A NEW APPROACH TO FINITE SEMIFIELDS

SIMEON BALL, GARY EBERT, AND MICHEL LAVRAUW

Abstract. A finite semifield is shown to be equivalent to the existence of a particular geometric configuration of subspaces with respect to a Desarguesian spread in a finite dimensional vector space over a finite field. In 1965 Knuth [12] showed that each finite semifield generates in total six (not necessarily isotopic) semifields. In certain cases, the geometric interpretation obtained here allows us to construct another six semifields. In 1987 Hiramine *et. al* [8] gave an iterative construction of semifields of order q^{2^n} starting from a semifield of order q of rank two over its left nucleus. The geometric interpretation, together with Knuth's operations, allows us to construct up to six non-isotopic semifields of order q^2 from a semifield of order q of rank two of its left nucleus, two of which serve as a base for the iterative construction.

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 [7]) when they were called *non-associative division rings* or *distributive quasifields*. Following Knuth [12] and the recent literature we will use the name semifield. Throughout this paper the term semifield 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 with respect to a Desarguesian spread. 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

Date: 2 June 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).

operation on semifields on a certain class of semifields, those of rank two over their left nucleus, and implications for the iterative construction of Hiramine *et al.* [8].

For more on spreads, translation planes and isotopy, see [1], [5], and [9].

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 [5]). 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 Desarguesian 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. 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

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

Note that this property implies that $V_r = U \oplus W$ but the converse does not hold in general. It also implies that $V_r = S \oplus W$ for all $S \in B(U)$.

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.

Now we show that $\mathcal{S}(U,W)$ is a semifield spread. Let $\{e_i \mid i = 1, \ldots, n\}$ be a basis for $\mathbb{F}$ viewed as a vector space over $\mathbb{F}_0$ and put $e_1 = 1$. Let ψ be the bijection from $\mathbb{F}$ to $\mathbb{F}_0^n$ defined by

$$\psi(\sum_{i=1}^{n} a_i e_i) = (a_1, a_2, \ldots, a_n).$$

Let V be a vector space of rank $r+1$ over $\mathbb{F}$ and extend ψ in the natural way to a bijection between V and $V_1 \oplus V_r$. Let $\{f_i \mid i = 1, \ldots, r+1\}$ be a basis for V over $\mathbb{F}$, such that V_1 is the image of $\langle f_1\rangle$ under ψ and V_r is the image of $\langle f_2, \ldots, f_{r+1}\rangle$, and let $\alpha = (1, \alpha_2, \ldots, \alpha_{r+1}) \in \mathbb{F}^{r+1}$. Consider the element ϕ_α of $\mathrm{GL}(V)$ defined by $\phi_\alpha(f_1) = \alpha$ and $\phi_\alpha(f_i) = f_i$ for $i = 2, \ldots, r+1$. The image of the vector $(x_1, \ldots, x_{r+1}) \in V$ is $(x_1, x_2 + \alpha_2 x_1, \ldots x_{r+1} + \alpha_{r+1} x_1)$. The composition $\psi_\alpha := \psi\phi_\alpha\psi^{-1}$ induces a semilinear automorphism of $V_1 \oplus V_r$, moreover this automorphism will fix V_r pointwise and will fix $A(U) := \langle U, (1, 0, \ldots, 0)\rangle$ setwise. Let S and T be distinct elements of $B(A(U)) \setminus B(U)$ and suppose $S \cap A(U) = \langle s\rangle$ and $T \cap A(U) = \langle t\rangle$. Then $\psi\phi_\alpha\psi^{-1}(t) = \psi(1, t_2 + \alpha_2, \ldots, t_{r+1} + \alpha_{r+1})$, and choosing $\alpha_k = s_k - t_k$ we obtain an element of $\mathrm{GL}(V_1 \oplus V_r)$ fixing $A(U)$ and taking T to S. The set of linear transformations obtained in this way form a group of order q^n acting transitively on the elements of $B(\langle v, U\rangle) \setminus B(U)$ and fixing V_r pointwise. In the quotient geometry this group induces a subgroup of $\Gamma\mathrm{L}((V_1 \oplus V_r)/W)$ fixing V_r/W pointwise and acting transitively on the other elements of $\mathcal{S}(U,W)$. Hence $\mathcal{S}(U,W)$ is a semifield spread. □

