A GEOMETRIC CONSTRUCTION OF FINITE SEMIFIELDS

SIMEON BALL, GARY EBERT, AND MICHEL LAVRAUW

Abstract. We give a geometric construction of a finite semifield from a certain configuration of two subspaces with respect to a Desarguesian spread in a finite dimensional vector space over a finite field, and prove that any finite semifield can be obtained in this way. In 1965 Knuth [13] showed that each finite semifield generates in total six (not necessarily non-isotopic) semifields. In certain cases, the geometric construction obtained here allows one to construct another six (not necessarily non-isotopic) semifields, which may or may not be isotopic to the six semifields obtained by Knuth's operations. Explicit formulas are calculated for the multiplications of the twelve isotopy classes of semifields associated with a semifield that is of rank two over its left nucleus.

1. Introduction

A *finite semifield* $\mathbb{S}$ is an algebra satisfying the axioms for a skew field except possibly associativity of multiplication. To be precise, $\mathbb{S}$ is an algebra with at least two elements, and two binary operations $+$ and $\circ$, satisfying the following axioms.

(S1) $(\mathbb{S}, +)$ is a group with identity element 0.
(S2) $x \circ (y + z) = x \circ y + x \circ z$ and $(x + y) \circ z = x \circ z + y \circ z$, for all $x, y, z \in \mathbb{S}$.
(S3) $x \circ y = 0$ implies $x = 0$ or $y = 0$.
(S4) $\exists 1 \in \mathbb{S}$ such that $1 \circ x = x \circ 1 = x$, for all $x \in \mathbb{S}$.

The study of semifields started about a century ago (see [9]) when they were called *non-associative division rings* or *distributive quasifields*. Following Knuth [13] and the recent literature we will use the name semifield, which will always be used to denote a finite semifield. Semifields can be used to construct certain translation planes (called *semifield planes*) and two semifield planes are isomorphic if and only if the corresponding semifields are *isotopic*, see [1]. Associated with a translation plane there is a spread by the so-called André-Bruck-Bose construction. The spread corresponding to a semifield plane is called a *semifield spread*. Two semifields are isotopic if and only if the corresponding semifield spreads are *equivalent*.

In the next section we give a geometric construction of a semifield spread (and hence a semifield) starting from a particular configuration of subspaces of a finite vector space. In Section 3 we construct some known examples in this way and in Section 4 we show that all semifields can be constructed from such a configuration. In Section 5 we consider the effect of a new operation which applies to a certain class of semifields on a sub-class of these semifields, those of rank two over their left nucleus.

Date: 20 October 2006.

The first author acknowledges the support of the Ministerio de Ciencia y Tecnologia, España.

During this research the third author was supported by a VENI grant, part of the Innovational Research Incentives Scheme of the Netherlands Organisation for Scientific Research (NWO).

For more on spreads, translation planes and isotopy, see [1], [7], and [10].

2. A geometric construction of finite semifields

If V is a vector space of rank d over a finite field with q elements, a *spread* of V is a set $\mathcal{S}$ of subspaces of V, all of the same rank d', $1 \leq d' \leq d$, such that every non-zero vector of V is contained in exactly one of the elements of $\mathcal{S}$. It follows that d' divides d and that $|\mathcal{S}| = (q^d - 1)/(q^{d'} - 1)$ (see [7]). In the case that d is even and $d' = d/2$ we call a spread of V a *semifield spread* if there exists an element S of this spread and a group G of semilinear automorphisms of V with the property that G fixes S pointwise and acts transitively on the other elements of the spread.

Let $\mathbb{F}$ be the finite field of q^n elements, let $\mathbb{F}_0$ be the subfield of q elements and assume $n \geq 2$. Let $V_1 \oplus V_r$ be a vector space of rank $r+1$ over $\mathbb{F}$, where V_i is a subspace of rank i over $\mathbb{F}$ and $r \geq 2$. Consider $V_1 \oplus V_r$ as a vector space of rank $(r+1)n$ over $\mathbb{F}_0$ and let $\mathcal{D}(V_1 \oplus V_r)$ be the spread of subspaces of rank n over $\mathbb{F}_0$ arising from the spread of subspaces of rank 1 over $\mathbb{F}$. Such a spread (i.e. arising from a spread of subspaces of rank 1 over some extension field) is called a *Desarguesian spread*. A Desarguesian spread has the property that it induces a spread in every subspace spanned by elements of the spread.

Throughout this paper (unless stated otherwise) $\mathcal{D} = \mathcal{D}(V_1 \oplus V_r)$ will denote the Desarguesian spread where the (unique) spread element containing the vector $(x_0, x_1, \ldots, x_r) \in (V_1 \oplus V_r) \setminus \{0\}$, is the $\mathbb{F}_0$-subspace $\{(ax_0, ax_1, \ldots, ax_r) \mid a \in \mathbb{F}\}$ of rank n. Note that it follows from our definitions of $V_1, V_r, V_1 \oplus V_r$, and $\mathcal{D}$, that $\mathcal{D}$ induces a Desarguesian spread in V_r and that V_1 is an element of $\mathcal{D}$.

