Commutative semifields of rank 2 over their middle nucleus

Simeon Ball[1] * and Michel Lavrauw[2]

[1] Queen Mary, University of London, London, E1 4NS, United Kingdom
[2] Eindhoven University of Technology, Eindhoven, 5600MB, The Netherlands

Abstract. This article is about finite commutative semifields that are of rank 2 over their middle nucleus, the largest subset of elements that is a finite field. These semifields have a direct correspondence to certain flocks of the quadratic cone in $PG(3,q)$ and to certain ovoids of the parabolic space $Q(4,q)$. We shall consider these links, the known examples and non-existence results.

1 Semifields

A *finite semifield* $\mathcal{S}$ is a finite algebraic system that possesses two binary operations, addition and multiplication, which satisfy the following axioms.

(S1) Addition is a group with identity 0.
(S2) $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ for all a, b, $c \in \mathcal{S}$.
(S3) There exists an element $1 \neq 0$ such that $1a = a = a1$ for all $a \in \mathcal{S}$.
(S4) If $ab = 0$ then either $a = 0$ or $b = 0$.

Throughout this article the term semifield will refer to a finite semifield. The additive group of a semifield must be commutative. By (S2),

$$(ac+ad)+(bc+bd) = (a+b)(c+d) = (ac+bc)+(ad+bd).$$

Hence, $ad+bc = bc+ad$ and any elements that can be written as products commute under addition. By (S4) and finiteness, any element of $\mathcal{S}$ can be written as a product and so it follows that the additive group is abelian. Moreover it is not difficult to show that the group is elementary abelian. Let $a \neq 0$, and let p be the additive order of a. If p is not prime then we can write $p = rs$ for r and s integers not equal to 1, and by observing that $0 = (pa)a = (rsa)a = (ra)(sa)$ we get a contradiction from (S4). The fact that every nonzero element has prime order suffices to show that the group is elementary abelian, and that all nonzero elements have the same prime order p. This number p is the *characteristic* of the semifield. An elementary abelian group can be viewed as a vector space over a finite field. In particular $\mathcal{S}$ has p^n elements where n is the dimension of $\mathcal{S}$ over the field $GF(p)$. There are

* The author acknowledges the support of an EPSRC (UK) Advanced Research Fellowship AF/990 480.

many examples of semifields known and some standard constructions can be found in Knuth [19]. If the order is p, the semifield must be $GF(p)$. If the order is p^2, the semifield is $GF(p^2)$. This is not difficult to see. Let $\{1, x\}$ be a basis for the semifield. Multiplication is determined by $x^2 = ax + b$ and the polynomial $x^2 - ax - b$ has no roots in $GF(p)$ else we would have $x^2 - ax - b = (x - r)(x - s) = 0$ contradicting (S4). Thus $x^2 - ax - b$ is irreducible and the multiplication is $GF(p^2)$. This short argument comes again from [19] where it is also determined that the only semifield of order 8 is $GF(8)$. And completing the question of existence Albert [1] and Knuth [19] construct semifields that are not finite fields for every other order $q = p^h$, that is $h \geq 3$ if p is odd and $h \geq 4$ if $p = 2$.

The major motivation to study semifields in the 1960's was their use in the construction of projective planes, see Hughes and Piper [16] or Hall [15]. Every semifield determines a projective plane and the projective plane is Desarguesian if and only if the semifield is a field. The incidence structure constructed from a semifield $\mathcal{S}$ with

$$\begin{array}{lll} \text{Points: } (0,0,1) & \text{Lines: } [0,0,1] & \\ (0,1,a) & [0,1,a] & a \in \mathcal{S} \\ (1,a,b) & [1,a,b] & a,\, b \in \mathcal{S} \end{array}$$

such that the point (x_1, x_2, x_3) is incident with the line $[y_1, y_2, y_3]$ if and only if

$$y_1 x_3 = x_2 y_2 + x_1 y_3$$

is a projective plane $\pi(\mathcal{S})$ of order $|\mathcal{S}|$. It is a simple matter to check that any two points of $\pi(\mathcal{S})$ are incident with a unique line and dually that any two lines of $\pi(\mathcal{S})$ are incident with a unique point and hence that $\pi(\mathcal{S})$ is a projective plane. However it is harder to determine when two semifields $\mathcal{S}$ and $\mathcal{S}'$ determine the same projective plane, i.e. $\pi(\mathcal{S}) \cong \pi(\mathcal{S}')$. In [19] Knuth defines an *isotopism* from $\mathcal{S}$ to $\mathcal{S}'$ and shows that an isotopism is equivalent to a set of three 1-1 maps (F, G, H) linear over $GF(p)$ from $\mathcal{S}$ to $\mathcal{S}'$, such that

$$(ab)H = (aF)(bG)$$

for all a, b, $c \in \mathcal{S}$. Two semifields $\mathcal{S}$ and $\mathcal{S}'$ are *isotopic* if there is an isotopism from $\mathcal{S}$ to $\mathcal{S}'$. We have the following theorem due to Albert, a proof of which can be found in [19].

Theorem 1. *Two semifields coordinatize the same projective plane if and only if they are isotopic.*

In his original work on semifields Dickson [12] considered constructing commutative semifields, that is semifields that satisfy

(S5) $ab = ba$ for all a and b in $\mathcal{S}$.

We define the *middle nucleus* of a commutative semifield to be

$$\mathcal{N} := \{x \mid (ax)b = a(xb),\ \forall a, b \in \mathcal{S}\}.$$

It is clear that $\mathcal{N}$ contains the field $GF(p)$ where p is the characteristic and that $\mathcal{N}$ is itself a finite field. Moreover, $\mathcal{S}$ can be viewed as a vector space over its middle nucleus. Dickson [13] gave a construction of a commutative semifield of rank 2 over its middle nucleus. It is as follows. Let $\mathcal{S} := \{(x, y) \mid x, y \in GF(q)\}$ and let σ be an automorphism of $GF(q)$ where q is odd. Addition is defined component-wise and multiplication by

$$(x, y)(u, v) = (xv + yu, yv + mx^\sigma u^\sigma)$$

where m is a non-square in $GF(q)$. The only axiom that requires much thought is (S4) and we shall check this in a more general setting shortly. In this article we shall only be concerned with commutative semifields that are of rank 2 over their middle nucleus which have a correspondence with certain useful geometric objects.

Cohen and Ganley [10] made significant progress in the investigation of commutative semifields of rank 2 over their middle nucleus. They put Dickson's construction in the following more general setting. Let $\mathcal{S}$ be a commutative semifield of order q^2 with middle nucleus $GF(q)$. Then there is an $\alpha \in \mathcal{S} \setminus GF(q)$ such that $\{1, \alpha\}$ is a basis for $\mathcal{S}$. Addition in $\mathcal{S}$ is componentwise and multiplication is defined as

$$\begin{aligned}(x, y)(u, v) = (x\alpha + y)(u\alpha + v) &= xu\alpha^2 + (xv + yu)\alpha + yv \qquad (1)\\ &= (xv + yu + g(xu), yv + f(ux))\end{aligned}$$

where $x\alpha^2 = g(x)\alpha + f(x)$, f and g are functions from $GF(q) \to GF(q)$. The distributive laws are satisfied if and only if both f and g are linear maps, in other words, $f(x + y) = f(x) + f(y)$ and $g(x + y) = g(x) + g(y)$ for all x, y in $GF(q)$. Thus we must check (S4). Suppose that

$$(x\alpha + y)(u\alpha + v) = 0$$

and that x, y, u and v are non-zero. It follows that

$$g(xu) + xv + yu = 0$$

and

$$f(xu) + yv = 0$$

and eliminating y that

$$xv^2 + vg(xu) - uf(xu) = 0.$$

Writing $xu = z$ and $v/u = w$

$$zw^2 + g(z)w - f(z) = 0.$$

If one or more of x, y, u or v is zero it follows immediately that at least one of (x, y) or (u, v) is $(0, 0)$. Hence we have proved the following theorem which comes from [10].

