The six semifield planes associated with a semifield flock

Simeon Ball *
Queen Mary, University of London,
London E1 4NS,
United Kingdom

Matthew R. Brown †
University of Ghent
Galglaan 2, 9000 Gent,
Belgium

24 October 2003

Abstract

In 1965 Knuth [17] noticed that a finite semifield was determined by a 3-cube array (a_{ijk}) and that any permutation of the indices would give another semifield. In this article we explain the geometrical significance of these permutations. It is known that a pair of functions (f, g) where f and g are functions from $GF(q)$ to $GF(q)$ with the property that f and g are linear over some subfield and $g(x)^2+4xf(x)$ is a non-square for all $x \in GF(q)^*$, q odd, give rise to certain semifields, one of which is commutative of rank 2 over its middle nucleus, one of which arises from a semifield flock of the quadratic cone, and another that comes from a translation ovoid of $Q(4, q)$. We show that there are in fact six non-isotopic semifields that can be constructed from such a pair of functions, which will give rise to six non-isomorphic semifield planes, unless (f, g) are of linear type or of Dickson-Kantor-Knuth type. These six semifields fall into two sets of three semifields related by Knuth operations.

1. Introduction and Definitions

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 at least one of a or b is zero.

Throughout this article the term semifield will refer to a finite semifield. Some authors refer to a semifield as a division ring. A finite field is a semifield. If the multiplication is associative then the semifield is a finite field.

A system $\mathcal{S}$ is a *finite pre-semifield* if it satisfies all the axioms of a finite semifield except possibly (S3). i.e. it need not have a multiplicative identity. Throughout this article the term pre-semifield will refer to a finite pre-semifield. We can obtain a semifield from a

*This author is supported by British EPSRC Fellowship No. AF/990-480.
†This author acknowledges the support of Ghent University grant GOA 12050300.

pre-semifield $\mathcal{S}$ with multiplication denoted by $\cdot$ by defining a new multiplication $\circ$ by the rule

$$(a \cdot u) \circ (u \cdot b) = a \cdot b.$$

This semifield has an identity element $u \cdot u$.

It is not difficult to show that the additive group of a pre-semifield is an elementary abelian p-group. The *left nucleus* of a pre-semifield $\mathcal{S}$ is defined to be $\mathcal{L} = \{x \mid x(ab) = (xa)b \text{ for all } a, b \in \mathcal{S}\}$. The *middle nucleus* is defined to be $\mathcal{M} = \{x \mid a(xb) = (ax)b \text{ for all } a, b \in \mathcal{S}\}$. The *right nucleus* is defined to be $\mathcal{R} = \{x \mid a(bx) = (ab)x \text{ for all } a, b \in \mathcal{S}\}$. The left, middle and right nuclei are all finite fields containing $GF(p)$ and so $\mathcal{S}$ is said to have *characteristic* p. The pre-semifield $\mathcal{S}$ can be viewed as a left vector space over the left nucleus, a right vector space over the right nucleus or either a left or right vector space over the middle nucleus.

Every semifield determines a projective plane and the projective plane is Desarguesian if and only if the semifield is a field. The plane π constructed from a pre-semifield $\mathcal{S}$ with multiplication $\circ$ has

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

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

$$y_1 x_3 = x_2 \circ y_2 + x_1 y_3.$$

Here, by definition, $1x = x1 = x$ and $0x = x0 = 0$. It is a simple matter to check that any two points of π are incident with a unique line and dually the any two lines of π are incident with a unique point and hence that π is a projective plane. We call π the plane coordinatised by $\mathcal{S}$. We would like to know when two pre-semifields $\mathcal{S}$ and $\mathcal{S}'$ determine the same projective plane. Let $\mathcal{S}$ and $\mathcal{S}'$ be two pre-semifields of characteristic p with multiplication $\cdot$ and $\circ$, respectively. An *isotopism* from $\mathcal{S}$ to $\mathcal{S}'$ is a triple (F, G, H) of non-singular linear transformations from $\mathcal{S}$ to $\mathcal{S}'$ over $GF(p)$ such that

$$F(a) \circ G(b) = H(a \cdot b) \quad \text{for all } a, b, c \in \mathcal{S}.$$

Two pre-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 [1], a proof of which can also be found in [17].

Theorem 1.1 *Two pre-semifields coordinatize the same projective plane if and only if they are isotopic.*

Note that the semifield we constructed from a pre-semifield is isotopic to the pre-semifield and as a consequence of the above will therefore coordinatise the same projective plane.

Let us consider a projective plane π coordinatised by a semifield $\mathcal{S}$ with multiplication $\circ$ and define

$$U_m = \{(x, y) \in \mathcal{S} \times \mathcal{S} \mid y = x \circ m\}.$$

The pair $(x, y) \in U_m$ if and only if the point $(1, x, y)$ is on the line $[1, m, 0]$. Let n be the rank (vector space dimension) of the vector space $\mathcal{S}$ viewed as a left vector space over its left nucleus $\mathcal{L}$. If (x_1, y_1) and $(x_2, y_2) \in U_m$ and λ, $\mu \in \mathcal{L}$ then

$$\lambda y_1 + \mu y_2 = \lambda(x_1 \circ m) + \mu(x_2 \circ m) = (\lambda x_1) \circ m + (\mu x_2) \circ m = (\lambda x_1 + \mu x_2) \circ m$$

and hence U_m is a subspace of the vector space $\mathcal{S} \times \mathcal{S}$. The equation $y = x \circ m$ has a unique solution y for each $x \in \mathcal{S}$ and hence U_m is of rank n. Moreover either $U_m = U_l$ or $U_m \cap U_l = \{(0, 0)\}$. If we put $U_\infty = \{(0, y) \mid y \in \mathcal{S}\}$ then

$$\{U_m \mid m \in \mathcal{S} \cup \{\infty\}\}$$

is a spread Σ of rank n subspaces of the vector space $\mathcal{S} \times \mathcal{S}$ of rank $2n$. This spread has the property that there is a group that acts on the elements of the spread fixing one element point-wise (U_∞) and acting regularly on the others. A spread with this property is called a *semifield spread*. The André construction of a (affine) translation plane from a spread (also referred to as the Bruck-Bose construction) takes as points the vectors of a vector space and as lines the cosets of the elements of a spread. The projective completion of the affine plane constructed via the André construction from the spread Σ is the plane π coordinatised by the semifield $\mathcal{S}$.

The dual plane π^* is the semifield plane that can be coordinatised by the semifield $\mathcal{S}^*$ which is the semifield with multiplication $\cdot$ defined by $a \cdot b = b \circ a$. The corresponding semifield spread Σ^* is given by the elements U_m^* and U_∞ where

$$U_m^* = \{(x, y) \mid y = x \cdot m = m \circ x\}$$

for each $m \in \mathcal{S}$. Let r be the rank of the vector space $\mathcal{S}$ viewed as a right vector space over its right nucleus $\mathcal{R}$. Then Σ^* is a spread of subspaces of rank r of the right vector space $\mathcal{S} \times \mathcal{S}$ of rank $2r$ over the right nucleus $\mathcal{R}$.

We have seen that the dual plane of a semifield plane is also a semifield plane. The following theorem is an important characterization of semifield planes, see [14, Chapter 8].

