Adv. Geom. **11** (2011), 399–410
DOI 10.1515/ADVGEOM.2011.014

Advances in Geometry

Finite semifields with a large nucleus and higher secant varieties to Segre varieties

Michel Lavrauw*

(Communicated by T. Pentilla)

Abstract. In [2] a geometric construction was given 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. Moreover, it was proved that any finite semifield can be obtained in this way. In [7] we proved that the configuration needed for the geometric construction given in [2] for finite semifields is equivalent with an $(n-1)$-dimensional subspace skew to a determinantal hypersurface in $\mathrm{PG}(n^2-1,q)$, and provided an answer to the isotopism problem in [2]. In this paper we give a generalisation of the BEL-construction using linear sets, and then concentrate on this configuration and the isotopism problem for semifields with nuclei that are larger than its centre.

1 Finite semifields

A *finite semifield* $\mathbb{S}$ is a finite division algebra, which is not necessarily associative, i.e., 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 $x\in\mathbb{S}$;

A finite field is of course a trivial example of a semifield. The first non-trivial examples of semifields were constructed by Dickon in [5]. One easily shows that the additive group of a semifield is elementary abelian, and the additive order of the elements of $\mathbb{S}$ is called the *characteristic* of $\mathbb{S}$. Contained in a semifield are the following important substructures, all of which are isomorphic to a finite field. The *left nucleus* $\mathbb{N}_l(\mathbb{S})$, the *middle nucleus*

*This research was supported by the Fund for Scientific Research - Flanders (FWO).

$\mathbb{N}_m(\mathbb{S})$, and the *right nucleus* $\mathbb{N}_r(\mathbb{S})$ are defined as follows:

$$\mathbb{N}_l(\mathbb{S}) := \{x : x \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \forall y, z \in \mathbb{S}\} \quad (1)$$

$$\mathbb{N}_m(\mathbb{S}) := \{y : y \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \forall x, z \in \mathbb{S}\} \quad (2)$$

$$\mathbb{N}_r(\mathbb{S}) := \{z : z \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \forall x, y \in \mathbb{S}\} \quad (3)$$

The intersection of the *associative centre* $\mathbb{N}(\mathbb{S})$ (the intersection of the three nuclei) and the commutative center is called the *center* of $\mathbb{S}$ and denoted by $C(\mathbb{S})$.

If $\mathbb{S}$ is an n-dimensional algebra over the field $\mathbb{F}$, and $\{e_1, \ldots, e_n\}$ is an $\mathbb{F}$-basis for $\mathbb{S}$, then the multiplication can be written in terms of the multiplication of the e_i, i.e., if $x = x_1e_1 + \cdots + x_ne_n$ and $y = y_1e_1 + \cdots + y_ne_n$, with $x_i, y_i \in \mathbb{F}$, then

$$x \circ y = \sum_{i,j=1}^{n} x_i y_j e_i \circ e_j = \sum_{i,j=1}^{n} x_i y_j \left(\sum_{k=1}^{n} a_{ijk} e_k \right) \quad (4)$$

for certain $a_{ijk} \in \mathbb{F}$, called the *structure constants* of $\mathbb{S}$ with respect to the basis $\{e_1, \ldots, e_n\}$. In [6] Knuth noted that the action, of the symmetric group S_3, on the indices of the structure constants gives rise to another five semifields starting from one semifield $\mathbb{S}$. This set of at most six semifields is called the S_3-*orbit* of $\mathbb{S}$, and consists of the semifields $\{\mathbb{S}, \mathbb{S}^{(12)}, \mathbb{S}^{(13)}, \mathbb{S}^{(23)}, \mathbb{S}^{(123)}, \mathbb{S}^{(132)}\}$.