Theorem 2. *Let $\mathcal{S}$ be a commutative semifield of rank 2 over its middle nucleus $GF(q)$. Then there exist linear functions f and g such that multiplication in $\mathcal{S}$ is defined as in (1) and $zw^2 + g(z)w - f(z) = 0$ has no solutions for all w, $z \in GF(q)$ and $z \neq 0$.*

If q is odd then this quadratic in w will have no solutions in $GF(q)$ if and only if

$$g(z)^2 + 4zf(z)$$

is a non-square for all $z \in GF(q)^*$. Cohen and Ganley [10] prove the following theorem for q even.

Theorem 3. *For q even the only commutative semifield of rank 2 over its middle nucleus $GF(q)$ is the finite field $GF(q^2)$.*

In light of this theorem we restrict ourselves to the case q is odd.

Let us consider again the example of Dickson. We have $g = 0$ and $f(z) = mz^\sigma$ where m is a non-square. We had only to check that (S4) is satisfied and this is clear since $g(z)^2 + 4zf(z) = 4mz^{\sigma+1}$ is a non-square for all $z \in GF(q)^*$.

2 Flocks of the Quadratic Cone

Let q be an odd prime power and let $\mathcal{K}$ be a quadratic cone of $PG(3, q)$ with vertex v and base a conic $\mathcal{C}$. The quadratic cones of $PG(3, q)$ are equivalent under the action of $PGL(4, q)$ so we can assume that v is the point $\langle 0, 0, 0, 1\rangle$ and the conic $\mathcal{C}$ in the plane π with equation $X_3 = 0$, is the set of zeros of $X_0X_1 = X_2^2$.

A *flock* $\mathcal{F}$ of $\mathcal{K}$ is a partition of $\mathcal{K} \setminus \{v\}$ into q conics. We call the planes that contain conics of the flock the *planes of the flock*. A flock $\mathcal{F}$ is equivalent to a flock $\mathcal{F}'$ if there is an element in the stabiliser group of the quadratic cone that maps the planes of the flock $\mathcal{F}$ to the planes of the flock $\mathcal{F}'$. If all the planes of the flock share a line then the flock is called *linear*.

Let

$$a_0X_0 + a_1X_1 + a_2X_2 + a_3X_3 = 0$$

be a plane of the flock. Since $\langle 0, 0, 0, 1\rangle$ is disjoint from any plane of the flock $a_3 \neq 0$ and hence we may assume that $a_3 = 1$. The point $\langle 1, 0, 0, -a_0\rangle$ is incident with the quadratic cone and this plane and hence the coefficients of X_0 in the planes of the flock are distinct. Hence we can parameterise by the elements of $GF(q)$ so that the planes of the flock are

$$\pi_t \,:\, tX_0 - f(t)X_1 + g(t)X_2 + X_3 = 0$$

where $t \in GF(q)$ and f and g are functions from $GF(q) \to GF(q)$.

The points that are incident with the line that is the intersection of two planes of the flock π_t and π_s are incident with the plane

$$(t-s)X_0 - (f(t)-f(s))X_1 + (g(t)-g(s))X_2 = 0.$$

The points that are incident with the cone $\mathcal{K}$ satisfy the equation $X_0X_1 = X_2^2$. If the equation

$$(t-s)X_2^2 - (f(t)-f(s))X_1^2 + (g(t)-g(s))X_1X_2 = 0$$

has a solution then we can find a line on the cone, by choosing the X_0 coordinate appropriately, that would be contained in the plane above, and hence a point on the cone and incident with both the planes π_t and π_s. The flock property implies that no such point exists and hence that this equation has no solutions. There is no solution with $X_1 = 0$ as this would imply that $X_2 = 0$ and that $t = s$. Hence we can put $w = X_2/X_1$ and we have the forward implication of the following theorem which is due to Thas [26].

Theorem 4. *Let $\mathcal{F}$ be a flock of the quadratic cone with vertex $\langle 0,0,0,1\rangle$ and base $X_0X_1 = X_2^2$. Then there exists functions f and g from $GF(q) \to GF(q)$ such that the planes of the flock are*

$$tX_0 - f(t)X_1 + g(t)X_2 + X_3 = 0$$

where $t \in GF(q)$ and $\mathcal{F}$ is a flock if and only if

$$(t-s)w^2 + (g(t)-g(s))w - (f(t)-f(s)) = 0$$

has no solution for all s and $t \in GF(q)$, $s \neq t$.

If f and g are additive then the condition of the theorem says that $\mathcal{F}$ is a flock if and only if

$$zw^2 + g(z)w - f(z) = 0$$

has no solutions for $w \in GF(q)$ and $z \in GF(q)^*$. A flock with this property is called a *semifield flock* as such a flock is in one-to-one correspondence with a commutative semifield of rank 2 over its middle nucleus. This is clear from Theorem 2. The commutative semifield $\mathcal{S} = \{(x,y) \mid x,y \in GF(q)\}$ where addition is defined component-wise and multiplication is defined by

$$(x,y)(u,v) = (xv + yu + g(xu), yv + f(xu))$$

is the semifield associated to the flock $\mathcal{F}$.

The known examples of semifield flocks up to equivalence are listed in Table 2. In all relevant cases m is taken to be a non-square in $GF(q)$ and σ is a nontrivial automorphism of $GF(q)$. Some of the links between the commutative semifields, certain ovoids of $Q(4,q)$, semifield flocks of the quadratic cone

name	$g(x)$	$f(x)$	$q=p^h$
linear	0	mx	all
Dickson [12] Kantor [18] Knuth [19]	0	mx^σ	
Cohen-Ganley [10] Thas-Payne [28]	x^3	$m^{-1}x+mx^9$	3^h
Penttila-Williams [24], Bader-Lunardon-Pinneri [4]	x^3	x^{27}	3^5

Table 1. The known examples of semifield flocks up to equivalence

and semifield translation planes were not known until recently and hence in most cases more than one person or persons is accredited with the discovery of the functions f and g. In fact in the second case Dickson [12] discovered the semifield, Kantor [18] the ovoid and Knuth [19] the semifield plane. In the third example Cohen and Ganley [10] discovered the semifield while Thas and Payne found the ovoid [28]. And in the fourth example Penttila and Williams discovered the ovoid [24] and details concerning the corresponding flock were investigated by Bader, Lunardon and Pinneri [4]. We shall discuss these equivalent objects in the following sections and explain the links between them and how this can be of use. Firstly however we shall check that the last two examples in Table 2 do indeed satisfy the condition of Theorem 2 and Theorem 4. In the Cohen-Ganley Thas-Payne example

$$g(x)^2+4xf(x)=g(x)^2+xf(x)=x^6+m^{-1}x^2+mx^{10}=m(x^5-m^{-1}x)^2$$

which is a non-square for all $x\in GF(3^h)^*$.

The Penttila-Williams example is somewhat more difficult to prove. The following comes from [2]. We have that

$$g(x)^2+4xf(x)=g(x)^2+xf(x)=x^6+x^{28}=x^6(1+x^{22})$$

and since $3^5-1=242=2.11^2$ we need to show that $1+\epsilon$ is a non-square for all ϵ such that $\epsilon^{11}=1$. Now $(q-1)/2=121=1+3+3^2+3^3+3^4$ and in $GF(3^5)$

$$(1+\epsilon)^{121}=(1+\epsilon)(1+\epsilon^3)(1+\epsilon^9)(1+\epsilon^{27})(1+\epsilon^{81}).$$

The set $\{1,3,9,27,81\}$ are the squares modulo 11 and each non-zero integer modulo 11 can be written exactly 3 times as the sum of elements of $\{1,3,9,27,81\}$ modulo 11. Hence in $GF(3^5)$

$$(1+\epsilon)^{121}=2=-1$$

and $1+\epsilon$ is a non-square for all ϵ such that $\epsilon^{11}=1$.