Remark 2.1. *The incidence structure constructed from a spread of t-spaces of a vector space of rank rt, generalising the André-Bruck-Bose construction of a translation plane, is a $2-(q^{rt}, q^t, 1)$-design with parallelism. This design is isomorphic to the incidence structure of points and lines of $AG(r, q^t)$ (the r-dimensional Desarguesian affine geometry over the finite field with q^t elements) if and only if the spread is a Desarguesian spread, see* [4]. *In the literature such spreads are sometimes called normal or geometric. The above motivates our choice to use the word Desarguesian.*

For any subset T of $V_1 \oplus V_r$ define

$$B(T) = \{S \in \mathcal{D}(V_1 \oplus V_r) \mid T \cap S \neq \{0\}\}.$$

Let U and W be $\mathbb{F}_0$-subspaces of V_r of rank n and rank $(r-1)n$, respectively, with the property that

$$B(U) \cap B(W) = \emptyset.$$

Let $0 \neq v \in V_1$. Let $\mathcal{S}(U, W)$ be the set of subspaces in the quotient space $(V_1 \oplus V_r)/W$ defined by

$$\mathcal{S}(U, W) := \{\langle S, W\rangle/W \mid S \in B(\langle v, U\rangle)\},$$

where the angle brackets $\langle, \rangle$ denote the span.

Theorem 2.2. *$\mathcal{S}(U, W)$ is a semifield spread of $(V_1 \oplus V_r)/W$.*

Proof. First we show that $\mathcal{S}(U,W)$ is a spread of $(V_1 \oplus V_r)/W$. The vector space $(V_1 \oplus V_r)/W$ has rank $2n$ and the elements of $\mathcal{S}(U,W)$ are subspaces of rank n. So if we show that any two elements of $\mathcal{S}(U,W)$ have a trivial intersection, we only then need to count that we have q^n+1 elements.

Note that $V_r/W \in \mathcal{S}(U,W)$ since $\langle S,W\rangle = V_r$ for all $S \in B(U)$. Moreover V_r/W has trivial intersection with every other element of $\mathcal{S}(U,W)$ since the elements of the Desarguesian spread are either contained in V_r or have trivial intersection with V_r.

Suppose that $\langle R,W\rangle/W$ and $\langle S,W\rangle/W$ are distinct elements of $\mathcal{S}(U,W)\setminus\{V_r/W\}$ which have a non-trivial intersection. Then the subspace $\langle R,S,W\rangle$ has rank at most $(r+1)n-1$ and, since R and S are subspaces belonging to a spread, the subspace they span has rank $2n$ and therefore a non-trivial intersection with W. Now $W \subset V_r$ and so $\langle R,S\rangle \cap W \subset V_r$. Since R and S are subspaces belonging to the Desarguesian spread, $\langle R,S\rangle$ intersects V_r in an element T of the Desarguesian spread. Thus $T \in B(W)$. The intersections of R and S with $\langle U,v\rangle$ are distinct and non-trivial and so $\langle R,S\rangle \cap \langle U,v\rangle$ has rank at least two. Therefore $\langle R,S\rangle$ has a non-trivial intersection with U. However $U \subset V_r$ and $\langle R,S\rangle$ intersects V_r in T. Thus $T \in B(U)\cap B(W)$ which, by hypothesis, does not occur.

It suffices to show that $B(\langle v,U\rangle)\setminus B(U)$ has q^n elements. If an element S of $B(\langle v,U\rangle)\setminus B(U)$ intersects $\langle v,U\rangle$ in a subspace of rank ≥ 2 then S intersects U and therefore belongs to $B(U)$, which it does not. Hence every element of $B(\langle v,U\rangle)\setminus B(U)$ intersects $\langle v,U\rangle$ in a subspace of rank 1. There are q^n subspaces of rank 1 in $\langle v,U\rangle$ that are not contained in U.

Moreover $\mathcal{S}(U,W)$ is a semifield spread because the pointwise stabiliser of V_r is transitive on the elements of $B(\langle v,U\rangle)\setminus B(U)$. □

Let $\mathbb{S}(U,W)$ denote the semifield corresponding to the semifield spread $\mathcal{S}(U,W)$.

Remark 2.3. *The notation $\mathbb{S}(U,W)$ and $\mathcal{S}(U,W)$ suggests that the semifield and the spread only depend on U and W and not on any other choices we made in the construction. This requires some explanation. Clearly, since up to equivalence there is only one Desarguesian spread of rank n subspaces of $V_1 \oplus V_r$ with the desired property that it induces a spread in V_1 and in V_r, the construction is independent of $\mathcal{D}$. We will show that different choices of v give equivalent spreads and hence isotopic semifields, and therefore $\mathbb{S}(U,W)$ and $\mathcal{S}(U,W)$ are independent of v.*

Suppose we have two semifield spreads $\mathcal{S}$ and $\mathcal{S}'$ constructed from (U,W) using v and v' respectively. If we can find an element ϕ of $\Gamma\mathrm{L}(rn+n,q)$ fixing U, W and the Desarguesian spread, with $v^\phi = v'$, then by considering its action on the quotient geometry $(V_1\oplus V_r)/W$, ϕ induces an element $\overline{\phi}$ of $\Gamma\mathrm{L}(2n,q)$ with $\mathcal{S}^{\overline{\phi}} = \mathcal{S}'$. Therefore we want that ϕ is induced by an element of $\Gamma\mathrm{L}(r+1,q^n)$ since then it fixes the Desarguesian spread. If $B(v) \neq B(v')$ then apply a collineation of $\mathrm{PG}(V_1 \oplus V_r)$, with axis $\mathrm{PG}(V_r)$ induced by an element of $\mathrm{PGL}(r+1,q^n)$, which maps $B(v)$ to $B(v')$. If $B(v)=B(v')$ then $v' = av$ for some $a \in \mathbb{F}$. Without loss of generality we may assume that $v=(1,0,\dots,0)$. Then for ϕ choose the element of $\Gamma\mathrm{L}(r+1,q^n)$ defined by