Theorem 1.2 *A plane is a translation plane and its dual plane is also a translation plane if and only if the plane is coordinatised by a semifield.*

Although the following theorem is well known we have included a short proof since we were unable to find a suitable reference.

Theorem 1.3 *Let π be a translation plane constructed from a spread Σ. The spread Σ is a semifield spread if and only if the plane π is coordinatised by a semifield.*

Proof : Suppose Σ is a semifield spread with a group G fixing the element U of Σ pointwise and acting regularly on $\Sigma \setminus \{U\}$. Let π be the projective plane constructed from Σ with ideal points $[X]$ for each $X \in \Sigma$. The group generated by G and the translations of π fixing $[U]$, fix $[U]$ linewise and act transitively on the lines of π not incident with $[U]$. Hence the dual projective plane is a translation plane with translation line $[U]$ and so π is coordinatised by a semifield.

Now suppose that π is coordinatised by a semifield $\mathcal{S}$ with multiplication $\cdot$. The maps $(x, y) \to (x, y + x \cdot a)$ fix the line $\{(0, y) \mid y \in \mathcal{S}\}$ pointwise and act regularly on the other lines incident with $(0, 0)$. Hence the associated spread is semifield. □

2. Spread sets, dual spreads and the Knuth cubical array

A *spread set* is a set of q^n $(n \times n)$-matrices $\mathcal{C}$ with the property that for all M, $N \in \mathcal{C}$ with $M \neq N$, $\det(M - N) \neq 0$. We can construct a spread of subspaces of rank n in a vector space of rank $2n$ from a spread set (hence the name) in the following way. Let U_M be the subspace spanned by the rows of the matrix

$$(I \mid M)$$

and let U_∞ be the subspace spanned by the rows of the matrix

$$(0 \mid I),$$

where I is the $(n \times n)$ identity matrix. The set of subspaces

$$\{U_M \mid M \in \mathcal{C} \cup \{\infty\}\}$$

is a spread. This can be checked in the following way. One shows that if there is a vector in both U_M and U_N then there exists a linear combination of the rows of $M - N$ which is zero, contradicting the spread set property. Conversely for any spread there is an equivalent spread which can be constructed as above, see [8].

Each column of the $(n \times 2n)$-matrix

$$\left(\frac{-M}{I}\right)$$

considered as a point of the vector space of rank $2n$ over $GF(q)$, dualises, with respect to the standard inner product, to a hyperplane which contains all the elements of U_M since

$$(I \mid M)\left(\frac{-M}{I}\right) = 0.$$

In the dual space the subspace U_M dualises to the subspace $U_M^\dagger$ spanned by the rows of the matrix

$$\left(I \mid -M^T\right)$$

where M^T denotes the transpose of the matrix M. We can construct the spread $\Sigma^\dagger$ which is equivalent to the spread

$$\{U_M^\dagger \mid M \in \mathcal{C} \cup \{\infty\}\}$$

from the spread set $\mathcal{C}^\dagger$ which we define to be

$$\{M^T \mid M \in \mathcal{C}\}.$$

We denote the translation plane constructed via the André construction from the spread $\Sigma^\dagger$ as $\pi^\dagger$.

Let us consider again the spread

$$\Sigma = \{U_m \mid m \in \mathcal{S} \cup \{\infty\}\}$$

constructed from the semifield $\mathcal{S}$ as in the previous section. We write the vector x as $x = \sum_{i=0}^{n-1} x_i \mathbf{e_i}$ and $m = \sum_{j=0}^{n-1} m_j \mathbf{e_j}$ so that

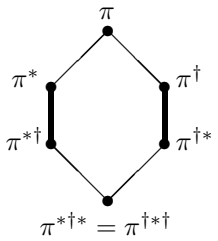
$$y = x \circ m = (\sum_{i=0}^{n-1} x_i \mathbf{e_i}) \circ (\sum_{j=0}^{n-1} m_j \mathbf{e_j}) = \sum_{i,j,k=0}^{n-1} x_i m_j a_{ijk} \mathbf{e_k},$$

where $\mathbf{e_i} \circ \mathbf{e_j} = \sum_{k=0}^{n-1} a_{ijk}\mathbf{e_k}$. If we let M_m be the $(n \times n)$ matrix whose ik-th entry is $\sum_{j=0}^{n-1} m_j a_{ijk}$ then the above equation can be written in matrix form as $y = xM_m$. The vector $(x, y) \in U_m$ satisfies

$$(x, y) = x\,(I \mid M_m)$$

and hence U_m is the subspace spanned by the rows of $(I \mid M_m)$. The set of matrices $\{M_m \mid m \in \mathcal{S}\}$ is a spread set whose corresponding spread gives rise via the André construction to the semifield plane π coordinatised by $\mathcal{S}$. Note that the spread set is closed under addition, which characterises spread sets arising from semifield spreads.

The multiplication $\circ$ of a semifield $\mathcal{S}$ determines and is determined by the multiplication of the basis elements $\mathbf{e_i} \circ \mathbf{e_j} = \sum_{k=0}^{n-1} a_{ijk}\mathbf{e_k}$. The elements (a_{ijk}) form what Knuth [17] describes as a 3-cube, an example of a cubical array. The multiplication $\cdot$ defined by $x \cdot y = y \circ x$ of the semifield S^* is described by the cubical array (a_{jik}). Knuth noticed that any permutation of the subscripts would determine a semifield from which one can of course construct a semifield plane. The matrices M_m^T have ik-th entry $\sum_{j=0}^{n-1} m_i a_{kji}$ and working our way back through the argument in the previous paragraph, these are the matrices of the spread set of the semifield determined by the cubical array (a_{kji}). So the permutation of the indices (13) will give the multiplication of the semifield $S^\dagger$ that coordinatises the plane $\pi^\dagger$, which can be constructed from the spread via the André construction, that is the dual of the spread that we obtain from the semifield $\mathcal{S}$. Now as Knuth noted there are six permutations of the indices giving possibly six non-isotopic semifields. He does not realize the geometric interpretation of the permutations of the indices as he looks at the permutation (23). However now we see that this takes the semifield $\mathcal{S}$ to $\mathcal{S}^{*\dagger*}$ and the plane π to $\pi^{*\dagger*}$.



The six semifield planes associated to π.

3. Rank 2 commutative semifields

A semifield $\mathcal{S}$ with multiplication $\circ$ is *commutative* if $a \circ b = b \circ a$ for all a, $b \in \mathcal{S}$. The translation plane π coordinatised by a commutative semifield is self-dual. Note however that commutativity is not an isotopic invariant and therefore that a semifield plane that is self-dual could be coordinatised by a non-commutative semifield. It is a simple matter to check that the left nucleus $\mathcal{L}$ is equal to the right nucleus $\mathcal{R}$ for a commutative semifield. Indeed $x \in \mathcal{L}$ if and only if for all a, $b \in \mathcal{S}$

$$x \circ (a \circ b) = (x \circ a) \circ b.$$

The commutativity implies that this is if and only if

$$(b \circ a) \circ x = b \circ (a \circ x)$$

and hence if and only if $x \in \mathcal{R}$.

In [7] Cohen and Ganley are concerned with commutative semifields that are of rank 2 over their middle nucleus $GF(q)$. When q is even they show that all such semifields are $GF(q^2)$ and for q odd they prove the following theorem. The proof is short and so we include it here.