The following theorem comes from [14].

Theorem 5. *The projective planes obtained from the flocks $\mathcal{F}$ and $\mathcal{F}'$ are isomorphic if and only if the flocks $\mathcal{F}$ and $\mathcal{F}'$ are equivalent.*

The projective planes in Theorem 5 are constructed, via the Bruck Bose André method, from the spread

$$\{\langle(y, x, 1, 0), (f(x), y + g(x), 0, 1)\rangle \mid x, y \in GF(q)\} \cup \{\langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle\}.$$

This plane is a semifield plane. Following [11, (5.1.2)] the spread comes from the spread set

$$\mathcal{D} = \left\{ \begin{pmatrix} y + g(x) & x \\ f(x) & y \end{pmatrix} \mid x, y \in GF(q) \right\}$$

which has the property that the determinant of $M - N$ is non-zero for all distinct M, $N \in \mathcal{D}$. The plane is coordinatised by the semifield whose multiplication is defined by

$$\begin{pmatrix} x \\ y \end{pmatrix} . \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} v + g(u) & u \\ f(u) & v \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} xv + yu + xg(u) \\ yv + xf(u) \end{pmatrix}.$$

We can check that this multiplication defines a semifield. It is only condition (S4) that requires some work. If

$$xg(u) + xv + yu = 0$$

and

$$xf(u) + yv = 0$$

then

$$xv^2 + xg(u)v - xuf(u) = 0.$$

If $x = 0$ one can check that then one of either (x, y) or (u, v) is equal to $(0, 0)$. If $x \neq 0$ then, since $g(u)^2 + 4uf(u)$ is a non-square for all $u \in GF(q)^*$, $u = 0$ and it follows that $(u, v) = (0, 0)$. Hence this is a semifield. Note that this means we can construct a not necessarily commutative semifield from the functions f and g. Now semifields that we get from the above multiplication will be isotopic if there corresponding flocks are equivalent by Theorem 1 and Theorem 5. However we have not proved that the commutative semifields that we get from the functions f and g are isotopic if and only if their associated flocks are equivalent.

The following theorem which we prove in Section 6 shows that there is an isotopism between two commutative semifields if their associated flocks are equivalent.

Theorem 6. *$\mathcal{F}$ and $\hat{\mathcal{F}}$ are equivalent semifield flocks if and only if there exists a linear one-to-one map F from $\mathcal{S}$ to $\hat{\mathcal{S}}$ and a $GF(p)$-linear map H from $\mathcal{S}$ to $\hat{\mathcal{S}}$ such that*

$$(ab)H = (aF).(bF)$$

for all a, $b \in \mathcal{S}$ where $.$ is multiplication in $\hat{\mathcal{S}}$ and $\mathcal{F}$ and $\hat{\mathcal{F}}$ are the semifield flocks associated to the commutative semifields $\mathcal{S}$ and $\hat{\mathcal{S}}$ of rank 2 over their middle nucleus $GF(q)$, $q = p^n$, respectively.

Let us consider for the moment a flock that is linear, i.e. with the property that all the planes of the flock contain a common line. The points that are dual to the planes of the flock

$$\{\langle t, -f(t), g(t), 1\rangle \mid t \in GF(q)\}$$

are collinear and so $(f(t)-f(s))/(t-s)$ and $(g(t)-g(s))/(t-s)$ are constant for all $s \neq t$. Hence f and g have polynomial degree 1. The following theorem is from Thas [26].

Theorem 7. *A flock whose planes are all incident with a common point is either linear (in which case the planes of the flock share a common line) or equivalent to a semifield flock of Dickson, Kantor, Knuth type.*

Remark 1. It follows from this theorem that the semifield flocks we obtain directly from the Cohen-Ganley so-called sporadic example of a semifield and the semifields from [25] are equivalent to a semifield flock of Dickson, Kantor, Knuth type. In [25, Theorem 1] $g(t) = t^{\sqrt{q}}$ and $f(t) = ct$ and it is a simple matter to check that the planes of the flock are all incident with the point $\langle c, 1, 0, 0\rangle$ and in [25, Theorem 2] $g(t) = at + bt^{\sqrt{q}}$ and $f(t) = t$ and the planes of the flock are all incident with the point $\langle 1, 1, 0, 0\rangle$. As mentioned in [14] the sporadic example of Cohen and Ganley over $GF(5^2)$ with $g(t) = t^5$ and $f(t) = 2\sqrt{2}t^5 + t$ the planes of the flock are all incident with the point $\langle 1, 1, 2\sqrt{2}, 0\rangle$. By Theorem 6 their associated commutative semifields are isotopic to a Dickson, Kantor, Knuth semifield. All known examples of commutative semifields rank 2 over their middle nucleus are isotopic to one of the commutative semifields rank 2 over their middle nucleus constructed from the pairs of functions in Table 1.

In the following argument we are going to use the so-called *linear representation* of $PG(2, q)$ so let us recall what we mean by this (for more details see [22]). Let $GF(q_0)$ be a subfield of $GF(q)$, $q = q_0^n$. Let $\mathcal{V}$ be the vector space of rank 3 over $GF(q)$. The projective plane $PG(2, q)$ is the incidence geometry whose points are the subspaces of rank 1 of $\mathcal{V}$ and whose lines are the subspaces of rank 2 of $\mathcal{V}$. However $\mathcal{V}$ is a vector space of rank $3n$ over $GF(q_0)$ and the points of $PG(2, q)$ are subspaces of rank n which are mutually disjoint and cover $\mathcal{V} \setminus \mathbf{0}$, i.e. they form a spread Λ. The spread Λ induces a spread in the subspace generated by any two elements of Λ (since this subspace is a line of $PG(2, q)$). We call a spread with this property *normal*.

Let us consider a semifield flock $\mathcal{F}$. The points

$$\{\langle t, -f(t), g(t), 1\rangle \mid t \in GF(q)\}$$

that are dual to the planes of the flock project on to the plane $X_3 = 0$ the set of points

$$\mathcal{W} := \{\langle t, -f(t), g(t), 0\rangle \mid t \in GF(q)\}.$$

Since the functions f and g are additive, they are linear over some subfield $GF(q_0)$ of $GF(q)$. The maximum subfield with this property is often called the kernel of the flock. This kernel is equal to the left nucleus of the semifield (and hence equal to the right nucleus since the semifield is commutative). If we look at the linear representation of the plane $X_3 = 0$ the set $\mathcal{W}$ is a subspace of rank n over $GF(q_0)$.

The vertex of the quadratic cone is the point $\langle 0, 0, 0, 1\rangle$ and this point is dual to the plane $X_3 = 0$ and the $q + 1$ lines on the quadratic cone are dual to a set of $q + 1$ lines in the plane $X_3 = 0$ that are tangents to some conic $\mathcal{C}'$. The definition of a flock implies that the points in $\mathcal{W}$ are not incident with a tangent to this conic $\mathcal{C}'$, i.e. the set $\mathcal{W}$ is contained in the internal points of the conic $\mathcal{C}'$. If the flock is linear then the set $\mathcal{W}$ is a point of the plane $X_3 = 0$. Theorem 7 implies that the flock is of Dickson, Kantor, Knuth type if and only if the set $\mathcal{W}$ is contained in a line of the plane $X_3 = 0$. In all other cases the set $\mathcal{W}$ in the linear representation contains a subplane $PG(2, q_0)$ that is contained in the internal points of a conic in $PG(2, q)$. However this cannot always occur. The following is from [5].