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 depends 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 $a \in \mathrm{GF}(q^n)$. Without loss of generality we may assume that $v = (1,0,\ldots,0)$ and we have bases as in the proof of Theorem 2.2. Then for ϕ choose the element of $\Gamma\mathrm{L}(r+1,q^n)$ defined by

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

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. Let ϕ be any element of $\Gamma\mathrm{L}(rn+n,q)$ fixing $\mathcal{D}(V_1 \oplus V_r)$ such that the restriction of ϕ to V_r equals φ. It follows from Remark 2.3 that $\mathbb{S}(U,W)$ is independent of the choice of v. So we may assume that

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

$$\mathcal{S}(U',W') = \{\langle R',W'\rangle/W' \mid R' \in B(\langle v^\phi,U'\rangle)\},$$

for some $v \in (V_1 \oplus V_r) \setminus V_r$. If $\overline{\phi}$ denotes the isomorphism between $(V_1 \oplus V_r)/W$ and $(V_1 \oplus V_r)/W'$ induced by the action of ϕ on the quotient geometry $(V_1 \oplus V_r)/W$ (and its subspaces), i.e.,

$$\begin{array}{rccc} \overline{\phi} \ : & (V_1 \oplus V_r)/W & \to & (V_1 \oplus V_r)/W^\phi \\ & \langle T,W\rangle/W & \mapsto & \langle T^\phi,W^\phi\rangle/W^\phi \end{array},$$

for any subspace T of $V_1 \oplus V_r$, then

$$\mathcal{S}(U,W)^{\overline{\phi}} = \{\langle R^\phi,W^\phi\rangle/W^\phi \mid R \in B(\langle v,U\rangle)\}.$$

Since ϕ fixes $\mathcal{D}$, it follows that

$$R \in B(T) \iff R^\phi \in B(T^\phi).$$

Hence

$$\mathcal{S}(U,W)^{\overline{\phi}} = \{\langle R,W^\phi\rangle/W^\phi \mid R \in B(\langle v^\phi,U^\phi\rangle)\} = \mathcal{S}(U',W'),$$

and therefore $\mathbb{S}(U,W)$ and $\mathbb{S}(U',W')$ are isotopic semifields. □

3. Examples

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

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

Let q be an odd prime power. The generalised twisted field $(\mathbb{F},+,\circ)$ 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 $\eta \in \mathbb{F}\setminus\{a^{q-1} \mid a\in\mathbb{F}\}$.

Note that the generalised twisted field is a pre-semifield and not a semifield since it does not contain a multiplicative identity. However, there is always a semifield isotopic to a pre-semifield, see [12], so for our purposes it suffices to consider pre-semifields.

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** [11]. ($r=3$)

Let q be even and $\mathbb{F}$ be an extension of $\mathbb{F}_0$ of odd degree n. Let $f(x)=\sum_{i=0}^{n-1}b_ix^{q^i}$ be an additive function from $\mathbb{F}$ to $\mathbb{F}$ such that

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

has no non-trivial solutions. Let $\hat{f}(x)=\sum_{i=0}^{n-1}(b_ix)^{q^{-i}}$, $b_i\in\mathbb{F}$. The Kantor-Williams symplectic pre-semifield $(\mathbb{F},+,\circ)$ is defined by

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

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

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

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

3.3. **The Coulter-Matthews commutative semifields** [4]**.** ($r = 3$)

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

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

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 $z = xy$, $z^3 - w^9 - z = x^9y$ and $w = x^{1/9}y$ hold simultaneously, which implies $(xy)^3 - xy^9 - xy = x^9y$. 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

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

As mentioned in [10] there is still no published proof that this semifield is not isotopic to a generalised twisted semfield. Note that the signs are mixed-up in the multiplication of the Coulter-Matthews semifield as listed in [10]; 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 [5]).