$$\phi(x_1,x_2,\dots,x_{r+1}) = (ax_1,x_2,\dots,x_{r+1}).$$

THEOREM 2.4. *Let $\mathbb{S}(U,W)$ and $\mathbb{S}(U',W')$ be two semifields constructed from subspaces U,U',W,W' of V_r. If there exists an element φ of $\Gamma\mathrm{L}(V_r)$ fixing $\mathcal{D}(V_r)$, and such $U^\varphi = U'$, and $W^\varphi = W'$, then $\mathbb{S}(U,W)$ and $\mathbb{S}(U',W')$ are isotopic semifields.*

Proof. This is elementary in view of the previous remark. □

3. EXAMPLES

Let us illustrate the construction of $\mathcal{S}(U,W)$ in Theorem 2.2 by determining subspaces U and W which give some known pre-semifields.

A pre-semifield satisfies all the axioms of a semifield except that it may not contain a multiplicative identity. However, there is always a semifield isotopic to a pre-semifield, see [13], so for our purposes it suffices to consider pre-semifields.

3.1. **Generalised twisted fields (Albert** [2]**).** $(r=2)$

Let q be an odd prime power. The generalised twisted field (a pre-semifield) $(\mathbb{F},+,\circ)$ has multiplication defined by

$$y \circ x = yx - \eta y^\sigma x^\alpha,$$

where σ and α are automorphisms of $\mathbb{F}$ with fixed field $\mathbb{F}_0$ and $\eta \in \mathbb{F} \setminus \{a^{q-1} \mid a \in \mathbb{F}\}$.

Let $\mathcal{D}(V_1 \oplus V_2)$ be the usual Desarguesian spread of rank n subspaces of $V_1 \oplus V_2$. Define subspaces $U = \{(0, x, -\eta^{1/\sigma} x^{\alpha/\sigma}) \mid x \in \mathbb{F}\}$ and $W = \{(0, -z^\sigma, z) \mid z \in \mathbb{F}\}$ of $V_2 \cong \mathbb{F}_0^{2n}$. Clearly

$$B(U) = \{\{(0, ax, -a\eta^{1/\sigma} x^{\alpha/\sigma}) \mid a \in \mathbb{F}\} \mid x \in \mathbb{F}^*\}$$

and

$$B(W) = \{\{(0, -by^\sigma, by) \mid b \in \mathbb{F}\} \mid y \in \mathbb{F}^*\}$$

and they are disjoint since η is not a $(q-1)$-th power.

Let $v = (1,0,0)$. An element of $B(\langle U, v\rangle) \setminus B(U)$ is of the form

$$S_x = \{(y, yx, -y\eta^{1/\sigma} x^{\alpha/\sigma}) \mid y \in \mathbb{F}\}.$$

We can obtain S_x/W by intersecting $\langle S_x, W\rangle$ with a subspace of rank $2n$ which has no non-trivial intersection with W, for example $X_3 = 0$. Now

$$\langle S_x, W\rangle = \{(y, yx - z^\sigma, -y\eta^{1/\sigma} x^{\alpha/\sigma} + z) \mid y, z \in \mathbb{F}\}$$

and so

$$\mathcal{S}(U,W) = \{\{(y, yx - \eta y^\sigma x^\alpha)\} \mid y \in \mathbb{F}\} \mid x \in \mathbb{F}\} \cup \{(0,y) \mid y \in \mathbb{F}\}.$$

The plane of order $|\mathbb{F}|$ defined by this spread is the semifield plane coordinatised by the generalised twisted field.

3.2. **The Kantor-Williams symplectic semifields** [12]**.** $(r = 3)$
Let q be even and $\mathbb{F}$ be an extension of $\mathbb{F}_0$ of odd degree n. Let $f(x) = \sum_{i=0}^{n-1} b_i x^{q^i}$ be an additive function from $\mathbb{F}$ to $\mathbb{F}$ such that

$$xy + y^2 f(x)^2 + f(y)^2 x^2 = 0$$

has no non-trivial solutions. Let $\hat{f}(x) = \sum_{i=0}^{n-1} (b_i x)^{q^{-i}}$, $b_i \in \mathbb{F}$.

The Kantor-Williams symplectic pre-semifields $(\mathbb{F}, +, \circ)$ have multiplication

$$y \circ x = \hat{f}(yx) + y^2 x + y f(x),$$

for some f satisfying the above condition.