Theorem 8. *If there is a subplane of order q_0 contained in the internal points of a conic in $PG(2, q)$ where $q = q_0^n$ then $q_0 < 4n^2 - 8n + 2$.*

The above argument leads immediately to the following corollaries.

Corollary 1. *A semifield flock of the quadratic cone of $PG(3, q)$ whose defining functions f and g are linear over the subfield $GF(q_0)$ where $q = q_0^n$ and $q_0 \geq 4n^2-8n+2$ is either a linear flock or a Dickson, Kantor, Knuth semifield flock.*

Corollary 2. *A commutative semifield of rank 2 over its middle nucleus $GF(q)$ that has defining functions f and g which are linear over the subfield $GF(q_0)$ where $q = q_0^n$ and $q_0 \geq 4n^2 - 8n + 2$ is either the finite field $GF(q^2)$ or isotopic to a Dickson, Kantor, Knuth semifield.*

Remark 2. We may expect something much stronger than this bound to hold. Indeed we can see that the theorem hypothesis requires that their is a subplane in the internal points of the conic. However in fact the set $\mathcal{W}$ is contained in the internal points of a conic and in the linear representation of $PG(2, q)$ it is a subspace of rank n over $GF(q_0)$.

The bound in the theorem for $n = 3$ gives $q_0 < 14$ and by computer Bloemen, Thas and van Maldeghem [7] have checked that there are no other semifield flocks other than the linear flock and the Dickson, Kantor, Knuth flocks. Note also that the only other known examples have $q_0 = 3$.

The following nice result of Bader and Lunardon [3] shows that in some sense the Pentilla-Williams example is sporadic, and any other examples yet to discovered.

Theorem 9. *If there is a polynomial $h(t)$ over $GF(q)$ such that for a fixed non-square m in $GF(q)$ the equality*

$$g(t) + 4tf(t) = mh(t)$$

is a polynomial identity then f and g are one of the first three examples in Table 1.

3 The generalized quadrangle $T(\mathcal{E})$

A *generalized quadrangle* is a set of points and a set of lines with an incidence relation that satisfies the following axioms.

(Q1) Every two points are incident with at most one line.
(Q2) For all anti-flags (p, L) (the point p is not incident with the line L) there is exactly one point incident with L and collinear with p.
(Q3) There is no point collinear with all others.

Let G be a generalized quadrangle in which there is a line incident with at least three points and a point incident with at least three lines. It is not difficult to prove that the number of points incident with a line, and the number of lines incident with a point, are constants. We say G is a generalized quadrangle of order s, t if every line is incident with $s+1$ points and every point is incident with $t+1$ lines.

An *egg* $\mathcal{E}_{m,n}$ of $PG(2n+m-1,q)$ is a set of q^m+1 $(n-1)$-subspaces with the properties that any three elements of $\mathcal{E}_{m,n}$ span a $(3n-1)$-space and every element of $\mathcal{E}_{m,n}$ is contained in a $(n+m-1)$-subspace called a *tangent space* that is skew from all other elements of $\mathcal{E}_{m,n}$. We write $\mathcal{E}$ for $\mathcal{E}_{m,n}$ when no confusion is possible.

The following construction of the generalized quadrangle $T(\mathcal{E}_{m,n})$ from an egg is based on a construction due to Tits and comes from Payne and Thas [23]. Let $\mathcal{E}_{m,n}$ be an egg of $\pi = PG(2n+m-1,q)$ and embed the space π in $PG(2n+m,q)$. Points are defined as

(i) the points of $PG(2n+m,q) \setminus \pi$,
(ii) the $(n+m)$-spaces of $PG(2n+m,q)$ that contain a tangent space of $\mathcal{E}_{m,n}$ but are not contained in π,
(iii) a symbol (∞).

Lines are defined as

(a) the n-spaces of $PG(2n+m,q)$ which contain an element of $\mathcal{E}_{m,n}$ but are not contained in π,
(b) the elements of $\mathcal{E}_{m,n}$.

Incidence is as follows. A point of type (i) is incident with a line of type (a) if they are incident in $PG(2n+m,q)$. A point of type (ii) is incident with the lines of type (a) which it contains and the unique line of type (b) which it contains. The point of type (iii) is incident with all lines of type (b).

$T(\mathcal{E}_{m,n})$ is a generalized quadrangle of order (q^n, q^m), [23, Theorem 8.7.1] or [20, Theorem 3.3.1]. Let $\mathcal{C}$ be a non-singular conic in $PG(2, q_0^n)$. In the linear representation described in the previous section the $q_0^n + 1$ points of $\mathcal{C}$ become $q_0^n + 1$ $(n-1)$-subspaces of $PG(3n-1, q_0)$ which form an egg $\mathcal{E}_{\mathcal{C}}$ whose tangent spaces correspond to the set of tangent lines of $\mathcal{C}$. The generalized quadrangle $T(\mathcal{E}_{\mathcal{C}})$ is the Tits generalized quadrangle $T_2(\mathcal{C})$ of order (q_0^n, q_0^n).

An *ovoid* $\mathcal{O}$ of a generalised quadrangle is a set of points with the property that every line is incident with exactly one point of $\mathcal{O}$. An ovoid of a generalised quadrangle of order (s,t) contains $st+1$ points.

Let us consider an ovoid $\mathcal{O}$ of $T_2(\mathcal{C})$ that contains the point (∞). The set $\mathcal{O} \setminus \{(\infty)\}$ is a set of q^{2n} points of type (a) with the property that the line of $PG(3n, q_0)$ spanned by any two of them meets π in a point not contained in an element of the egg $\mathcal{E}_{\mathcal{C}}$.

Let us consider again the set $\mathcal{W}$ from the previous section which is contained in the internal points of a conic $\mathcal{C}'$. In the linear representation $\mathcal{W}$ is a $(n-1)$-subspace of a $(3n-1)$-space π' disjoint from all elements and all tangent spaces of the egg $\mathcal{E}_{\mathcal{C}'}$. In the dual space the space $\mathcal{W}^*$ dual to $\mathcal{W}$ is a $(2n-1)$-subspace of a $(3n-1)$-space π disjoint from the $(n-1)$-subspaces dual to the tangent spaces. In the dual setting we have an egg $\mathcal{E}_{\mathcal{C}}$ where $\mathcal{C}$ is the dual of the conic $\mathcal{C}'$. Embed π in a $(3n)$-space and let P be any point of $PG(3n,q) \setminus \pi$. The $(2n)$-subspace $\langle \mathcal{W}^*, P \rangle$ has the property that any two of its points span a line that meets π in point not in the egg $\mathcal{E}_{\mathcal{C}}$. Hence

$$(\langle \mathcal{W}^*, P \rangle \setminus \pi) \cup \{(\infty)\}$$

is an ovoid of the generalised quadrangle $T_2(\mathcal{C})$.

The above argument was first explained by Thas [27].

4 Ovoids of $Q(4,q)$

In this section we shall see that $T_2(\mathcal{C})$ is isomorphic to the classical generalised quadrangle $Q(4,q)$ and hence that commutative semifields of rank 2 over their middle nucleus imply certain ovoids of $Q(4,q)$.