Theorem 3.1 *A commutative semifield $\mathcal{S}$ of rank 2 over its middle nucleus $\mathcal{M} = GF(q)$, q odd, can be represented by the set $\{(x, y) \mid x, y \in GF(q)\}$ such that multiplication $\circ$ is determined by two additive functions f and g from $GF(q)$ to $GF(q)$ with the property that*

$$g(x)^2 + 4xf(x)$$

is a non-square in $GF(q)$ for all $x \in GF(q)^*$ and

$$(x, y) \circ (u, v) = (xv + yu + g(ux), yv + f(ux)).$$

Proof : Let $\alpha \in \mathcal{S} \setminus \mathcal{M}$. Then $\{1, \alpha\}$ forms a basis for $\mathcal{S}$ over its middle nucleus.

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

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

$$= ((xu \circ \alpha) \circ \alpha) + (xv + yu) \circ \alpha + yv.$$

Now let f and g by functions from $GF(q)$ to $GF(q)$ such that $(x \circ \alpha) \circ \alpha = g(x) \circ \alpha + f(x)$. The distributive laws, (S2) in the axioms of a semifield, imply that f and g are additive functions, or in other words that $f(x + y) = f(x) + f(y)$ and $g(x + y) = g(x) + g(y)$ for all x, $y \in GF(q)$. And

$$(x \circ \alpha + y) \circ (u \circ \alpha + v) = (xv + yu + g(ux)) \circ \alpha + yv + f(ux).$$

We have only to check axiom (S4) now so we assume that

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

and

$$yv + f(ux) = 0.$$

Then eliminating y and writing $U = ux$ and $V = vx$ we have that

$$V^2 + g(U)V - f(U)U = 0.$$

If U or V is 0 then either (x, y) or (u, v) is $(0, 0)$. Hence (S4) is always satisfied if for every non-zero U this has no solutions which is if and only if $g(x)^2 + 4xf(x)$ is a non-square for all $x \in GF(q)^*$. □

We call a pair of functions (f, g) which are additive and have the property that

$$g(x)^2 + 4xf(x)$$

is a non-square for all $x \in GF(q)^*$ a *Cohen-Ganley pair* (of functions). We say that two Cohen-Ganley pairs of functions (f, g) and $(\hat{f}, \hat{g})$ are equivalent if there corresponding commutative semifields of rank 2 over their middle nuclei are isotopic.

The following are all the known examples of inequivalent Cohen-Ganley pairs of functions. The Cohen-Ganley pairs can be used to construct flocks of the quadratic cone, ovoids of $Q(4, q)$ and, as we have seen, translation planes. It is because of this that the known examples are attributed to various people since their discovery occurred in different settings.

1. The linear example where $f(x) = mx$ and $g(x) = 0$.
2. The Dickson [9], Kantor [15], Knuth [17] example where $f(x) = mx^\sigma$, $g(x) = 0$, m is a non-square in $GF(q)$ and σ is an automorphism of $GF(q)$.
3. The Cohen-Ganley [7], Thas-Payne [26] example where $q = 3^h$, $f(x) = m^{-1}x + mx^9$ and $g(x) = x^3$ with m a non-square in $GF(q)$.
4. The Penttila-Williams [22] example where $q = 3^5$, $f(x) = x^9$ and $g(x) = x^{27}$.

4. Flocks of the quadratic cone

Let $\mathcal{K}$ be a quadratic cone of $PG(3, q)$ with vertex v. A *flock* $\mathcal{F}$ of $\mathcal{K}$ is a partition of $\mathcal{K} \setminus \{v\}$ into q conics. Two flocks $\mathcal{F}$ and $\mathcal{F}'$ are equivalent if there exists an element of the stabilizer group of $\mathcal{K}$ that is a bijection between the planes of $\mathcal{F}$ and the planes of $\mathcal{F}'$.

The quadratic cones of $PG(3, q)$ are equivalent under an element of $\mathrm{PGL}(4, q)$. Therefore we let v be the point $\langle 0, 0, 0, 1\rangle$ and let the conic $\mathcal{C}$, defined by the equation $X_0X_1 = X_2^2$ in the plane π with equation $X_3 = 0$, be the base of the cone $\mathcal{K}$. The planes determined by the conics can be written as

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

where $t \in GF(q)$ and f, g are functions from $GF(q)$ to $GF(q)$ and this flock is denoted $\mathcal{F}(f, g)$.

The line that is incident with both the planes π_t and π_s is

$$\langle (f(t) - f(s), t - s, 0, tf(s) - sf(t)), (g(t) - g(s), 0, -(t - s), tg(s) - sg(t))\rangle.$$

A point on this line

$$\langle \lambda(f(t) - f(s)) + \nu(g(t) - g(s)), \lambda(t - s), -\nu(t - s), \lambda(tf(s) - sf(t)) + \nu(tg(s) - sg(t))\rangle$$

is skew from $\mathcal{K}$ and therefore for λ and $\nu \in GF(q)$ not both zero the equation

$$0 = (t - s)\nu^2 - (g(t) - g(s))\lambda\nu - (f(t) - f(s))\lambda^2$$

has no solutions for $s \neq t$. Hence for q odd, the pair of functions (f, g) will give a flock if and only if

$$(g(t) - g(s))^2 + 4(t - s)(f(t) - f(s))$$

is a non-square in $GF(q)$ for all distinct t and $s \in GF(q)$. Note that if f and g are additive functions then the pair of functions (f, g) will give a flock if and only if they are a Cohen-Ganley pair.

The following construction of a spread of $PG(3,q)$ from a flock of the quadratic cone is due to Thas and Walker [27].

Let $Q^+(5,q)$ denote the hyperbolic quadric. A canonical form for such a quadric is

$$Q^+ := X_0X_1 + X_2X_3 + X_4X_5.$$

The quadratic cone $\mathcal{K}$ is embedded in Q^+, it is the intersection of the hyperplanes $X_4 = 0$ and $X_2 + X_3 = 0$ and Q^+. The associated bilinear form to Q^+ is

$$b(X,Y) := X_0Y_1 + Y_0X_1 + X_2Y_3 + Y_2X_3 + X_4Y_5 + Y_4X_5.$$

Let $\pi_t^\perp$ denote the plane that is dual to the plane π_t dualising with respect to the bilinear form b. Then

$$\pi_t^\perp = \langle(-f(t), t, 0, g(t), 1, 0), (0,0,0,0,0,1), (0,0,1,1,0,0)\rangle$$

$$= \{\langle -f(t), t, u, u+g(t), 1, s\rangle \mid s,u \in GF(q)\} \cup \{\langle 0,0,u,u,0,s\rangle \mid s,u \in GF(q)\}.$$

The plane π_t meets the quadric Q^+ in a conic and hence likewise the plane $\pi_t^\perp$ meets the quadric Q^+ in a conic. The points of this intersection $Q^+ \cap \pi_t^\perp$ are

$$\{\langle -f(t), t, u, u+g(t), 1, tf(t) - u^2 - ug(t)\rangle \mid u \in GF(q)\} \cup \{\langle 0,0,0,0,0,1\rangle\}.$$

For any point $x \in Q^+ \cap \pi_t^\perp$ and $y \in Q^+ \cap \pi_s^\perp$ with $x \neq y$,

$$b(x,y) = -sf(t) - tf(s) + uw + ug(s) + uw + wg(t) + sf(s) - w^2 - wg(s) + tf(t) - u^2 - ug(t)$$