The study of semifields was stimulated by the connection with projective planes and in this context the following notion of isotopism arose. An *isotopism* between the two semifields $\mathbb{S}$ and $\hat{\mathbb{S}}$ is a triple (F, G, H) of non-singular linear transformations from $\mathbb{S}$ to $\hat{\mathbb{S}}$ such that $x^F \hat{\circ} y^G = (x \circ y)^H$, for all $x, y \in \mathbb{S}$. In this case the semifields $\mathbb{S}$ and $\hat{\mathbb{S}}$ are called isotopic. The set of semifields isotopic to a given semifield $\mathbb{S}$ is called the *isotopism class* of $\mathbb{S}$ and is denoted by $[\mathbb{S}]$. In the next section we give the necessary preliminaries needed for Section 3, where we generalise the geometric construction given in [2].

2 Semifield spreads, Desarguesian spreads and linear sets

Let $\mathrm{PG}(V)$ denote the projective space induced by the vector space V. If we want to specify the dimension d and the field $\mathbb{F}$ of scalars, then we write $V(d, \mathbb{F})$ (or $V(d, q)$ if $\mathbb{F} = \mathbb{F}_q$, the finite field of order q), and similarly for the corresponding projective space $\mathrm{PG}(V)$, we write $\mathrm{PG}(d-1, \mathbb{F})$ (or $\mathrm{PG}(d-1, q)$). We denote the collineation group of a projective space $\mathrm{PG}(d-1, \mathbb{F})$ (respectively Σ) by $\mathrm{P\Gamma L}(d, \mathbb{F})$ (respectively $\mathrm{P\Gamma L}(\Sigma)$).

A *spread* of $V = V(d, q)$ is a set $\mathcal{S}$ of subspaces of V, all of the same dimension 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 $|\mathcal{S}| = (q^d - 1)/(q^{d'} - 1)$. A trivial example of a spread of V is the set of all subspaces of dimension 1 of V. 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. Spreads play a key role in the theory of translation planes due to the André–Bruck–Bose construction. The translation planes corresponding to semifield spreads are called *semifield planes*.

The semifield spread $\mathcal{S}(\mathbb{S})$ of $\mathrm{PG}(2n-1,q)$ corresponding to the semifield $\mathbb{S}$ of order q^n, with multiplication given by $x \circ y$ and left nucleus $\mathbb{F}_q$, consists of the subspace $S_\infty = \{(0,y) : y \in \mathbb{F}_{q^n}^*\}$, together with the subspaces

$$S_x = \left\{(y, y \circ x) : y \in \mathbb{F}_{q^n}^*\right\}, \quad x \in \mathbb{F}_{q^n}.$$

Let $\mathbb{F}_{q^n}$ be the finite field of q^n elements, let $\mathbb{F}_q$ be the subfield of q elements and assume $n \geq 2$. Consider $V(d,q^n)$ as a vector space of dimension dn over $\mathbb{F}_q$ and consider the spread of subspaces of dimension n over $\mathbb{F}_q$ arising from the spread of subspaces of dimension 1 over $\mathbb{F}_{q^n}$. Such a spread (i.e. arising from a spread of subspaces of dimension 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. All of the above notions, defined in terms of vector spaces, can also be defined in terms of projective spaces. In this paper we will use the same terminology for both points of view.

The correspondence between the points of the projective space over $\mathbb{F}_{q^n}$ and the elements of the Desarguesian $(n-1)$-spread $\mathcal{D}$ in $\mathrm{PG}(dn-1,q)$ is sometimes referred to as *field reduction*. Once this correspondence is established we will often consider the set of spread elements intersecting a given subspace or subset U, and we use the following notation:

$$B_{\mathcal{D}}(U) := \{R \in \mathcal{D} : R \cap U \neq \emptyset\}.$$

If there is no confusion possible we write $B(U)$ instead of $B_{\mathcal{D}}(U)$, and we will often identify the elements of $\mathcal{D}$ with the points of $\mathrm{PG}(d-1,q)$. By doing so, each subset U of $\mathrm{PG}(dn-1,q^n)$ induces a set $B(U)$ of points in $\mathrm{PG}(d-1,q^n)$.