A quadratic form $Q(\mathbf{x})$ on a vector space $\mathcal{V}$ over a field F satisfies the axioms

$$Q(\lambda \mathbf{x}) = \lambda^2 Q(\mathbf{x}) \text{ for all } \mathbf{x} \in \mathcal{V}$$

$$Q(\mathbf{x}+\mathbf{y}) = Q(\mathbf{x}) + Q(\mathbf{y}) + b(\mathbf{x},\mathbf{y})$$

where $b(\mathbf{x},\mathbf{y})$ is a bilinear form. A *totally singular* subspace $\mathcal{S}$ is a subspace with the property that $Q(\mathbf{x}) = 0$, $Q(\mathbf{y}) = 0$ and $b(\mathbf{x},\mathbf{y}) = 0$ for all $\mathbf{x}$, $\mathbf{y} \in \mathcal{S}$.

We restrict ourselves to the case where the field $F = GF(q)$ and the maximum rank of a totally singular subspace is 2. The classification of quadratic forms over a finite field says that there are three such inequivalent non-singular quadratic forms (for more details on the equivalence and singularity of quadratic forms see [8]). Let $\mathcal{G}$ denote the geometry whose points are the totally singular subspaces of rank 1 and whose lines are the totally singular subspaces of rank 2 for one of these quadratic forms. Let $\langle \mathbf{x} \rangle$ and $\mathcal{S}$ be totally singular subspaces of rank 1 and 2 respectively such that $\mathbf{x} \notin \mathcal{S}$, i.e. a non-incident point and line of $\mathcal{G}$. The rank of $\mathcal{S} \cap \mathbf{x}^\perp$ where $\mathbf{x}^\perp := \{\mathbf{z} \in \mathcal{V} \mid b(\mathbf{x}, \mathbf{z}) = 0\}$ is 1 since $\mathbf{x}^\perp$ is a hyperplane not containing $\mathcal{S}$. In terms of the geometry this implies that for a non-incident point P and line l of $\mathcal{G}$ there is a unique point P' incident with l and collinear with P. Hence from the three quadratic forms we obtain three generalised quadrangles which are called the classical orthogonal generalised quadrangles. These are listed in Table 2 in which g is an irreducible homogeneous quadratic form.

name	label	n	Canonical form
Hyperbolic	$Q^+(3,q)$	4	$Q(\mathbf{x}) = x_0x_1 + x_2x_3$
Parabolic	$Q(4,q)$	5	$Q(\mathbf{x}) = x_0x_1 + x_3x_4 - x_2^2$
Elliptic	$Q^-(5,q)$	6	$Q(\mathbf{x}) = x_0x_1 + x_2x_3 + g(x_4,x_5)$

Table 2. The classical orthogonal generalised quadrangles

An ovoid $\mathcal{O}$ of a classical orthogonal generalised quadrangle of order (s,t) is a set of $st+1$ totally singular subspaces of rank 1 with the property that for all distinct $\langle \mathbf{x} \rangle, \langle \mathbf{y} \rangle \in \mathcal{O}$ the bilinear form $b(\mathbf{x}, \mathbf{y}) \neq 0$.

Let the generalised quadrangle $Q(4,q)$ of order (q,q) be defined by the quadratic form

$$Q(\mathbf{x}) = x_0x_1 + x_3x_4 - x_2^2.$$

An ovoid $\mathcal{O}$ of $Q(4,q)$ has q^2+1 points. We may assume that $\langle 0,0,0,0,1 \rangle \in \mathcal{O}$. The associated bilinear form to Q is

$$b(\mathbf{x}, \mathbf{y}) = x_0y_1 + y_0x_1 + x_3y_4 + x_4y_3 - 2x_2y_2.$$

For any $\langle x \rangle \in \mathcal{O}$

$$0 \neq b(\mathbf{x}, \langle 0,0,0,0,1 \rangle) = x_3$$

and hence we can assume that $x_3 = 1$. Moreover if $\mathbf{x} = (x_0, x_1, x_2, 1, x_4)$ and $\mathbf{y} = (x_0, y_1, x_2, 1, y_4)$ where $\langle x \rangle$ and $\langle y \rangle \in \mathcal{O}$ then

$$b(\mathbf{x}, \mathbf{y}) = x_0y_1 + x_0x_1 + y_4 + x_4 - 2x_2^2 = Q(\mathbf{x}) + Q(\mathbf{y}) = 0$$

and so the first and third coordinate pair are distinct pairs for distinct points of the ovoid. Hence there is a polynomial $F(x,y)$ such that the ovoid

$$\mathcal{O} = \{\langle x, F(x,y), y, 1, y^2 - xF(x,y) \rangle \mid x, y \in GF(q)\} \cup \{\langle 0,0,0,0,1 \rangle\}.$$

name	$F(x,y)$	q	restrictions
elliptic quadrics	mx	all	
Kantor [18]	mx^α	odd	$\alpha \in Aut(GF(q))$
Thas-Payne [28]	$m^{-1}x + (mx)^{1/9} + y^{1/3}$	3^h	
Penttila-Williams [24]	$x^9 + y^{81}$	3^5	
Ree-Tits slice [18]	$x^{2\alpha+3} + y^\alpha$	3^{2h+1}	$\alpha = \sqrt{3q}$
Tits [29]	$x^{\alpha+1} + y^\alpha$	2^{2h+1}	$\alpha = \sqrt{2q}$

Table 3. The known examples of ovoids of $Q(4,q)$

In the article of Penttila and Williams [24] the stabiliser group of each of the known ovoids is calculated. Note that in four examples of Table 3 $F(x,y) = f(x) + g(y)$ where f and g are linear over some subfield of $GF(q)$. In the previous section we constructed an ovoid of $T_2(\mathcal{C})$ from a semifield flock. However the generalised quadrangle $T_2(\mathcal{C})$ is isomorphic to $Q(4,q)$. Let $\phi : Q(4,q) \to T_2(\mathcal{C})$, where $\mathcal{C}$ is the conic $X_0X_1 = X_2^2$, be the map

$$\begin{aligned}
\langle 0,0,0,0,1\rangle &\mapsto (\infty)\\
\langle a,b,c,1,c^2-ab\rangle &\mapsto \langle a,b,c,1\rangle\\
\langle a^2,1,a,0,b\rangle &\mapsto \langle (a^2,1,a,0),(-b,0,0,1)\rangle\\
\langle 1,0,0,0,a\rangle &\mapsto \langle (1,0,0,0),(0,-a,0,1)\rangle.
\end{aligned}$$

This is indeed an isomorphism since collinearity is preserved. The points $\langle \mathbf{x}\rangle = \langle a,b,c,1,c^2-ab\rangle$ and $\langle \mathbf{x}'\rangle = \langle a',b',c',1,c'^2-a'b'\rangle$ are collinear in $Q(4,q)$ if and only if $b(\mathbf{x},\mathbf{x}') = ab' + ba' - ab - a'b' + c^2 - 2cc' + c'^2 = (c-c')^2 - (a-a')(b-b') = 0$ if and only if the point $\langle a-a', b-b', c-c'\rangle$ lies on the conic $X_0X_1 = X_2^2$. One can check that the other incidences are preserved.

Hence from the ovoid of $T_2(\mathcal{C})$ that was constructed in the previous section we get an ovoid of $Q(4,q)$. In the next section we shall use explicit coordinates to calculate $F(x,y)$ from the functions f and g that determine the semifield flock. The following theorem is from Lunardon [22].

Theorem 10. *If $\mathcal{F}$ and $\mathcal{F}'$ are semifield flocks of the quadratic cone then the ovoids that come from the flocks are equivalent if and only if the flocks $\mathcal{F}$ and $\mathcal{F}'$ are equivalent.*

5 Correspondence between the ovoid and the flock using coordinates

As in [20] we follow the argument of Thas [27] using coordinates. Let us see how this works. It may help to refer back to end of Section 3.

