *Finite Geometries*, volume 82 of *Lecture Notes in Pure and Applied Math.*, pages 445–454. Dekker, 1986.

[64] G. Zappa. Sui gruppi di collineazioni dei piani di Hughes. *Boll. Un. Mat. Ital.*, 12:507–516, 1957.

[65] M. Zassenhaus. Über endliche Fastkörper. *Abh. Math. Sem. Univ. Hamburg*, 11:187–220, 1935.