Let $\mathcal{D}(V_1 \oplus V_3)$ be the usual Desarguesian spread of rank n subspaces of $V_1 \oplus V_3$. Define subspaces $U = \{(0, f(x), x^{1/2}, x) \mid x \in \mathbb{F}\}$ and $W = \{(0, \hat{f}(z) + w^2, w, z) \mid z, w \in \mathbb{F}\}$ of $V_3 = {\mathbb{F}_0}^{3n}$, of rank n and rank $2n$ respectively. Now if

$$B(U) = \{\{(0, yf(x), yx^{1/2}, yx) \mid y \in \mathbb{F}\} \mid x \in \mathbb{F}^*\}$$

and

$$B(W) = \{\{(0, a\hat{f}(z) + aw^2, aw, az) \mid a \in \mathbb{F}\} \mid (z, w) \in \mathbb{F}^2 \setminus \{(0, 0)\}\}$$

have an non-empty intersection then there is an $a \in \mathbb{F}^*$, and $w, z, x, y \in \mathbb{F}$ satisfying the set of equations $az = yx$, $aw = yx^{1/2}$, and $a\hat{f}(z) + aw^2 = yf(x)$. But then $(ya^{-1}) \circ x = \hat{f}(ya^{-1}x) + (ya^{-1})^2 x + ya^{-1} f(x) = 0$, which implies $x = 0$ or $y = 0$. Thus $B(U)$ and $B(W)$ are disjoint.

Let $v = (1, 0, 0, 0)$. An element of $B(\langle U, v \rangle) \setminus B(U)$ is of the form

$$S_x = \{(y, yf(x), yx^{1/2}, yx) \mid y \in \mathbb{F}\}.$$

We obtain S_x/W by intersecting $\langle S_x, W \rangle$ with a subspace of rank $2n$ which has no non-trivial intersection with W, for example $X_3 = X_4 = 0$. Now $\langle S_x, W \rangle = \{(y, yf(x) + \hat{f}(z) + w^2, yx^{1/2} + w, yx + z) \mid y, z, w \in \mathbb{F}\}$ and so

$$S_x/W = \{(y, yf(x) + \hat{f}(yx) + y^2 x) \mid y \in \mathbb{F}\}.$$

The plane defined by the semifield spread $\mathcal{S}(U, W)$ is a semifield plane coordinatised by a Kantor-Williams symplectic semifield.

3.3. **The Coulter-Matthews commutative semifields** [6]**.** $(r = 3)$
Let $\mathbb{F}$ be an odd degree extension of the field with three elements. The Coulter-Matthews commutative pre-semifield $(\mathbb{F}, +, \circ)$ is defined by

$$y \circ x = x^9 y + xy^9 - (xy)^3 + xy.$$

Define subspaces $U = \{(0, x, x^9, x^{1/9}) \mid x \in \mathbb{F}\}$ and $W = \{(0, z, z^3 - w^9 - z, w) \mid z, w \in \mathbb{F}\}$ of $V_3 = {\mathbb{F}_0}^{3n}$, of rank n and rank $2n$ respectively. If $B(U)$ and $B(W)$ have a non-empty intersection then there is a $y \in \mathbb{F}$ with the property that $z = xy$, $z^3 - w^9 - z = x^9 y$ and $w = x^{1/9} y$ hold simultaneously, which implies $(xy)^3 - xy^9 - xy = x^9 y$. This cannot occur non-trivially since $\circ$ defines a pre-semifield.

Let $v = (1, 0, 0, 0)$. An element of $B(\langle U, v \rangle) \setminus B(U)$ is of the form

$$S_x = \{(y, yx, yx^9, yx^{1/9}) \mid y \in \mathbb{F}\}.$$

We obtain S_x/W by intersecting $\langle S_x, W\rangle$ with a subspace of rank $2n$ which has no non-trivial intersection with W, for example $X_2 = X_4 = 0$. Now $\langle S_x, W\rangle = \{(y, yx + z, yx^9 + z^3 - w^9 - z, yx^{1/9} + w) \mid y, z, w \in \mathbb{F}\}$ and so

$$S_x/W = \{(y, x^9y + xy^9 - (xy)^3 + xy) \mid y \in \mathbb{F}\}.$$

Note that the signs are mixed-up in the multiplication of the Coulter-Matthews semifield as listed in [11]; they should be as above.

4. The construction covers all finite semifields

In the previous section we saw examples of semifields that can be constructed using Theorem 2.2. In this section we shall prove that any semifield can be constructed in this way. Firstly, note that a finite semifield $\mathbb{S}$ has a characteristic p, for some prime p, and that $\mathbb{S}$ is a vector space over the field of p elements.

Let $\mathbb{S} = (\mathbb{F}, +, \circ)$ be a finite semifield of order p^n. Define

$$S_x := \{(y, y \circ x) \mid y \in \mathbb{F}\},$$

for every $x \in \mathbb{F}$ and

$$S_\infty := \{(0, y) \mid y \in \mathbb{F}\}.$$

Then $\{S_x \mid x \in \mathbb{F}\} \cup \{S_\infty\}$ is a spread of the vector space $V(\mathbb{F} \times \mathbb{F})$ of rank $2n$ over $\mathbb{F}_0$ consisting of subspaces of rank n over $\mathbb{F}_0$, where $\mathbb{F}_0$ is the subfield of $\mathbb{F}$ of order p. For some $c_{ij} \in \mathbb{F}$ we can write

$$y \circ x = \sum_{i,j=0}^{n-1} c_{ij} x^{p^i} y^{p^j} = \sum_{j=0}^{n-1} c_j(x) y^{p^j}.$$

This spread is a semifield spread with respect to S_∞ (see [7]).