The lines on the quadratic cone with vertex $\langle 0,0,0,1\rangle$ and base defined by the equation $X_0X_1 = X_2^2$ dualise with respect to the standard inner product

to lines in the plane $X_3 = 0$ with equation

$$X_0 + a^2 X_1 + aX_2 = 0.$$

These lines are tangents to the conic whose points are the zeros of the quadratic form $\mathcal{Q}' = 4X_0X_1 - X_2^2$. The associated bilinear form is

$$b'(\mathbf{x}, \mathbf{y}) = 4x_0y_1 + 4y_0x_1 - 2x_2y_2.$$

We wish to view the vector space of rank 3 over $GF(q)$ as a vector space of rank $3n$ over $GF(q_0)$ and the bilinear form b' over this vector space is

$$\hat{b}(\mathbf{x}, \mathbf{y}) = Tr_{q\to q_0}(4x_0y_1 + 4y_0x_1 - 2x_2y_2).$$

In Section 3 the set $\mathcal{W}$ is contained in the hyperplane $X_3 = 0$ and is the set of points $\{\langle t, -f(t), g(t)\rangle \mid t \in GF(q)\}$. The functions f and g are linear over some subfield $GF(q_0)$ and so we can write

$$f(t) = \sum_{i=0}^{n-1} c_i t^{q_0^i} \quad \text{and} \quad g(t) = \sum_{i=0}^{n-1} b_i t^{q_0^i}.$$

We follow the argument at the end of Section 3 and dualise with respect to the bilinear form $\hat{b}$. A point $\langle x_0, x_1, x_2\rangle \in \mathcal{W}^*$ if and only if

$$Tr_{q\to q_0}(-4x_0f(t) + 4x_1t - 2x_2g(t)) = 0$$

for all $t \in GF(q)$ if and only if

$$Tr_{q\to q_0}((-4c_0x_0 + 4x_1 - 2b_0x_2)t + \sum_{i=1}^{n-1}(-4c_ix_0 - 2b_ix_2)t^{q_0^i}) = 0$$

if and only if

$$Tr_{q\to q_0}((-4c_0x_0 + 4x_1 - 2b_0x_2 + \sum_{i=1}^{n-1}(-4c_ix_0 - 2b_ix_2)^{q_0^{n-i}})t) = 0$$

for all $t \in GF(q)$. Hence

$$4x_1 = \sum_{i=0}^{n-1}(4c_ix_0 + 2b_ix_2)^{q_0^{n-i}}.$$

The set

$$\mathcal{W}^* = \{\langle x_0, \sum_{i=0}^{n-1}(c_ix_0 + \frac{1}{2}b_ix_2)^{q_0^{n-i}}, x_2\rangle \mid x_0, x_2 \in GF(q)\}.$$

Now if we were to cone $\mathcal{W}^*$ to the set $\langle W^*, P\rangle$ where P is a point not on the hyperplane $X_3 = 0$ we would have q^2 points of an ovoid of the $\mathcal{T}_2(\mathcal{C})$ defined with conic $4X_0X_1 = X_2^2$. However we wish to have an ovoid of the $\mathcal{T}_2(\mathcal{C})$ defined by the conic $X_0X_1 = X_2^2$ and so we use the map ψ that takes

$$\begin{aligned} X_0 &\mapsto X_0 \\ X_1 &\mapsto X_1 \\ X_2 &\mapsto \tfrac{1}{2}X_2 \end{aligned}$$

and maps the subspace $\mathcal{W}^*$ to the subspace

$$\{\langle x, F(x,y), y\rangle \mid x, y \in GF(q)\}$$

where

$$F(x,y) = \sum_{i=0}^{n-1} (-c_i x + b_i y)^{q_0^{n-i}}.$$

We take the point P to be the point $\langle 0,0,0,1\rangle$ so that the set

$$\{\langle x, F(x,y), y, 1\rangle \mid x, y \in GF(q)\}$$

is a set of q^2 points of an ovoid of $T_2(\mathcal{C})$. We apply the isomorphism ϕ^{-1} from the previous section to give the explicit points of an ovoid of $Q(4,q)$ that comes from the semifield flock defined by the functions f and g,

$$\mathcal{O} = \{\langle x, F(x,y), y, 1, y^2 - xF(x,y) \mid x, y \in GF(q)\} \cup \{\langle 0,0,0,0,1\rangle\}.$$

6 Correspondence between the commutative semifield and the flock

In this section we look at the correspondence between the commutative semifields of rank 2 over their middle nucleus and the associated semifield flocks. This is a proof of Theorem 6.

Let $\mathcal{S}$ and $\hat{\mathcal{S}}$ be commutative semifields of rank 2 over their middle nucleus $GF(q)$, $q = p^n$, constructed from the pairs of functions (f,g) and $(\hat{f},\hat{g})$ respectively. The functions f, g, $\hat{f}$, $\hat{g}$ are linear over $GF(p)$ so we can write them as

$$f(x) = \sum_{i=0}^{n-1} f_i x^{p^i}, \quad g(x) = \sum_{i=0}^{n-1} g_i x^{p^i},$$

$$\hat{f}(x) = \sum_{i=0}^{n-1} \hat{f}_i x^{p^i}, \quad \hat{g}(x) = \sum_{i=0}^{n-1} \hat{g}_i x^{p^i}.$$

Let us assume that there exists a one-to-one $GF(p)$-linear map H from $\mathcal{S}$ to $\hat{\mathcal{S}}$ and a one-to-one linear map F from $\mathcal{S}$ to $\hat{\mathcal{S}}$ such that

$$((x,y)(u,v))H = ((x,y)F).((u,v)F)$$

for all (x,y) and $(u,v) \in \mathcal{S}$. Expanding the left-hand side we get

$$((x,y)(u,v))H = ((xv + yu + \hat{g}(ux), yv + \hat{f}(ux))H$$

$$= \left(\sum_{i=0}^{n-1} h_i(xv + yu + \hat{g}(ux))^{p^i} + \sum_{i=0}^{n-1} m_i(yv + \hat{f}(ux))^{p^i}, \right.$$
$$\left. \sum_{i=0}^{n-1} k_i(xv + yu + \hat{g}(ux))^{p^i} + \sum_{i=0}^{n-1} l_i(yv + \hat{f}(ux))^{p^i} \right),$$

for some h_i, m_i, k_i and l_i. Expanding the right-hand side we get

$$((x,y)F).((u,v)F) = (\alpha_0 x + \alpha_1 y, \beta_0 x + \beta_1 y).(\alpha_0 u + \alpha_1 v, \beta_0 u + \beta_1 v) =$$
$$(2\alpha_0\beta_0 xu + 2\alpha_1\beta_1 yv + (\alpha_0\beta_1 + \alpha_1\beta_0)(xv + yu) +$$
$$g((\alpha_0 x + \alpha_1 y)(\alpha_0 u + \alpha_1 v)),$$
$$\beta_0^2 xu + \beta_1^2 yv + \beta_0\beta_1(xv + yu) + f((\alpha_0 x + \alpha_1 y)(\alpha_0 u + \alpha_1 v))),$$

for some α_0, α_1, β_0 and β_1. Equate the coefficient of $(yv)^{p^i}$ to get

$$(i > 0) \;\; m_i = \alpha_1^{2p^i} g_i \quad (i = 0) \;\; m_0 = 2\alpha_1\beta_1 + \alpha_1^2 g_0,$$

$$(i > 0) \;\; l_i = \alpha_1^{2p^i} f_i \quad (i = 0) \;\; l_0 = \beta_1^2 + \alpha_1^2 f_0.$$