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

is non-zero by the flock condition. We could also argue that x and y are not orthogonal in Q^+ geometrically. The plane π_t and π_s are incident with a line l that is skew from Q^+. The space $l^\perp$ meets the quadric Q^+ in an elliptic quadric, no two of whose points are orthogonal, and contains $\pi_t^\perp$ and $\pi_s^\perp$. Hence the set

$$\bigcup_{t \in GF(q)} Q^+ \cap \pi_t^\perp$$

$$= \{\langle -f(t), t, u, u+g(t), 1, tf(t) - u^2 - ug(t)\rangle \mid t,u \in GF(q)\} \cup \{\langle 0,0,0,0,0,1\rangle\}$$

is an ovoid of Q^+. The Klein correspondence takes an ovoid of $Q^+(5,q)$ to a spread of $PG(3,q)$ and vice-versa and in this case one can check using Plücker coordinates that the lines of the corresponding spread $\Sigma(f,g)$ are

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

Indeed the point $\langle -f(t), t, u, u+g(t), 1, tf(t) - u^2 - ug(t)\rangle$ on $X_0X_1 + X_2X_3 + X_4X_5 = 0$ is the point $\langle p_{12}, p_{03}, p_{31}, p_{02}, p_{01}, p_{23}\rangle$ where p_{ij} are the Plücker coordinates of the line. Let π be the plane constructed from this spread via the André construction. This spread $\Sigma(f,g)$ is that constructed from the spread set

$$\mathcal{C}(f,g) := \left\{ \begin{pmatrix} f(t) & u \\ u+g(t) & t \end{pmatrix} \mid u,t \in GF(q) \right\}.$$

Theorem 4.1 *The spread* $\Sigma(f,g)$ *of* $PG(3,q)$

$$\{\langle (f(t),u+g(t),0,1),(u,t,1,0)\rangle \mid t,u\in GF(q)\}\cup\{\langle (1,0,0,0),(0,1,0,0)\rangle\},$$

is self-dual.

Proof : Under the Klein correspondence a duality of $PG(3,q)$ is equivalent to a collineation of $PG(5,q)$ that fixes $Q^+(5,q)$ and interchanges the two classes of generators of $Q^+(5,q)$ (see [12, Chapter 15]). Using this we will work in $Q^+(5,q)$. Following the Thas/Walker construction above we embed the quadratic cone $\mathcal{K}$ in $Q^+(5,q)$ and if $\mathcal{F}=\{\pi_t \ : t\in GF(q)\}$, then the ovoid $\mathcal{O}(\mathcal{F})$ is $\bigcup_{t\in GF(q)} Q^+(5,q)\cap \pi_t^\perp$. Now any collineation fixing $Q^+(5,q)$ and $\mathcal{K}$ pointwise must also fix $\mathcal{O}(\mathcal{F})$, so we look for such a collineation that also interchanges the two classes of generators of $Q^+(5,q)$. The polar image of $\langle\mathcal{K}\rangle$ is a line of $PG(5,q)$ tangent to $Q^+(5,q)$ at the point v which is the vertex of $\mathcal{K}$. Let u be any other point on this line. The collineation μ_u (see [13, Chapter 22]) that acts by $x\mapsto x-(b(x,u)/Q^+(u))u$ is an involution that fixes $Q^+(5,q)$ and u. Further, if p is a point of $Q^+(5,q)$, then μ_u fixes p if up is a tangent to $Q^+(5,q)$ and interchanges p with p' if pu meets $Q^+(5,q)$ again in p'. Any generator π of $Q^+(5,q)$ meets $u^\perp$ in a line which is fixed by μ_u which implies that π and $\mu_u(\pi)$ intersect in this line. Consequently, π and $\mu_u(\pi)$ belong to different classes, and μ_u is of the required form. □

Lemma 4.2 *Let* $\mathcal{O}$ *be an ovoid of* $Q^+(5,q)$ *arising from a flock by the Thas/Walker construction, that is, there is a line* ℓ *tangent to* $\mathcal{O}$ *at a point* v *such that* $\mathcal{O}$ *is the union of* q *conics each of whose planes contains* ℓ*. If there is a second such tangent* $\ell'\neq\ell$ *to* $\mathcal{O}$*, then* $\mathcal{O}$ *is an elliptic quadric.*

Proof : First suppose that the line ℓ' also contains the point v. Consider a conic $\mathcal{C}$ contained in $\mathcal{O}$, containing v and with tangent ℓ' at v. Taking the span of ℓ with the points of $\mathcal{C}\setminus\{v\}$ in turn yields the q conic sections of $\mathcal{O}$ with tangent ℓ at v. Further, these are all contained in the space spanned by the plane of $\mathcal{C}$ and ℓ. Hence $\mathcal{O}$ must be an elliptic quadric.

Next suppose that ℓ' is tangent to $\mathcal{O}$ at a point $u\neq v$ and that ℓ and ℓ' intersect in a point w. The plane $\langle u,v,w\rangle$ meets $\mathcal{O}$ in a conic $\mathcal{C}$, and let $\mathcal{C}'$ be a second conic contained in $\mathcal{O}$ with tangent ℓ at v. For each point of $x\in\mathcal{C}'\setminus\{v\}$ the plane $\langle\ell',x\rangle$ meets $\mathcal{O}$ in a conic. Thus in the three dimensional subspace Π generated by $\mathcal{C}$ and $\mathcal{C}'$ there are at least $q^2/2+q+1$ points of $\mathcal{O}$ and at least $q^2/2$ points of $\mathcal{O}\setminus\mathcal{C}$. Since this is more than half the points of $\mathcal{O}\setminus\mathcal{C}$ it follows that no other three space containing $\mathcal{C}$ may contain a point of $\mathcal{O}\setminus\mathcal{C}$. Hence $\mathcal{O}$ is contained in Π and is an elliptic quadric.

Finally suppose that ℓ' is tangent to $\mathcal{O}$ at a point $u\neq v$ and that ℓ and ℓ' are skew. Let $\mathcal{C}$ be any conic section of $\mathcal{O}$ containing u and with tangent ℓ' at u. The span of ℓ with any point of $\mathcal{C}$ must meet $\mathcal{O}$ in a conic section with tangent ℓ at v. Since there are only q such sections it follows that at least one of these planes contains two points of $\mathcal{C}$. Thus the plane of $\mathcal{C}$ must contain a point of ℓ and so $\mathcal{C}$ is contained in $\langle\ell,\ell'\rangle$. It follows that $\mathcal{O}$ is contained in $\langle\ell,\ell'\rangle$ and is hence an elliptic quadric. □

Note that Gevaert, Johnson and Thas ([11]) have a stronger version of this result requiring that $\mathcal{O}$ has only one additional conic to those whose planes contain ℓ.

Theorem 4.3 *Let $\mathcal{F}$ and $\mathcal{G}$ be flocks of a quadratic cone in $PG(3,q)$, then the following are equivalent:*

1. *The flocks $\mathcal{F}$ and $\mathcal{G}$ are equivalent.*
2. *The spreads $\Sigma(\mathcal{F})$ and $\Sigma(\mathcal{G})$ are isomorphic.*
3. *The planes $\pi(\mathcal{F})$ and $\pi(\mathcal{G})$ that are constructed from $\Sigma(\mathcal{F})$ and $\Sigma(\mathcal{G})$ via the André construction are isomorphic.*

Proof : These equivalences come from [10, Theorem 7.3], but we shall also provide our own proof. The equivalence of 2. and 3. is found in [2], so we will now prove the equivalence of 1. and 2.