A set of points L in $PG(r-1,q_0)$ is called a *linear set* if there exists a subspace U in $PG(rt-1,q)$, for some $t \geq 1$, $q^t = q_0$, such that $L = B(U)$ is the set of points corresponding to the elements of a Desarguesian $(t-1)$-spread of $PG(rt-1,q)$ intersecting U. If we want to specify the field over which L is linear we call L an *$\mathbb{F}_q$-linear set*. The same notation and terminology is used when U is a subspace of the vector space $V(rt,q)$ instead of a projective subspace. If moreover we want to mention the dimension of U, we call $B(U)$ a linear set *of rank* d or *of dimension* $d-1$, if U is a $(d-1)$-dimensional subspace of $\mathrm{PG}(rt-1,q)$. Lunardon [8] was one of the first to give importance to these linear sets, and in the last ten years linear sets have played an important role in Finite Geometry, for an overview of applications and connections we refer to [11]. The algebraic connection between linear sets and finite semifields has been successfully used in recent years, see e.g. [4], [10]. In the next section we will give a geometric construction of finite semifields starting from a linear set.

3 A generalisation of the BEL-construction

In this section we generalise the geometric construction for semifields given in [2] starting from a configuration of two subspaces with respect to a Desarguesian spread to a geometric construction starting from a linear set and a subspace. Another difference with the construction given in [2] is that now we do not start with a fixed Desarguesian spread

$\mathcal{D}$. We only use geometric properties of $\mathcal{D}$ in the proof and different choices of $\mathcal{D}$ may give different semifields. Because of this approach the spread $\mathcal{D}$ should be included in the notation of the obtained semifield and of the semifield spread. This is why in what follows we write $\mathbb{S}(\mathcal{D}, U, W)$ instead of the notation $\mathbb{S}(U, W)$ used in [2].

First we recall the BEL-construction as given in [2]. Let U be a subspace of dimension $n-1$, W a subspace of dimension $rn-n-1$ in $\Sigma := \mathrm{PG}(rn-1, q)$, and $\mathcal{D}$ a Desarguesian $(n-1)$-spread in Σ, such that no element of $\mathcal{D}$ intersects both W and U. In [2] it was shown that this configuration of subspaces gives rise to a semifield $\mathbb{S}(\mathcal{D}, U, W)$ of order q^n, corresponding to the semifield spread $\mathcal{S}(\mathcal{D}, U, W)$ constructed as follows.

(a) Embed Σ in $\Lambda \cong \mathrm{PG}(rn+n-1, q)$ and extend $\mathcal{D}$ to a Desarguesian spread $\mathcal{D}_1$ of Λ.
(b) Let A be a n-dimensional subspace of Λ intersecting Σ in U.
(c) Let $\mathcal{S}(U, W)$ be the set of subspaces in the quotient space Λ/W defined by A in the following way:

$$\mathcal{S}(\mathcal{D}, U, W) := \{\langle R, W\rangle/W : R \in \mathcal{D}_1, R \cap A \neq \emptyset\}.$$

Now we extend this to a geometric construction of a semifield spread starting from a linear set L and subspace W instead of two subspaces U and W. Let $L = B(U)$ be an $\mathbb{F}_q$-linear set of $\Sigma_1 := \mathrm{PG}(rn-1, q^s)$ of rank ns, $s \geq 1$, $r \geq 2$, and let W be a subspace of Σ_1 of dimension $rn-n-1$, and $\mathcal{D}$ a Desarguesian $(n-1)$-spread of Σ_1, such that no element of $\mathcal{D}$ intersects both L and W. We will show that this configuration gives rise to a semifield of order q^{ns}. For future reference we call a triple $(\mathcal{D}, U, W)$ satisfying the above properties a *BEL-configuration*. The construction of the semifield spread goes as follows

(i) Embed Σ_1 in $\Lambda_1 \cong \mathrm{PG}(rn+n-1, q^s)$ and extend $\mathcal{D}$ to a Desarguesian $(n-1)$-spread $\mathcal{D}_1$ of Λ_1.
(ii) Let $L' = B(U')$, $U \subset U'$, be an $\mathbb{F}_q$-linear set of Λ_1 of rank $ns+1$, such that $L' \cap \Sigma_1 = L$.
(iii) Let $\mathcal{S}(\mathcal{D}, U, W)$ be the set of subspaces defined by L' in the quotient geometry $\Lambda_1/W \cong \mathrm{PG}(2n-1, q^s)$ of W, in the following way:

$$\mathcal{S}(\mathcal{D}, U, W) = \{\langle R, W\rangle/W : R \in \mathcal{D}_1, R \cap L' \neq \emptyset\}.$$

Theorem 3.1. *The set $\mathcal{S}(\mathcal{D}, U, W)$ is a semifield spread of* $\mathrm{PG}(2n-1, q^s)$.