Equate the coefficient of $(yu)^{p^i}$ to get

$$(i > 0) \;\; h_i = (\alpha_0\alpha_1)^{p^i} g_i \quad (i = 0) \;\; h_0 = \alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_0\alpha_1 g_0,$$

$$(i > 0) \;\; k_i = (\alpha_0\alpha_1)^{p^i} f_i \quad (i = 0) \;\; k_0 = \beta_0\beta_1 + \alpha_0\alpha_1 f_0.$$

Equate the coefficient of $(xu)^{p^j}$ to get

$$(j > 0) \quad \sum_{i=0}^{n-1} h_i \hat{g}_{j-i} + \sum_{i=0}^{n-1} m_i \hat{f}_{j-i} = \alpha_0^{2p^j} g_j,$$

$$(j = 0) \quad \sum_{i=0}^{n-1} h_i \hat{g}_{n-i} + \sum_{i=0}^{n-1} m_i \hat{f}_{n-i} = 2\alpha_0\beta_0 + \alpha_0^2 g_0,$$

$$(j > 0) \quad \sum_{i=0}^{n-1} k_i \hat{g}_{j-i} + \sum_{i=0}^{n-1} l_i \hat{f}_{j-i} = \alpha_0^{2p^j} f_j,$$

$$(j = 0) \quad \sum_{i=0}^{n-1} k_i \hat{g}_{n-i} + \sum_{i=0}^{n-1} l_i \hat{f}_{n-i} = \beta_0^2 + \alpha_0^2 f_0,$$

where all indices are taken modulo n. Substitute the expressions for the h_i, m_i, k_i and l_i in the previous four equations and get the equations A_j for $j = 1, \ldots, n-1$

$$\sum_{i=0}^{n-1} (\alpha_0\alpha_1)^{p^i} g_i \hat{g}_{j-i} + (\alpha_0\beta_1 + \alpha_1\beta_0)\hat{g}_j + \sum_{i=0}^{n-1} \alpha_1^{2p^i} g_i \hat{f}_{j-i} + 2\alpha_1\beta_1 \hat{f}_j = \alpha_0^{2p^j} g_j,$$

the equation A_0

$$\sum_{i=0}^{n-1}(\alpha_0\alpha_1)^{p^i}g_i\hat{g}_{n-i}+(\alpha_0\beta_1+\alpha_1\beta_0)\hat{g}_0+\sum_{i=0}^{n-1}\alpha_1^{2p^i}g_i\hat{f}_{n-i}+2\alpha_1\beta_1\hat{f}_0=$$

$$2\alpha_0\beta_0+\alpha_0^2g_0,$$

the equations B_j for $j=1,\ldots,n-1$

$$\sum_{i=0}^{n-1}(\alpha_0\alpha_1)^{p^i}f_i\hat{g}_{j-i}+\beta_0\beta_1\hat{g}_j+\sum_{i=0}^{n-1}\alpha_1^{2p^i}f_i\hat{f}_{j-i}+\beta_1^2\hat{f}_j=\alpha_0^{2p^j}f_j,$$

and the equation B_0

$$\sum_{i=0}^{n-1}(\alpha_0\alpha_1)^{p^i}f_i\hat{g}_{n-i}+\beta_0\beta_1\hat{g}_0+\sum_{i=0}^{n-1}\alpha_1^{2p^i}f_i\hat{f}_{n-i}+\beta_1^2\hat{f}_0=\beta_0^2+\alpha_0^2f_0.$$

Now the sums $\sum_{j=0}^{n-1}A_jt^{p^j}$ and $\sum_{j=0}^{n-1}B_jt^{p^j}$ give

$$g(\alpha_0\alpha_1\hat{g}(t))+(\alpha_0\beta_1+\beta_0\alpha_1)\hat{g}(t)+g(\alpha_1^2\hat{f}(t))+2\alpha_1\beta_1\hat{f}(t)=2\alpha_0\beta_0t+g(\alpha_0^2t)$$

and

$$f(\alpha_0\alpha_1\hat{g}(t))+\beta_0\beta_1\hat{g}(t)+f(\alpha_1^2\hat{f}(t))+\beta_1^2\hat{f}(t)=\beta_0^2t+f(\alpha_0^2t).$$

The functions f and g are additive and so these equations can be written as

$$g(-\alpha_0^2t+\alpha_1^2\hat{f}(t)+\alpha_1\alpha_0\hat{g}(t))=2\alpha_0\beta_0t-2\alpha_1\beta_1\hat{f}(t)-(\alpha_0\beta_1+\beta_0\alpha_1)\hat{g}(t)$$

and

$$f(-\alpha_0^2t+\alpha_1^2\hat{f}(t)+\alpha_1\alpha_0\hat{g}(t))=\beta_0^2t-\beta_1^2\hat{f}(t)-\beta_0\beta_1\hat{g}(t).$$

Put $u=-\alpha_0^2t+\alpha_1^2\hat{f}(t)+\alpha_0\alpha_1\hat{g}(t)$ and rewrite the above equations in matrix form as

$$\begin{pmatrix}-\alpha_0^2 & -\alpha_1^2 & \alpha_0\alpha_1 & 0\\ -\beta_0^2 & -\beta_1^2 & \beta_0\beta_1 & 0\\ 2\alpha_0\beta_0 & 2\alpha_1\beta_1 & -(\alpha_0\beta_1+\beta_0\alpha_1) & 0\\ 0 & 0 & 0 & 1\end{pmatrix}\begin{pmatrix}t\\ -\hat{f}(t)\\ \hat{g}(t)\\ 1\end{pmatrix}=\begin{pmatrix}u\\ -f(u)\\ g(u)\\ 1\end{pmatrix}.$$

The matrix is an element of the stabiliser group of the quadratic cone defined by the equation $4X_0X_1=X_2^2$ with vertex $\langle 0,0,0,1\rangle$. Dualising as in the previous section this implies that there is an element of the stabiliser group of the quadratic cone defined by the equation $X_0X_1=X_2^2$ with vertex $\langle 0,0,0,1\rangle$ that maps the set of planes

$$\{tX_0-\hat{f}(t)X_1+\hat{g}(t)X_2+X_3=0\mid t\in GF(q)\}$$

to the planes

$$\{uX_0 - f(u)X_1 + g(u)X_2 + X_3 = 0 \mid u \in GF(q)\}.$$

The converse argument works following the above argument in reverse. Note that the determinant of the matrix is $-(\alpha_0\beta_1 - \alpha_1\beta_0)^3$ and the determinant of map F is $\alpha_0\beta_1 - \alpha_1\beta_0$. Therefore F will be a non-singular map and hence H will be non-singular too.

7 q-clans and translation generalised quadrangles

A *q-clan* is a set $\{A_t \mid t \in GF(q)\}$ of q two by two matrices with entries from $GF(q)$ with the property that the difference of any two distinct matrices is anisotropic, i.e.

$$\alpha(A_t - A_s)\alpha^T = 0$$

$s \neq t$ implies $\alpha = (0,0)$. A q-clan is *additive* if $A_t + A_s = A_{t+s}$.

Consider the set of matrices

$$\left\{ \begin{pmatrix} t & g(t) \\ 0 & -f(t) \end{pmatrix} \mid t \in GF(q) \right\}$$

where f and g are linear over some subfield $GF(q_0)$. Let (v,u) be such that $(v,u)(A_t - A_s)(v,u)^T = 0$, $s \neq t$. It follows that

$$(v,u) \begin{pmatrix} z & g(z) \\ 0 & -f(z) \end{pmatrix} (v,u)^T = 0$$

where $z = t - s$. This implies that $zv^2 + vug(z) - u^2 f(z) = 0$ and $z \neq 0$. If either $u = 0$ or $v = 0$ then $(u,v) = (0,0)$. If $u \neq 0$ then making the substitution $z = v/u$

$$zw^2 + wg(z) - f(z) = 0.$$

If this quadratic has no solutions for $w, z \in GF(q)$ and $z \neq 0$ this set of matrices is a q-clan. However this is the same condition as in Theorem 2 and so to a commutative semifield of rank 2 over its middle nucleus $GF(q)$ there is an associated additive q-clan. The following theorem is from [21]. For the definition of an egg see Section 3.