Following the Thas/Walker construction let $\Sigma(\mathcal{F})$ be constructed from the flock $\mathcal{F}$ of the cone $\mathcal{K}_{\mathcal{F}}$ embedded in Q^+ with $\langle \mathcal{K}_{\mathcal{F}} \rangle^{\perp} = \ell_{\mathcal{F}}$, and similarly for $\Sigma(\mathcal{G})$ replacing $\mathcal{F}$ with $\mathcal{G}$.

Firstly suppose that the spreads $\Sigma(\mathcal{F})$ and $\Sigma(\mathcal{G})$ are equivalent. We shall consider the classical and non-classical cases separately. If they are both regular spreads, then they correspond to elliptic quadric ovoids $\mathcal{E}(\mathcal{F})$ and $\mathcal{E}(\mathcal{G})$ of Q^+ and there is an automorphism of Q^+ mapping $\mathcal{E}(\mathcal{F})$ to $\mathcal{E}(\mathcal{G})$. Further, since the group of an elliptic quadric ovoid of Q^+ is induced by the group of Q^+ we may also assume that $\ell_{\mathcal{F}}$ is mapped onto $\ell_{\mathcal{G}}$. From this it follows that the same automorphism must map $\mathcal{K}_{\mathcal{F}}$ onto $\mathcal{K}_{\mathcal{G}}$ and $\mathcal{F}$ onto $\mathcal{G}$. Now suppose that $\Sigma(\mathcal{F})$ and $\Sigma(\mathcal{G})$ are not classical. The corresponding ovoids $\mathcal{O}(\mathcal{F})$ and $\mathcal{O}(\mathcal{G})$ of Q^+ are the union of q conics about $\ell_{\mathcal{F}}$ and $\ell_{\mathcal{G}}$, respectively. Since the spreads are equivalent it follows that there is an automorphism of Q^+ that maps $\mathcal{O}(\mathcal{F})$ onto $\mathcal{O}(\mathcal{G})$. Further, by applying Lemma 4.2 this automorphism must also map $\ell_{\mathcal{F}}$ onto $\ell_{\mathcal{G}}$ and $\mathcal{F}$ onto $\mathcal{G}$.

Next suppose that $\mathcal{F}$ and $\mathcal{G}$ are equivalent flocks. Since the group of Q^+ is transitive on quadratic cones we may assume that $\mathcal{F}$ and $\mathcal{G}$ are embedded as flocks of the same quadratic cone of Q^+. Since the group of Q^+ induces the full group of the quadratic cone it follows that there is an automorphism of Q^+ mapping $\mathcal{F}$ to $\mathcal{G}$. We may also assume that this automorphism fixes the generator classes of Q^+. (Since in the proof of Theorem 4.1 we saw an automorphism of Q^+ fixing the subspace of a quadratic cone pointwise and swapping the generator classes of Q^+.) Under the Klein correspondence this automorphism of Q^+ becomes a collineation of $PG(3,q)$ mapping $\Sigma(\mathcal{F})$ to $\Sigma(\mathcal{G})$. □

The following theorem on flocks is due to Thas [24].

Theorem 4.4 *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.*

If the functions f and g are additive functions then the spread $\Sigma(f,g)$ is a semifield spread. For this reason we call the flock $\mathcal{F}(f,g)$ where the functions f and g are additive a *semifield flock*. The maximal subfield with the property that f and g are linear over the subfield is called the kernel of the (semifield) flock.

Let $\mathcal{F}(f,g)$ be a semifield flock. The functions f and g are a Cohen-Ganley pair and can be used to construct a commutative semifield of rank 2 over its nucleus following Section 3.

In Section 2. we saw that for a semifield spread the matrices in the corresponding spread set determine the multiplication in the semifield. The matrices of the spread set $\mathcal{C}(f,g)$ determine the multiplication $\circ$ in the pre-semifield $\mathcal{S}$ that coordinatises the plane $\pi(f,g)$ constructed via the André construction from the spread $\Sigma(f,g)$. Indeed

$$(x,y)\circ(u,t) = (x,y)\begin{pmatrix} f(t) & u \\ u+g(t) & t \end{pmatrix} = (uy + xf(t) + yg(t), ux + ty).$$

5. Ovoids of $Q(4,q)$

The generalised quadrangle $Q(4,q)$ is the structure of totally isotropic points and lines of a non-degenerate quadric over $PG(4,q)$. Let Q be the non-degenerate quadratic form defined by

$$Q(X) := X_0X_4 + X_1X_3 - X_2^2.$$

An ovoid of $Q(4,q)$ is equivalent to an ovoid containing $\langle 0,0,0,0,1\rangle$ and for any such ovoid $\mathcal{O}(F)$ there is a function F such that

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

Thas [25] and later Lunardon [20] show that it is possible to construct an ovoid of $Q(4,q)$ from a semifield flock and vice-versa. Lunardon also proves that two such ovoids are equivalent if and only if the corresponding semifields are equivalent. Lavrauw [18] (see also [3]) explicitly calculates the polynomial $F(x,y)$ from the flock $\mathcal{F}(f,g)$. Let $GF(q_0)$ be the kernel of the semifield flock, that is the largest subfield of $GF(q)$ over which f and g are linear. Then f and g can be written as

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

for some c_i, $b_i \in GF(q)$. The semifield flock $\mathcal{F}(f,g)$ is in one-to-one correspondence with the ovoid $\mathcal{O}(F)$ of $Q(4,q)$ given by $F(x,y) = \hat{f}(y) + \hat{g}(x)$ where

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

This ovoid $\mathcal{O}(F)$ has the property that there is a distinguished point, namely $\langle 0,0,0,0,1\rangle$, such that for each line ℓ of $Q(4,q)$ incident with $\langle 0,0,0,0,1\rangle$ there is an automorphism group of $Q(4,q)$ fixing $\mathcal{O}(F)$, fixing $\langle 0,0,0,0,1\rangle$ linewise, fixing ℓ pointwise, and for each $P \in \ell \setminus \{\langle 0,0,0,0,1\rangle\}$ acts transitively on the set of points of $\mathcal{O}(F)\setminus\{\langle 0,0,0,0,1\rangle\}$ collinear with P. An ovoid with this property is called a *translation ovoid with respect to the point* P, or sometimes just a *translation ovoid*, see [6]. Using the Klein correspondence the points of an ovoid of $Q(4,q)$ corresponds to a spread $\hat{\Sigma}(F)$ of the symplectic generalised quadrangle $W(q)$ and vice-versa.