Theorem 4.1. *For every finite semifield $\mathbb{S}$, there exist subspaces U and W of $\mathbb{F}_0^{n^2}$ such that $\mathbb{S}$ is isotopic to $\mathbb{S}(U, W)$.*

Proof. Consider $V_1 \oplus V_n$ as a vector space of rank $n + 1$ over $\mathbb{F}$. The spread element of the Desarguesian spread $\mathcal{D}(V_1 \oplus V_n)$ containing $x \in \mathbb{F}^{n+1}$ is the rank n subspace over $\mathbb{F}_0$

$$\{(yx_0, yx_1, \ldots, yx_n) \mid y \in \mathbb{F}\}.$$

Define subspaces of V_n by

$$U = \{(0, c_0(x), c_1(x)^{p^{-1}}, \ldots, c_{n-1}(x)^{p^{-n+1}}) \mid x \in \mathbb{F}\}$$

and

$$W = \{(0, -\sum_{i=1}^{n-1} z_i^{p^i}, z_1, z_2, \ldots, z_{n-1}) \mid z_i \in \mathbb{F}\}.$$

If $B(U) \cap B(W) \neq \emptyset$ then there is an element of the Desarguesian spread meeting both U and W and so there is a

$$z = (0, -\sum_{i=1}^{n-1} z_i^{p^i}, z_1, z_2, \ldots, z_{n-1}) \in W$$

and a $y \in \mathbb{F}^*$ with the property that $y^{-1}z \in U$. Hence there exists an $x \in \mathbb{F}^*$ such that

$$z_i = yc_i(x)^{p^{-i}},\ i \neq 0$$

and

$$-\sum_{i=1}^{n-1} z_i^{p^i} = yc_0(x).$$

Substituting for the z_i in the second equality we get

$$y \circ x = \sum_{j=0}^{n-1} c_j(x)y^{p^j} = 0$$

which implies $x = 0$ or $y = 0$, a contradiction. Thus $B(U) \cap B(W) = \emptyset$.

Let $v = (1, 0, \ldots, 0)$. The element of the Desarguesian spread $\mathcal{D}(V_1 \oplus V_n)$ containing the vector

$$(1, c_0(x), c_1(x)^{p^{-1}}, \ldots, c_{n-1}(x)^{p^{-n+1}})\ \in \langle U, v\rangle$$

is

$$R_x := \{(y, yc_0(x), yc_1(x)^{p^{-1}}, \ldots, yc_{n-1}(x)^{p^{-n+1}}) \mid y \in \mathbb{F}\}.$$

The quotient space $(V_1 \oplus V_n)/W$ is isomorphic to the projection of all subspaces containing W onto a subspace of rank $2n$ intersecting W trivially. In order to calculate the quotient subspace $\langle R_x, W\rangle/W$ we first form the span

$$\langle R_x, W\rangle = \{(y, yc_0(x) - \sum_{i=1}^{n-1} z_i^{p^i}, yc_1(x)^{p^{-1}} + z_1, \ldots, yc_{n-1}(x)^{p^{-n+1}} + z_{n-1}) \mid y, z_i \in \mathbb{F}\},$$

and then intersect this with the subspace defined by $X_2 = X_3 = \ldots = X_n = 0$. Hence

$$\langle R_x, W\rangle/W = \{(y, \sum_{j=0}^{n-1} c_j(x)y^{p^j}) \mid y \in \mathbb{F}\} = \{(y, y \circ x) \mid y \in \mathbb{F}\}.$$

Thus the semifield spread $S(U, W)$ is isomorphic to the semifield spread associated with $\mathbb{S}$. □

Remark 4.2. *The theorem shows that any semifield of size $|\mathbb{F}|$ can be constructed for $r = n$, that is from subspaces of rank n and $n^2 - n$ of $\mathbb{F}_0^{n^2}$, where $n = [\mathbb{F} : \mathbb{F}_0]$. In the previous section we saw that we could construct certain semifields from subspaces of $\mathbb{F}_0^{rn}$, where $r = 2$ and 3.*

Remark 4.3. *In a random search for a semifield of order q^n there are q^{n^3} variables, since there are q^n choices for each c_{ij}, whereas in the construction there are only q^{rn^2} choices, q^{n^2} choices to find a basis for U and $q^{(r-1)n^2}$ to find a basis for W. Thus choosing r to be small would considerably reduce the search space.*

Remark 4.4. *Theorem 2.2 gives us a construction of a finite semifield from a configurations of two subspaces and a Desarguesian spread, Theorem 2.4 states that two equivalent configurations give isotopic semifields, and by Theorem 4.1 every finite semifield can be constructed using Theorem 2.2.*

A logical next step would be to prove that two isotopic semifields arise from equivalent configurations, i.e., a converse of Theorem 2.4. It is tempting to conjecture that if two *semifields* $\mathbb{S}(U,W)$ *and* $\mathbb{S}(U',W)$ *are isotopic, then there exists an element* $\varphi \in \Gamma L(V_r)$*, such that* φ *fixes the Desarguesian spread and* W *and* $U^\varphi = U'$ *or, if two semifields* $\mathbb{S}(U,W)$ *and* $\mathbb{S}(U,W')$ *are isotopic, then there exists an element* $\varphi \in \Gamma L(V_r)$*, such that* φ *fixes the Desarguesian spread and* U *and* $W^\varphi = W'$*.*

However, these conjectures would turn out to be false due to the following counterexamples, which were found using the computer package MAGMA [14]*.*