Theorem 11. *The set $\{A_t \mid t \in GF(q)\}$ of 2×2 matrices over $GF(q)$ is an additive q-clan if and only if the set $\mathcal{E} = \{E_\gamma \mid \gamma \in GF(q)^2 \cup \{\infty\}\}$, with*

$$E_\gamma = \{\langle t, -\gamma A_t \gamma^T, -\gamma(A_t + A_t^T)\rangle \mid t \in GF(q)\},$$

$$E_\infty = \{\langle 0, t, 0, 0\rangle \mid t \in GF(q)\},$$

and tangent spaces $T_\mathcal{E} = \{T_{E_\gamma} \mid \gamma \in GF(q)^2 \cup \{\infty\}\}$,

$$T_{E_\gamma} = \{\langle t, \beta\gamma^T + \gamma A_t^T \gamma^T, \beta\rangle \mid t \in GF(q),\ \beta \in GF(q)^2\},$$

$$T_{E_\infty} = \{\langle 0, t, \beta\rangle \mid t \in GF(q),\ \beta \in GF(q)^2\}$$

is an egg of $PG(4n-1, q_0)$ where $q = q_0^n$.

The construction of a generalized quadrangle $T(\mathcal{E})$ in Section 3 from an egg $\mathcal{E}$ implies that from a commutative semifields of rank 2 over its middle nucleus one can construct a generalized quadrangle of order (q, q^2). This is a special case of a more general construction of generalized quadrangles due to Kantor [17]. If a generalized quadrangle $\mathcal{G}$ has an abelian collineation group that acts regularly on the points not collinear with a base point P while fixing every line incident with P then $\mathcal{G}$ is called a *translation generalized quadrangle*. The following theorem is from [23, (8.7.1)].

Theorem 12. *The incidence structure $T(\mathcal{E})$ is a translation generalized quadrangle of order (q^n, q^m) with base point (∞) and conversely every translation generalized quadrangle is isomorphic to a $T(\mathcal{E})$ for some egg $\mathcal{E}$ of $PG(2n + m - 1, q)$.*

For more details and other results concerning eggs and translation generalized quadrangles refer to [20] or [21].

8 Concluding remarks

It was the intention of this article to show how useful pairs of functions f and g from $GF(q) \to GF(q)$ linear over a subfield with the property that $g^2(x) + 4xf(x)$ is a non-square for all $x \in GF(q)^*$ are. Of course it would be of great interest to have more examples. The recent geometrical construction of the Penttila-Williams ovoid by Cardinali [9] from a Cohen-Ganley Thas-Payne flock and a Dickson Kantor Knuth flock gives hope that there may be a geometrical way to construct new examples.

The fact that the set $\mathcal{W}$ is a subspace of rank n contained in the internal points of a conic is not necessarily required in the hypothesis of Theorem 8. The theorem only requires that $\mathcal{W}$ contains a subplane. One might expect that a much stronger bound should hold in Corollary 1 and Corollary 2 if one could utilise the fact that $\mathcal{W}$ is a much larger subspace for $n \geq 4$.

We have seen that the functions f and g allow us to construct not just a commutative semifield of rank 2 over its middle nucleus but other semifields as well. A geometrical explanation of these semifields (including the commutative semifield of rank 2 over its middle nucleus) will appear in [6].

9 Acknowledgements

We would like to thank Peter Cameron and Greg Stein for helpful discussions and to Dieter Jungnickel for useful remarks.

References

1. Albert, A. A. (1952) On non-associative division algebras. Trans. Amer. Math. Soc. **72**, 296–309.

2. Bader L., Ghinelli D., Penttila T. (2001) On monomial flocks. European J. Combin. **22**, 454–474.
3. Bader, L., Lunardon, G., (1994) On non-hyperelliptic flocks. European J. Combin. **15**, 411–415.
4. Bader, L., Lunardon, G., Pinneri, I. (1999) A new semifield flock. J. Combin. Theory Ser. A **86**, 49–62.
5. Ball, S., Blokhuis, A., Lavrauw, M. On the classification of semifield flocks, preprint.
6. Ball, S., Brown, M. The six semifields associated with a semifield flock, preprint.
7. Bloemen, I., Thas, J. A., van Maldeghem, H. (1998) Translation ovoids and generalised quadrangles and hexagons. Geom. Dedicata **72**, 19–62.
8. Cameron, P. J. *Projective and Polar Spaces*, available from `http://www.maths.qmw.ac.uk/~pjc/pps/`
9. Cardinali, I., Polverino, O., Trombetti, R. On the sporadic semifield flock, preprint.
10. Cohen, S. D., Ganley, M. J. (1982) Commutative semifields two dimensional over their middle nuclei. J. Algebra **75**, 373–385.
11. Dembowski, P. *Finite Geometries*, Springer-Verlag, New York, 1968.
12. Dickson, L. E. (1906) Linear algebra in which division is always uniquely possible. Trans. Amer. Math. Soc. **7**, 370–390, 514–527.
13. Dickson, L. E. (1935) Linear algebras with associativity not assumed. Duke. Math. J. **1**, 113–125.
14. Gevaert, H., Johnson, N. L. (1988) Flocks of quadratic cones, generalized quadrangles and translation planes. Geom. Dedicata **27**, 301–317.
15. Hall Jr., M. *The Theory of Groups*, Macmillan, New York, pp. 346–420, 1959.
16. Hughes, D. R., Piper, F. *Projective Planes*, Springer-Verlag, New York, 1973.
17. Kantor, W. M. (1980) Generalized quadrangles associated with $G_2(q)$. J. Combin. Theory Ser. A **29**, 212–219.
18. Kantor, W. M. (1982) Ovoids and translation planes. Canad. J. Math. **34**, 1195–1207.
19. Knuth, D. E. (1965) Finite semifields and projective planes. J. Algebra **2**, 182–217.
20. Lavrauw, M., *Scattered subspaces with respect to spreads and eggs in finite projective spaces*, Ph. D. thesis, Technical University of Eindhoven, The Netherlands, 2001.
21. Lavrauw, M., Penttila, T. (2001) On eggs and translation generalized quadrangles. J. Combin. Theory Ser. A **96**, 303–315.
22. Lunardon, G. (1997) Flocks, ovoids of $Q(4, q)$ and designs. Geom. Dedicata **66**, 163–173.
23. Payne, S. E., Thas, J. A. *Finite generalized quadrangles*, Research Notes in Mathematics, 110. Pitman, Boston, 1984.
24. Penttila, T., Williams, B. (2000) Ovoids of parabolic spaces. Geom. Dedicata **82**, 1–19.
25. Prince, A. R. (2000) Two new families of commutative semifields. Bull. London Math. Soc. **32**, 547–550.
26. Thas, J. A. (1987) Generalized quadrangles and flocks of cones. European J. Combin. **8**, 441–452.
27. Thas, J. A. (1997) Generalized quadrangles of order (s, s^2). II. J. Combin. Theory Ser. A **79**, 223–254.

28. Thas, J. A., Payne, S. E. (1994) Spreads and ovoids in finite generalized quadrangles. Geom. Dedicata **52**, 227–253.
29. Tits, J. (1962) Ovoides et Groupes de Suzuki. Arch. Math. Vol. XIII, 187–198.