Theorem 5.1 *([20], [5]) An ovoid $\mathcal{O}(F)$ of $Q(4,q)$ is a translation ovoid with respect to a point if and only if the corresponding spread $\hat{\Sigma}(F)$ of $W(q)$ is a semifield spread.*

Proof : If $\mathcal{O}(F)$ is a translation ovoid with respect to the point P, then by [6] there is a group G of collineations of $PG(4,q)$ fixing $Q(4,q)$, the point P, the lines of $Q(4,q)$ on P, and acting regularly on $\mathcal{O}(F) \setminus \{P\}$. Embedding $Q(4,q)$ in the Klein quadric $Q^+(5,q)$ as a hyperplane intersection we can extend G to a group of $PG(5,q)$ fixing $Q^+(5,q)$ and the generators (the totally isotropic planes) of $Q^+(5,q)$ on P. Under the Klein correspondence this is equivalent to a spread $\hat{\Sigma}(F)$ stabilised by a group fixing one element pointwise and acting regularly on the remaining lines, that is, a semifield spread. □

The previous theorem implies that from a translation ovoid of $Q(4,q)$ we obtain a semifield. One may expect that this semifield will be that constructed directly from the corresponding semifield flock, however we shall see that in general this is not the case. Firstly we calculate the multiplication for the semifield $\hat{\mathcal{S}}$ that coordinatises the plane $\hat{\pi}(F)$, where $\hat{\pi}(F)$ is the plane constructed from the symplectic spread $\hat{\Sigma}(F)$ via the André construction. One can check that the spread $\hat{\Sigma}(F)$

$$\{\langle(1,0,F(x,y),x),(0,1,x,y)\rangle \mid x,y \in GF(q)\} \cup \{\langle(1,0,0,0),(0,1,0,0)\rangle\}$$

corresponds via the Klein correspondence to the ovoid $\mathcal{O}(F)$. Indeed the point

$$\langle 1, y, x, F(x,y), x^2 - yF\rangle$$

is the point on $X_0X_4 + X_1X_3 - X_2^2 = 0$ is $\langle p_{01}, p_{03}, p_{02}, p_{21}, p_{32}\rangle$ in the Plücker coordinates of the line

$$\langle(1,0,F(x,y),x),(0,1,x,y)\rangle.$$

This is the spread constructed from the spread set

$$\left\{ \begin{pmatrix} F(x,y) & x \\ x & y \end{pmatrix} \mid x,y \in GF(q) \right\}.$$

As before we conclude that the plane $\hat{\pi}$ is coordinatised by the pre-semifield $\hat{\mathcal{S}}$ with multiplication $\circ$

$$(x,y) \circ (u,v) = (x,y) \begin{pmatrix} F(u,v) & u \\ u & v \end{pmatrix} = (xF(u,v) + uy, xu + yv),$$

$$(x,y) \circ (u,v) = (x\hat{f}(v) + x\hat{g}(u) + uy, xu + yv).$$

Theorem 5.2 *The following are equivalent:*

1. *The translation ovoids $\mathcal{O}(F)$ and $\mathcal{O}(G)$ are equivalent.*
2. *The spreads $\hat{\Sigma}(F)$ and $\hat{\Sigma}(G)$ are equivalent.*
3. *The planes $\hat{\pi}(F)$ and $\hat{\pi}(G)$ that are constructed from $\hat{\Sigma}(F)$ and $\hat{\Sigma}(G)$ via the André construction are isomorphic.*

Proof : By the Klein correspondence 1. and 2. are equivalent, while 2. and 3. are equivalent comes from [2]. □

We conclude this section with the following theorem which is a straightforward consequence of Theorem 4.4. However it is important to note that this shows in general for a Cohen-Ganley pair of functions (f,g) that the semifield $\hat{\mathcal{S}}$ constructed from the translation ovoid of $Q(4,q)$ is not isotopic to the semifield $\mathcal{S}$ constructed from the semifield flock.

Theorem 5.3 *Let (f,g) be a Cohen-Ganley pair of functions. The pre-semifield $\mathcal{S}$ constructed from the semifield flock $\mathcal{F}(f,g)$ with multiplication $\circ$ given by*

$$(x,y)\circ(u,v)=(uy+xf(v)+yg(v),xu+yv)$$

and the pre-semifield $\hat{\mathcal{S}}$ constructed from the translation ovoid $\mathcal{O}$ with multiplication $\cdot$ given by

$$(x,y)\cdot(u,v)=(x\hat{f}(v)+x\hat{g}(u)+uy,xu+yv)$$

are isotopic if and only if the pair of functions (f,g) are linear or Dickson-Kantor-Knuth.

Proof : The two pre-semifields $\mathcal{S}$ and $\hat{\mathcal{S}}$ are isotopic if and only if the semifield planes they coordinatise are isomorphic. By [2] this is the case if and only if the spreads of $PG(3,q)$ giving rise to the planes are equivalent, that is, if and only if the spread arising from the flock $\mathcal{F}$ is symplectic. Via the Thas/Walker construction this is equivalent to the planes of $\mathcal{F}$ having a common point. By Theorem 4.4 this is the case if and only if $\mathcal{F}$ is linear or Dickson-Kantor-Knuth which is if and only if the pair of functions (f,g) are linear or Dickson-Kantor-Knuth.

6. The six semifields associated with a semifield flock

Throughout the remainder of the article (f,g) will be a Cohen-Ganley pair of functions and $\mathcal{F}(f,g)$ will be the semifield flock. Let $GF(q_0)$ be the kernel of the semifield flock, the maximal subfield such that f and g can be written as

$$f(x)=\sum_{i=0}^{n-1}c_ix^{q_0^i}\ \text{ and }\ g(x)=\sum_{i=0}^{n-1}b_ix^{q_0^i}$$

for some c_i, $b_i\in GF(q)$. Let $\hat{f}$ and $\hat{g}$ be the polynomials defined from f and g as in the previous section and let $\mathcal{O}(\hat{f},\hat{g})$ be the translation ovoid $\mathcal{O}(F)$ where $F(x,y)=\hat{f}(y)+\hat{g}(x)$. Let $\mathcal{S}$ be the pre-semifield constructed from the semifield flock $\mathcal{F}(f,g)$ and let $\hat{\mathcal{S}}$ be the pre-semifield constructed from the translation ovoid $\mathcal{O}(\hat{f},\hat{g})$. We shall calculate the pre-semifields associated to $\mathcal{S}$ and $\hat{\mathcal{S}}$ via the Knuth cubical array method described in Section 2..

In Section 4. we saw that the pre-semifield $\mathcal{S}$ has multiplication $\circ$ where

$$(x,y)\circ(u,v)=(uy+xf(v)+yg(v),xu+yv)$$

and that the plane π coordinatised by $\mathcal{S}$ is a translation plane whose spread $\Sigma(f,g)$ can be constructed from the spread set

$$\left\{\begin{pmatrix} f(v) & u+g(v)\\ u & v\end{pmatrix}\mid u,v\in GF(q)\right\}.$$

In Section 1. we saw that the plane π^*, the dual plane of π, is the plane coordinatised by $\mathcal{S}^*$, the semifield whose multiplication is

$$(x,y)\circ(u,v)=(xv+uf(y)+vg(y),xu+yv).$$

In Theorem 4.1 we saw that the spread Σ is self-dual and therefore that the plane $\pi^\dagger$ constructed from the spread dual to Σ via the André construction is isomorphic to π. The

plane $\pi^\dagger$ is coordinatised by a semifield $\mathcal{S}^\dagger$ isotopic to $\mathcal{S}$, we write $\mathcal{S} \simeq \mathcal{S}^\dagger$. It follows immediately that the plane $\pi^{\dagger *}$, the plane dual to $\pi^\dagger$, is isomorphic to the plane π^* and hence that the semifield $\mathcal{S}^{\dagger *} \simeq \mathcal{S}^*$.