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 $\mathbb{F}_0$

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

Let U and W be the subspaces of V_n defined 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 let

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

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

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

and

$$-\sum_{i=1}^{n-1} z_i^{p^i} = y c_0(x).$$

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. We shall see more examples of semifields that can be constructed with r small in Section 5.*

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. Of course assuming a large left, right or middle nucleus (see Section 5 for definitions) is another way to reduce the search space but choosing r to be small opens up the possibility of finding other semifields. The generalised twisted semifields for example, constructed in the last section with $r = 2$, do not generally have a large nucleus.*

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. In fact, it follows from the proof of Theorem 4.1 that all finite semifields of a given order over a fixed prime field, can be constructed using the same W. With this knowledge it is quite tempting to conjecture that if two semifields $\mathbb{S}(U, W)$ and $\mathbb{S}(U', W)$ (where U, U', and W are subspaces of V_r) are isotopic, then there exists an element $\varphi \in \Gamma L(V_r)$, such that φ fixes the Desarguesian spread and $U^\varphi = U'$. However this conjecture would turn out to be false due to the following counterexample, which was found using the computer package MAGMA* [14]. *In $\mathbb{F}_3^9$ one can construct a Desarguesian spread and find $\mathbb{F}_3$-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 (*[6]*), 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'.*

5. Semifield operations

In [12] Knuth noted the group S_3 acts on the set of finite semifields. The group S_3 is generated by the involutions τ_1, which changes the order of multiplication and is equivalent to dualising the semifield plane, and τ_2 which dualises the semifield spread; this geometrical interpretation was first observed in [3] and elaborated in [10]. In [12] Knuth also shows that 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 exist 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 $x, y \in \mathbb{F}$. The identity map will be denoted as id.

If a semifield $\mathbb{S} = \mathbb{S}(U, W)$ 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 $\mathbb{S}(W, U)$. We shall consider the effect of this switching operation on some classes of semifields and look for isotopisms between the resulting semfields.

5.1. **The semifields associated with semifields of rank 2 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 $h, g \in \mathbb{K}[x, y]$, 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 and h be bilinear forms, linear over $\mathbb{F}_0$, in $\mathbb{K}[x, y]$. Let

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

and let

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

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

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

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

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

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

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 $((u, v) \mapsto (u, \theta^{-1}v), id, id)$) 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 $u = 0$.

5.2. **The semifields associated with a semifield flock** [3]**.** The switching operation is a generalisation of the geometric operation $\mathbb{S} \mapsto \hat{\mathbb{S}}^{*\dagger}$, for semifields associated with a semifield flock, which appears in [13]. For these semifields $g(x,y) = x + f_2(y)$ and $h(x,y) = f_1(y)$ so the condition $xg(x,y) = yh(x,y)$ has no non-trivial solutions becomes the condition that $f_2(y)^2 + 4yf_1(y)$ is a non-square for all $y \in \mathbb{K}^*$. Thus the six semifields associated with a semifield flock are related by the switching operation together with the Knuth operations.

5.3. **The Hiramine, Matsumoto, Oyama construction** [8]**.** Let λ be an element of $\mathbb{F}$ with the property that $\lambda^2 + \lambda \in \mathbb{K}$ and let $x \mapsto x^{\sigma+1}$ be the norm map from $\mathbb{F}$ to $\mathbb{K}$.

In [8] Hiramine *et al.* note that if $\mathbb{T} = (\mathbb{K}^2, +, \cdot)$ is a semifield of rank two over its left nucleus, defined by

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

then $\mathbb{S} = (\mathbb{F}^2, +, \circ)$ is a semifield (also of rank two over its left nucleus) defined by

$$(u,v) \circ (x,y) = (ux + vf(y), uy + vx^\sigma),$$

where $f(a + \lambda b) = g(a,b) - h(a,b) + \lambda g(a,b)$.