In $\mathbb{F}_3^9$ *one can construct a Desarguesian spread and find subspaces* U*,* U' *of rank* 3 *and* W *of rank* 6 *with the property that* U *meets* 13 *spread elements and* U' *only* 10*. Implementing the construction it turns out that neither* $\mathbb{S}(U,W)$ *nor* $\mathbb{S}(U',W)$ *are isotopic to* $\mathbb{F}_{27}$*. Since, up to isotopism, there is only one semifield (the generalised twisted field) with* 27 *elements which is not a field (*[8]*), they are isotopic. Therefore the fact that two semifields* $\mathbb{S}(U,W)$ *and* $\mathbb{S}(U',W)$ *are isotopic does not imply the existence of an element of* $\Gamma\mathrm{L}(V_r)$ *which fixes the Desarguesian spread and* W *and maps* U *to* U'*.*

In the same space one can find subspaces U *of rank* 3*, and* W *and* W' *of rank* 6 *with the property that* W *meets* 271 *spread elements and* W' *meets* 352*. Implementing the construction it turns out that both* $\mathbb{S}(U,W)$ *and* $\mathbb{S}(U,W')$ *are isotopic to* $\mathbb{F}_{27}$*.*

5. Semifield operations

In [13] Knuth noted the group S_3 acts on the set of finite semifields. The group S_3 is generated by involutions τ_1 and τ_2.

The operation τ_1 changes the order of multiplication and is equivalent to dualising the semifield plane.

The operation τ_2 has the effect of dualising the semifield spread associated with the semifield; this geometrical interpretation was first observed in [3] and elaborated in [11]. Knuth [13] proved that τ_2 is well-defined up to isotopism.

We denote by $[\mathbb{S}]$ the set of semifields isotopic to the semifield $\mathbb{S}$, and by $\tau_i([\mathbb{S}])$ we mean $[\tau_i(\mathbb{S})]$.

Two semifields $\mathbb{S} = (\mathbb{F}, +, \circ)$ and $\mathbb{S}' = (\mathbb{F}, +, \cdot)$ of characteristic p are isotopic, for which we write $\mathbb{S} \simeq \mathbb{S}'$, if and only if there exists a triple (f_1, f_2, f_3) of non-singular maps from $\mathbb{F}$ to $\mathbb{F}$, linear over the field with p elements, with the property that

$$f_1(x) \cdot f_2(y) = f_3(x \circ y),$$

for all $x, y \in \mathbb{F}$. Albert [1] proved that two semifields are isotopic if and only if their corresponding planes are isomorphic.

The identity map will be denoted as id.

If a semifield $\mathbb{S}(U,W)$ can be constructed from subspaces of rank n of $\mathbb{F}_0^{2n}$ then we can switch the roles of U and W to construct the semifield $\mathbb{S}(W,U)$. It is not clear whether this operation is well-defined up to isotopism, in other words, whether if $\mathbb{S}(U,W)$ and $\mathbb{S}(U',W')$ are isotopic implies that $\mathbb{S}(W,U)$ and $\mathbb{S}(W',U')$ are isotopic.

In the following section we shall look at the effect of this operation on the class of semifields that are of rank 2 over their left nucleus.

6. The semifields associated with semifields of rank two over their left nucleus

The left nucleus of a semifield $\mathbb{S} = (\mathbb{F}, +, \circ)$ is

$$\{x \in \mathbb{F} \mid x \circ (y \circ z) = (x \circ y) \circ z \text{ for all } y, z \in \mathbb{F}\},$$

the middle and right nucleus are defined analogously. The left nucleus is a field and $\mathbb{S}$ can be viewed as a vector space over the left nucleus. Suppose that the rank of this vector space is two. Then there is a field $\mathbb{K}$ with the property that $\mathbb{S} = (\mathbb{K}^2, +, \circ)$ and $\{(u, 0) \mid u \in \mathbb{K}\}$ is the left nucleus. Therefore

$$(u, 0) \circ (x, y) = (ux, uy),$$

for all $u, x, y \in \mathbb{K}$ and

$$(0, v) \circ (x, y) = ((v, 0) \circ (0, 1)) \circ (x, y) = (v, 0) \circ ((0, 1) \circ (x, y)) = (v, 0) \circ (h(x, y), g(x, y))$$

for some functions h and g from $\mathbb{K}^2$ to $\mathbb{K}^2$, linear over some subfield of $\mathbb{K}$. Thus

$$(0, v) \circ (x, y) = (vh(x, y), vg(x, y))$$

and the distributive laws imply

$$(u, v) \circ (x, y) = (ux + vh(x, y), uy + vg(x, y)).$$

Let us show that $\mathbb{S}$ can be constructed as $\mathbb{S}(U, W)$ where U and W are subspaces of $\mathbb{F}^2$, so in the construction we have $r = 2$.