Theorem 6.1 *Let Σ^* be the spread from which the translation plane π^* is constructed via the André construction. Let $\Sigma^{*\dagger}$ be the spread dual to the spread Σ^*. Let the semifield $\mathcal{S}^{*\dagger}$ be a semifield which coordinatises the plane $\pi^{*\dagger}$ obtained from the spread $\Sigma^{*\dagger}$ via the André construction. Then the semifield $\mathcal{S}^{*\dagger}$ is isotopic to a pre-semifield with multiplication given by*

$$(x, y) \circ (u, v) = (xv + yu, yv + \hat{f}(xu) + \hat{g}(xv)).$$

Proof : This proof was significantly shortened using the ideas that appear in [16].

For all $u, v \in GF(q)$

$$\{(x, y, xv + uf(y) + vg(y), xu + yv) \mid x, y \in GF(q)\}$$

is an element of the spread Σ^*. Following Section 2. we dualise with respect to the inner-product

$$((x, y, z, w), (a, b, c, d)) = \mathrm{Tr}(xa + yb + zc + wd),$$

where $\mathrm{Tr}(x) = x + x^{q_0} + x^{q_0^2} + \ldots + x^{q/q_0}$ is the trace function from $GF(q)$ to $GF(q_0)$. So we want to find (a, b, c, d) such that

$$\mathrm{Tr}(xa + yb + c(xv + uf(y) + vg(y)) + d(xu + yv)) = 0,$$

for all $x, y \in GF(q)$. If we put $x = 0$ then

$$\mathrm{Tr}(y(b + \hat{f}(uc) + \hat{g}(vc) + dv)) = 0$$

and hence $b = -(\hat{f}(uc) + \hat{g}(vc) + dv)$. If we put $y = 0$ then

$$\mathrm{Tr}(x(a + cv + du)) = 0$$

and hence $a = -(cv + du)$. The corresponding spread element of $\Sigma^{*\dagger}$ is therefore

$$\{(-(cv + du), -(\hat{f}(uc) + \hat{g}(vc) + dv), c, d) \mid c, d \in GF(q)\}.$$

By a straightforward change of coordinates the multiplication for $\mathcal{S}^{*\dagger}$ is as claimed. □

In Section we saw that the pre-semifield $\hat{\mathcal{S}}$ constructed from the ovoid $\mathcal{O}(\hat{f}, \hat{g})$ of $Q(4, q)$ has multiplication $\circ$ where

$$(x, y) \circ (u, v) = (x\hat{f}(v) + x\hat{g}(u) + uy, xu + yv).$$

and that the plane $\hat{\pi}$ coordinatised by $\hat{\mathcal{S}}$ is a translation plane whose spread $\hat{\Sigma}$ can be constructed from the spread set

$$\left\{ \begin{pmatrix} \hat{f}(v) + \hat{g}(u) & u \\ u & v \end{pmatrix} \mid u, v \in GF(q) \right\}.$$

The matrices in this spread set are symmetric and so the spread constructed from the spread set will be self dual. Hence the planes π and $\pi^\dagger$ are isomorphic and the semifields that coordinatise these planes $\hat{\mathcal{S}}$ and $\hat{\mathcal{S}}^\dagger$ are isotopic, $\hat{\mathcal{S}} \simeq \hat{\mathcal{S}}^\dagger$. The multiplication in the semifield $\hat{\mathcal{S}}^*$ is given by

$$(x, y) \circ (u, v) = (u\hat{f}(y) + u\hat{g}(x) + xv, xu + yv)$$

and it follows immediately that $\hat{\mathcal{S}}^* \simeq \hat{\mathcal{S}}^{\dagger *}$.

Theorem 6.2 *Let $\hat{\Sigma}^*$ be the spread from which the translation plane $\hat{\pi}^*$ is constructed via the André construction. Let $\hat{\Sigma}^{*\dagger}$ be the spread dual to the spread $\hat{\Sigma}^*$. Let the semifield $\hat{\mathcal{S}}^{*\dagger}$ be a semifield which coordinatises the plane $\hat{\pi}^{*\dagger}$ obtained from the spread $\hat{\Sigma}^{*\dagger}$ via the André construction. Then the semifield $\hat{\mathcal{S}}^{*\dagger}$ is isotopic to a pre-semifield with multiplication given by*

$$(x, y) \cdot (u, v) = (xv + yu + g(ux), yv + f(ux)).$$

Proof : The proof of this theorem is similar to that of Theorem 6.1.

For all $u, v \in GF(q)$

$$\{(x, y, u\hat{f}(y) + u\hat{g}(x) + xv, xu + yv) \mid x, y \in GF(q)\}$$

is an element of the spread $\hat{\Sigma}^*$. Again we dualise with respect to the inner-product

$$((x, y, z, w), (a, b, c, d)) = \mathrm{Tr}(xa + yb + zc + wd).$$

So we want to find (a, b, c, d) such that

$$\mathrm{Tr}(xa + yb + c(u\hat{f}(y) + u\hat{g}(x) + xv) + d(xu + yv)) = 0,$$

for all $x, y \in GF(q)$. If we put $x = 0$ then

$$\mathrm{Tr}(y(b + f(uc) + dv)) = 0$$

and hence $b = -(f(uc) + dv)$. If we put $y = 0$ then

$$\mathrm{Tr}(x(a + g(uc) + cv + du)) = 0$$

and hence $a = -(g(uc) + cv + du)$. The corresponding spread element of $\hat{\Sigma}^{*\dagger}$ is therefore

$$\{(-(g(uc) + cv + du), -(f(uc) + dv), c, d) \mid c, d \in GF(q)\}.$$

By a straightforward change of coordinates the multiplication for $\hat{\mathcal{S}}^{*\dagger}$ is as claimed.

□

Note that the semifield $\hat{\mathcal{S}}^{*\dagger}$ is the commutative semifield of rank 2 over its middle nucleus that we saw in Section 3.

In this section we have constructed potentially six non-isotopic semifields from a Cohen-Ganley pair of functions (f, g). The following table we list the left, right and middle nuclei of these six semifields. We have determined the multiplication of a pre-semifield isotopic to each these six semifields. However to determine the nuclei one must first calculate the multiplication in the semifield itself using the method described in Section 1. In the table we list the multiplication in a pre-semifield isotopic to the relevant semifield. This table does not apply to the linear example in which all nuclei are $\mathcal{S}$ itself since associativity holds. In this case all the six semifields are $GF(q^2)$.