The switching operation applied to semifields of rank two over their left nucleus that we saw in Section 5.1 allows us to construct another semifield $\tau_3(\mathbb{S})$ of order $|\mathbb{F}|^2$ defined by

$$(u,v) \circ (x,y) = (ux + f(vy), uy + (vx)^\sigma).$$

Note that $\tau_3(\mathbb{S})$ is isotopic to $\tau_1\tau_3(\mathbb{S})$ and so the plane coordinatised by $\tau_3(\mathbb{S})$ is self-dual.

Remark 5.1. *There is a direct proof that $\tau_3(\mathbb{S})$ is a semifield given that*

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

defines a semifield $(\mathbb{K}^2, +, \cdot)$. If

$$(ux + f(vy), uy + (vx)^\sigma) = (0,0)$$

and $(x,y) \neq 0$ then $yf(vy) = v^\sigma x^{\sigma+1}$. Writing $vy = a + \lambda b$ we have

$$(a + \lambda b)(g(a,b) - h(a,b) + \lambda g(a,b)) = (vx)^{\sigma+1} \in \mathbb{K},$$

from which it follows that $ag(a,b) - bh(a,b) = 0$, since $\lambda^2 + \lambda \in \mathbb{K}$. In Section 5.1 we saw that this implies that $a = b = 0$ and hence $vy = 0$. If $v = 0$ then $u = 0$ and if $y = 0$ then $(u,v) = (0,0)$, so either way $(u,v) = (0,0)$.

We could expect that there are six non-isotopic semifields associated with $\mathbb{S}$ via the Knuth operations, however we shall see that this is not the case.

To calculate the multiplication for $\tau_2(\mathbb{S})$ we dualise the spread associated with $\mathbb{S}$. Let $(,)$ be the alternating form $((u,v,w,z),(a,b,c,d)) = Tr(cu + dv - aw - bz)$, where Tr is the trace function from $\mathbb{K}$ to the prime field. A typical element of the spread associated with $\mathbb{S}$ is of the form

$$\{(u,v,ux + vf(y), uy + vx^\sigma) \mid u,v \in \mathbb{K}\}.$$

The dual subspace of this subspace is

$$\{(a,b,c,d) \mid Tr(cu + dv - a(ux + vf(y)) - b(uy + vx^\sigma)) = 0\},$$

Putting $v = 0$ we see that $c = ax + by$ and putting $u = 0$ we have $d = af(y) + bx^\sigma$. Thus the semifield $\tau_2(\mathbb{S})$ has multiplication

$$(u, v) \circ (x, y) = (vy + ux, vx^\sigma + uf(y)),$$

which, applying the isotopism $((u, v) \mapsto (v, u), (x, y) \mapsto (x^\sigma, y), (a, b) \mapsto (b, a))$, is the multiplication that defines the semifield $\mathbb{S}$, thus $\tau_2(\mathbb{S}) \simeq \mathbb{S}$.

Clearly $\tau_1(\mathbb{S})$ has multiplication defined by

$$(u, v) \circ (x, y) = (ux + yf(v), xv + yu^\sigma).$$

For any additive function $f(x) = \sum_{i=0}^{n-1} b_i x^{q^i}$ we define $\hat{f}(x) = \sum_{i=0}^{n-1} (b_i x)^{q^{-i}}$