Let $\{1, t\}$ be a basis for $\mathbb{F}$ over $\mathbb{K}$, where $t^2 = t + \theta$ for some $\theta \in \mathbb{K}$. A typical element of the Desarguesian spread of $\mathbb{F}^3$ is $\{(\lambda, \lambda\alpha, \lambda\beta) \mid \lambda \in \mathbb{F}\}$, for some $\alpha, \beta \in \mathbb{F}$. Writing $\lambda = u + tv$, $\alpha = a + tb$ and $\beta = c + td$ this subspace is

$$\{(u + tv, ua + v\theta b + t(ub + v(a + b)), uc + v\theta d + t(ud + v(c + d))) \mid u, v \in \mathbb{K}\}.$$

Thus $\mathcal{D}(V_1 \oplus V_2)$, the Desarguesian spread of $V_1 \oplus V_2 \cong \mathbb{F}^3 \cong \mathbb{K}^6$, is the union of $\mathcal{D}(V_2)$ which is

$$\{(0, 0, 0, 0, u, v) \mid u, v \in \mathbb{K}\} \cup \{\{(0, 0, u, v, ua + v\theta b, ub + v(a + b)) \mid u, v \in \mathbb{K}\} \mid a, b \in \mathbb{K}\}$$

and $\mathcal{D}(V_1 \oplus V_2) \setminus \mathcal{D}(V_2)$ which is

$$= \{\{(u, v, ua + v\theta b, ub + v(a + b), uc + v\theta d, ud + v(c + d)) \mid u, v \in \mathbb{K}\} \mid a, b, c, d \in \mathbb{K}\}.$$

Let $g, h \in \mathbb{K}[x, y]$ be linear over $\mathbb{F}_0$ and define

$$W = \{(0, 0, 0, w, 0, z) \mid z, w \in \mathbb{K}\}$$

and

$$U = \{(0, 0, x, h(x, y), y, g(x, y)) \mid x, y \in \mathbb{K}\}.$$

A typical spread element in $B(W)$ is of the form $\{(0, 0, u, v, ua, va) \mid u, v \in \mathbb{K}\}$ for some $a \in \mathbb{K}$, which is element of $B(U)$ if and only if there exist $x, y \in \mathbb{K}$ with the property that $xg(x, y) = yh(x, y)$. Thus we can construct the semifields $\mathbb{S}(U, W)$ and $\mathbb{S}(W, U)$ so long as $xg(x, y) = yh(x, y)$ has no non-trivial solution.

Let $v = (1, 0, 0, 0, 0, 0)$.

An element $R \in B(\langle U + v \rangle)$ is of the form

$$\{(u, v, ux + v\theta h(x, y), uh(x, y) + v(x + h(x, y)),$$

$$uy + v\theta g(x, y), ug(x, y) + v(y + g(x, y))) \mid u, v \in \mathbb{K}\},$$

for some $x, y \in \mathbb{K}$, and so

$$R/W = \{(u, v, ux + v\theta h(x, y), uy + v\theta g(x, y)) \mid u, v \in \mathbb{K}\}.$$

An element $T \in B(\langle W + v \rangle)$ is of the form

$$\{(u, v, v\theta w, uw + vw, v\theta z, uz + vz) \mid u, v \in \mathbb{K}\},$$

for some $w, z \in \mathbb{K}$. To calculate the quotient T/U we first form the span

$$T + U = \{(u, v, \theta vw + x, vw + uw + h(x, y), \theta vz + y, vz + uz + g(x, y)) \mid u, v, x, y \in \mathbb{K}\}$$

and intersect with a subspace of rank n which has trivial intersection with U, for example $X_3 = X_5 = 0$. Thus

$$T/U = \{(u, v, (u + v)w + h(\theta vw, \theta vz), (u + v)z + g(\theta vw, \theta vz)) \mid u, v \in \mathbb{K}\}.$$

Therefore the semifield $\mathbb{S}(U, W)$ (after applying the isotopism $((u, v) \mapsto (u, \theta^{-1}v), id, id)$) is defined by the multiplication

$$(u, v) \circ (x, y) = (ux + vh(x, y), uy + vg(x, y)),$$

which is the semifield $\mathbb{S}$, and the pre-semifield $\mathbb{S}(W, U)$ (after applying the isotopism $((u, v) \mapsto (u - v, \theta^{-1}v), id, id)$) is defined by the multiplication

$$(u, v) \circ (x, y) = (ux + h(vx, vy), uy + g(vx, vy)).$$

Note that given that $xg(x, y) = yh(x, y)$ implies $(x, y) = (0, 0)$ there is a quick proof that the multiplcation for $\mathbb{S}(W, U)$ gives a semifield. If $(ux + h(vx, vy), uy + g(vx, vy)) = 0$ and $(x, y) \neq 0$ then $vyh(vx, vy) = vxg(vx, vy)$ and so $v = 0$ and hence $u = 0$.

The Knuth operations allow us to construct twelve semifields, six from the semifield $\mathbb{S}(U, W)$ and six from the $\mathbb{S}(W, U)$. It seems difficult to determine if and when these twelve semifields will be pairwise non-isotopic. In the case that $\mathbb{S}(U, W)$ is related to a semifield flock, and is not a Dickson semifield, it is known that the Knuth operations produce three non-isotopic semifields from $\mathbb{S}(U, W)$ and another three non-isotopic semifields from $\mathbb{S}(W, U)$, see [3].

The multiplications for the twelve isotopy classes of semifields are listed in the table below. The semifield $\mathbb{S} = \mathbb{S}(U, W)$ and the semifield $\mathbb{T} = \mathbb{S}(W, U)$. The function f^t is the *transpose*, or *adjoint*, of the endomorphism f, defined by $(x, f(y)) = (f^t(x), y)$ for all $x, y \in \mathbb{F}$, where $(,)$ is a non-degenerate bilinear form on $\mathbb{F}$, viewed as a vector space over the ground field.