Semifield	$(x,y)\circ(u,v)$	$\mathcal{L}$	$\mathcal{M}$	$\mathcal{R}$
$\mathcal{S}$	$(yu+xf(v)+yg(v), xu+yv)$	$GF(q)$	$GF(q_0)$	$GF(q_0)$
$\mathcal{S}^*$	$(xv+uf(y)+vg(y), xu+yv)$	$GF(q_0)$	$GF(q_0)$	$GF(q)$
$\mathcal{S}^{*\dagger}$	$(xv+\hat{f}(yu)+\hat{g}(yv), xu+yv)$	$GF(q_0)$	$GF(q)$	$GF(q_0)$
$\hat{\mathcal{S}}$	$(yu+x\hat{f}(v)+x\hat{g}(u), xu+yv)$	$GF(q)$	$GF(q_0)$	$GF(q_0)$
$\hat{\mathcal{S}}^*$	$(xv+u\hat{f}(y)+u\hat{g}(x), xu+yv)$	$GF(q_0)$	$GF(q_0)$	$GF(q)$
$\hat{\mathcal{S}}^{*\dagger}$	$(xv+yu+g(xu), yv+f(ux))$	$GF(q_0)$	$GF(q)$	$GF(q_0)$

The nuclei of the six semifields associated with a semifield flock

Theorem 6.3 *The six semifields $\mathcal{S}$, $\mathcal{S}^*$, $\mathcal{S}^{*\dagger}$, $\hat{\mathcal{S}}$, $\hat{\mathcal{S}}^*$, $\hat{\mathcal{S}}^{*\dagger}$ are pairwise non-isotopic unless (f,g), is of Dickson-Kantor-Knuth type in which case $\mathcal{S}\simeq\hat{\mathcal{S}}$, $\mathcal{S}^*\simeq\hat{\mathcal{S}}^*$, $\mathcal{S}^{*\dagger}\simeq\hat{\mathcal{S}}^{*\dagger}$ are three pairwise non-isotopic, or linear in which case they are all isotopic to $GF(q^2)$.*

Proof : As mentioned before in the case of the linear example all the six semifields are $GF(q^2)$ so we consider only the so-called proper semifields. If two planes π and π' coordinatised by semifields $\mathcal{S}$ and $\mathcal{S}'$ respectively are isomorphic then the ranks of $\mathcal{S}$ and $\mathcal{S}'$ over their left/right nucleus are equal. Hence it is only possible that $\mathcal{S}\simeq\hat{\mathcal{S}}$, $\mathcal{S}^*\simeq\hat{\mathcal{S}}^*$ and $\mathcal{S}^{*\dagger}=\hat{\mathcal{S}}^{*\dagger}$. By Theorem 5.3 $\mathcal{S}\simeq\hat{\mathcal{S}}$ if and only if $\mathcal{S}$ is a linear or Dickson-Kantor-Knuth example and hence in these cases we also have that $\mathcal{S}^*\simeq\mathcal{S}^*$ and $\mathcal{S}^{*\dagger}\simeq\hat{\mathcal{S}}^{*\dagger}$. In the Dickson-Kantor-Knuth examples $GF(q_0)\neq GF(q)$ and so by the preceding argument $\mathcal{S}\not\simeq\mathcal{S}^*$, $\mathcal{S}\not\simeq\mathcal{S}^{*\dagger}$ and $\mathcal{S}^*\not\simeq\mathcal{S}^{*\dagger}$. □

7. Literature

The literature concerning this subject is somewhat confusing. As proved in [3] the so-called sporadic examples of Cohen-Ganley pairs of functions in [7] and the examples in [23] are equivalent to Dickson-Kantor-Knuth examples. The fact that the commutative semifield of rank 2 over its middle nucleus in these examples is isotopic to a Dickson-Kantor-Knuth example now follows from Theorem 4.4, Theorem 6.1, Theorem 5.2 and Theorem 6.3.

Finally for q odd the only non-existence theorem concerning Cohen-Ganley pairs of functions is the following result which is a consequence of the main theorem in [4].

Theorem 7.1 *Let (f,g) be a Cohen-Ganley pair of functions in $GF(q)[X]$, q odd, and suppose that $GF(q_0)$, $q=q_0^n$, is the largest subfield of $GF(q)$ such that both f and g are linear over $GF(q_0)$. If (f,g) is not linear over $GF(q)$ and not of Dickson-Kantor-Knuth type then $q_0<4n^2-8n+2$.*

References

[1] A. A. Albert, Finite division algebras and finite planes, *Proc. Sympos. Appl. Math.*, Vol. 10, 53–70, American Mathematical Society, Providence, R.I.

[2] J. André, Über nicht-Desarguessche Ebenen mit transitiver Translationgruppe, *Math. Z.*, **60**, (1954), 156–186.

[3] S. Ball and M. Lavrauw, Commutative semifields of rank 2 over their middle nucleus, in: *Finite fields with Applications to Coding Theory, Cryptography and Related Areas*, G. L. Mullen. (ed) *et al*, Springer-Verlag, 2002, pp. 1–21.

[4] S. Ball, A. Blokhuis and M. Lavrauw, On the classification of semifield flocks, *Adv. Math.*, to appear.

[5] I. Bloemen, *Substructures and characterizations of finite generalized polygons*, Ph.D. thesis, University of Ghent, 1995.

[6] I. Bloemen, J. A. Thas and H. Van Maldeghem, Translation ovoids of generalized quadrangles and hexagons, *Geom. Dedicata*, **72**, (1998), 19–62.

[7] S. D. Cohen and M. J. Ganley, Commutative semifields, two dimensional over their middle nuclei, *J. Algebra*, **75**, (1982), 373–385.

[8] P. Dembowski, *Finite Geometries*, Springer, Berlin, 1968.

[9] L. E. Dickson, Linear algebra in which division is always uniquely possible, *Trans. Amer. Math. Soc*, **7**, (1906), 514–527.

[10] H. Gevaert and N. L. Johnson, Flocks of quadratic cones, generalized quadrangles and translation planes, *Geom. Dedicata*, **27**, (1988), 301–317.

[11] H. Gevaert, N. L. Johnson and J. A. Thas, Spreads covered by reguli, *Simon Stevin*, **62**, (1988), no. 1, 51–62.

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

[13] J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries*, Clarendon Press, Oxford, 1991.

[14] D. R. Hughes and F. C. Piper, *Projective Planes*, Springer, 1973.

[15] W. M. Kantor, Ovoids and translation planes, *Canad. J. Math.*, **34**, (1982), 1195–1207.

[16] W. M. Kantor, Commutative semifields and symplectic spreads, preprint.

[17] D. E. Knuth, Finite semifields and projective planes, *J. Algebra*, **2**, (1965), 182–217.

[18] M. Lavrauw, *Scattered subspaces with respect to spreads and eggs in finite projective spaces*, Ph. D. thesis, Technical University of Eindhoven, The Netherlands, 2001.

[19] R. Lidl and H. Niederreiter, *Finite Fields*, Second Edition, Cambridge, 1997.

[20] G. Lunardon, Flocks, ovoids of $Q(4, q)$ and designs, *Geom. Dedicata*, **66**, (1997), 163–173.

[21] S. E. Payne and J. A. Thas, *Finite Generalized Quadrangles*, Research Notes in Mathematics, 110, Pitman, Boston, 1984.

[22] T. Penttila and B. Williams, Ovoids of parabolic spaces, *Geom. Dedicata*, **82**, (2000), 1–19.

[23] A. R. Prince, Two new families of commutative semifields, *Bull. London Math. Soc.*, **32**, (2000), 547–550.

[24] J. A. Thas, Generalized quadrangles and flocks of cones, *European J. Combin.*, **8**, (1987), 441–452.

[25] J. A. Thas, Generalized quadrangles of order (s, s^2). II. *J. Combin. Theory Ser. A*, **79**, (1997), 223–254.

[26] J. A. Thas and S. E. Payne, Spreads and ovoids in finite generalized quadrangles, *Geom. Dedicata*, **52**, (1994), 227–253.

[27] M. Walker, A class of translation planes, *Geom. Dedicata*, **5**, (1976), 135–146.