Calculating as above the multiplication for $\tau_2\tau_1(\mathbb{S})$ is

$$(u, v) \circ (x, y) = (ux + (vy)^\sigma, vx + \hat{f}(uy))$$

which, applying the isotopism $((u, v) \mapsto (v, u), (x, y) \mapsto (y, x), (a, b) \mapsto (a^\sigma, b))$, is isotopic to the semifield with multiplication

$$(u, v) \circ (x, y) = (ux + (vy)^\sigma, uy + \hat{f}(xv)).$$

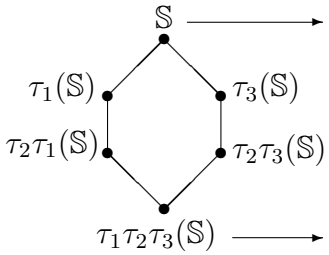
Note that this also shows that $\tau_1\tau_2\tau_1(\mathbb{S}) \simeq \tau_2\tau_1(\mathbb{S})$, which already follows from $\mathbb{S} \simeq \tau_2(\mathbb{S})$.

Now according to Section 5.1 we can apply τ_3 to this semifield and get the semifield $\tau_3\tau_2\tau_1(\mathbb{S})$ (of rank two over its left nucleus !) defined by the multiplication

$$(u, v) \circ (x, y) = (ux + vy^\sigma, uy + v\hat{f}(x)).$$

Furthermore, by calculating $\tau_2\tau_3(\mathbb{S})$ as above, one can check that $\tau_1\tau_2\tau_3(\mathbb{S}) \simeq \tau_3\tau_2\tau_1(\mathbb{S})$.

To summarise, the Knuth and switching operations generate six (possibly non-isotopic) semifields two of which are of rank two over their left nucleus and so serve as bases for iterative constructions of semifields of order $|\mathbb{F}|^{2^n}$. The very first time we use the iterative process we can also use $\tau_2(\mathbb{T})$ as a base, since the Knuth operation τ_2 dualises the spread and does not affect the size of the left nucleus.



The six semifields associated with the Hiramine *et al.* construction.

In the figure the arrows indicate the semifields that can be used as a basis for the iterative process. Note that isotopisms between the six semifields will depend on the semifield $\mathbb{S}$ and even for specific semifields it seems difficult to determine when the six semifields are mutually non-isotopic. For example, in [3] it was shown that the six semifields of order 3^{10} associated with the Penttila-Williams semifield, for which $g(x, y) = x + y^{27}$ and $h(x, y) = y^9$, are mutually non-isotopic. This means that we can construct twelve

semifields of order 3^{20} but it is not clear to us whether there are any isotopisms between them.

6. Acknowledgements

The authors would like to thank Tim Penttila for his useful suggestions and Bill Kantor for his many comments on an earlier version 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] R. S. Coulter and R. W. Matthews, Planar functions and planes of Lenz-Barlotti class II, *Des. Codes Cryptogr.*, **10** (1997) 167–184.
[5] P. Dembowski, *Finite Geometries*, Springer, Berlin, 1968.
[6] U. Dempwolff, Translation Planes of Order 27, *Des. Codes Cryptogr.*, **4** (1994) 105–121.
[7] L. E. Dickson, On finite algebras, *Göttingen Nachrichtung*, (1905) 358–393.
[8] Y. Hiramine, M. Matsumoto and T. Oyama, On some extension of 1-spread sets, *Osaka Math. J.*, **24** (1987), 123–137.
[9] D. R. Hughes and F. C. Piper, *Projective Planes*, Springer, Berlin, 1973.
[10] W. M. Kantor, Commutative semifields and symplectic spreads, *J. Algebra*, **270** (2003) 96–114.
[11] W. M. Kantor and M. E. Williams, Symplectic semifield planes and $\mathbb{Z}_4$-linear codes, *Trans. Amer. Math. Soc.*, **356** (2004) 895–938.
[12] D. E. Knuth, Finite semifields and projective planes, *J. Algebra*, **2** (1965) 182–217.
[13] M. Lavrauw, The two sets of three semifields associated with a semifield flock, *Innovations in Inicidence Geometry*, **2** (2005) 101–107.
[14] The Magma Computational Algebra System for Algebra, Number Theory and Geometry (http://magma.maths.usyd.edu.au/).