Isotopy Class	$(u,v)\circ(x,y)$
$[\mathbb{S}]$	$(ux+vh_1(x)+vh_2(y), uy+vg_1(x)+vg_2(y))$
$\tau_1([\mathbb{S}])$	$(ux+yh_1(u)+yh_2(v), vx+yg_1(u)+yg_2(v))$
$\tau_2([\mathbb{S}])$	$(ux+vy, uh_1(x)+uh_2(y)+vg_1(x)+vg_2(y)$
$\tau_1\tau_2([\mathbb{S}])$	$(ux+vy, xh_1(u)+xh_2(v)+yg_1(u)+yg_2(v))$
$\tau_2\tau_1([\mathbb{S}])$	$(ux+h_1^t(uy)+g_1^t(vy), vx+h_2^t(uy)+g_2^t(vy))$
$\tau_1\tau_2\tau_1([\mathbb{S}])$	$(ux+h_1^t(xv)+g_1^t(vy), uy+h_2^t(xv)+g_2^t(vy))$
$[\mathbb{T}]$	$(ux+h_1(vx)+h_2(vy), uy+g_1(vx)+g_2(vy))$
$\tau_1([\mathbb{T}])$	$(ux+h_1(uy)+h_2(vy), vx+g_1(uy)+g_2(vy))$
$\tau_2([\mathbb{T}])$	$(ux+vy, xh_1^t(u)+xg_1^t(v)+yh_2^t(u)+yg_2^t(v)$
$\tau_1\tau_2([\mathbb{T}])$	$(ux+vy, uh_1^t(x)+ug_1^t(y)+vh_2^t(x)+vg_2^t(y))$
$\tau_2\tau_1([\mathbb{T}])$	$(ux+yh_1^t(u)+yg_1^t(v), vx+yh_2^t(u)+yg_2^t(v))$
$\tau_1\tau_2\tau_1([\mathbb{T}])$	$(ux+vh_1^t(x)+vg_1^t(y), uy+vh_2^t(x)+vg_2^t(y))$

The twelve isotopy classes of semifields associated with a semifield $\mathbb{S}$ of rank 2 over its left nucleus

7. Final remarks

The importance of the equivalence between a finite semifield and the existence of the geometric configuration of subspaces U and W as explained in this article, is illustrated by the classification result of Cardinali *et al.* [5]. In the case that n is even and W is a line over $\mathbb{F}_{q^{n/2}}$, U can be seen as an $(n-1)$-dimensional subspace over $\mathbb{F}_q$, skew from a hyperbolic quadric in $PG(3,q^{n/2})$. (The Desarguesian spread over $\mathbb{F}_q$ becomes a Desarguesian spread of lines D' over $\mathbb{F}_{q^{n/2}}$ and the hyperbolic quadric is determined by the set of lines of D' which intersect W.) By studying these so-called *linear sets* skew from a hyperbolic quadric, Cardinali *et al.* managed to classify all semifields of order q^4 with kernel $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$.

On the other hand, this article leaves a number of issues unresolved.

Unlike the special case studied by Cardinali *et al.*, in general, the geometric construction does not appear to give much information about isotopism, see Remark 4.4. Can Theorem 2.1 in [5] be generalised to resolve this issue ?

We do not know if the operation that interchanges U and W is well defined on the semfields which can be constructed with $r=2$. More precisely, is it true that if $\mathbb{S}(U,W)$ is isotopic to $\mathbb{S}(U',W')$, then $\mathbb{S}(W,U)$ is isotopic to $\mathbb{S}(W',U')$?

Does the operation that interchanges U and W extend to all semifields and if so, how many semifields does this operation produce in conjunction with the Knuth operations ?

8. Acknowledgements

The authors would like to thank Tim Penttila for his useful suggestions and Bill Kantor for his many comments, suggestions and queries on earlier versions of this article.

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., 1960.

[2] A. A. Albert, Generalized Twisted Fields, *Pacific J. Math.*, **11** (1961), 1–8.

[3] S. Ball and M. R. Brown, The six semifield planes associated with a semifield flock, *Adv. Math.*, **189** (2004) 68–87.

[4] A. Barlotti and J. Cofman, Finite Sperner spaces constructed from projective and affine spaces. *Abh. Math. Sem. Univ. Hamburg*, **40** (1974) 231–241.

[5] I. Cardinali, O. Polverino, R. Trombetti, Semifield planes of order q^4 with kernel $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$, it Europ. J. Combin., **27** (2006) 940-961.

[6] R. S. Coulter and R. W. Matthews, Planar functions and planes of Lenz-Barlotti class II, *Des. Codes Cryptogr.*, **10** (1997) 167–184.

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

[8] U. Dempwolff, Translation Planes of Order 27, *Des. Codes Cryptogr.*, **4** (1994) 105–121.

[9] L. E. Dickson, On finite algebras, *Göttingen Nachrichtung*, (1905) 358–393.

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

[11] W. M. Kantor, Commutative semifields and symplectic spreads, *J. Algebra*, **270** (2003) 96–114.

[12] W. M. Kantor and M. E. Williams, Symplectic semifield planes and $\mathbb{Z}_4$-linear codes, *Trans. Amer. Math. Soc.*, **356** (2004) 895–938.

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

[14] The Magma Computational Algebra System for Algebra, Number Theory and Geometry (http://magma.maths.usyd.edu.au/).