Proof. Consider the Desarguesian $(s-1)$-spread $\mathcal{D}_2$ of $\Lambda_2 \cong \mathrm{PG}(rns+ns-1, q)$, obtained by considering the points of Λ_1 as subspaces over $\mathbb{F}_q$ (i.e. by field reduction). Recall that if T is a subset of Λ_i, then

$$B_{\mathcal{D}_i}(T) := \{R \in \mathcal{D}_i : R \cap T \neq \emptyset\}.$$

If there is no confusion, then we identify the elements of $\mathcal{D}_2$ with the points of Λ_1, and the elements of $\mathcal{D}_1$ with the points of $\mathrm{PG}(r, q^{ns})$. Let Σ_2 denote the $(rns-1)$-dimensional subspace of Λ_2 corresponding to Σ_1, i.e., $B_{\mathcal{D}_2}(\Sigma_2) = \Sigma_1$. For any subset T of Λ_1, we denote the set of elements of $\mathcal{D}_2$ corresponding to T by $S_{\mathcal{D}_2}(T)$, i.e.

$$S_{\mathcal{D}_2}(T) := \{X \in \mathcal{D}_2 : B_{\mathcal{D}_2}(X) \in T\}. \tag{5}$$

Note that $S_{\mathcal{D}_2}(\Lambda_1) = \mathcal{D}_2$.

First we show that two different elements of $\mathcal{S}(\mathcal{D}, U, W)$ are skew. Suppose by way of contradiction that two different elements $\langle R_1, W\rangle/W$ and $\langle R_2, W\rangle/W$ of $\mathcal{S}(\mathcal{D}, U, W)$, have a non-trivial intersection. Note that this clearly implies that not both R_1 and R_2 are contained in Σ_1. Also, if one of R_1 and R_2 is contained in Σ_1, then W, R_1 and R_2 span the whole of Λ_1, and hence $\langle R_1, W\rangle/W$ and $\langle R_2, W\rangle/W$ cannot have a point in common, contradicting our hypothesis. So the only possibility that is left is the case where both R_1 and R_2 are skew to Σ_1, since an element of $\mathcal{D}_1$ either intersects Σ_1 trivially, or is contained in Σ_1. By the hypothesis the dimension of the subspace spanned by R_1, R_2 and W can be at most $rn+n-2$, and hence the subspace $\langle R_1, R_2\rangle$ (of dimension $2n-1$) must intersect the subspace W in at least a point, say the point $x \in \langle R_1, R_2\rangle \cap W$. It follows that

$$\langle R_1, R_2\rangle \cap \Sigma_1 = B_{\mathcal{D}_1}(x) \in B_{\mathcal{D}_1}(W).$$

Applying $S_{\mathcal{D}_2}$ we obtain

$$S_{\mathcal{D}_2}(\langle R_1, R_2\rangle \cap \Sigma_1) = S_{\mathcal{D}_2}(B_{\mathcal{D}_1}(x)),$$

and since each of the arguments of $S_{\mathcal{D}_2}$ in the above equality is either an element of $\mathcal{D}_1$ or spanned by elements of $\mathcal{D}_1$, it follows that

$$\langle S_{\mathcal{D}_2}(R_1), S_{\mathcal{D}_2}(R_2)\rangle \cap \Sigma_2 = \langle S_{\mathcal{D}_2}(B_{\mathcal{D}_1}(x))\rangle. \tag{6}$$

By construction we know that R_i $(i = 1, 2)$ meets $B_{\mathcal{D}_2}(U')$ non-trivially. Also, since U' has rank $ns + 1$, is not contained in Σ_1 but contains U, it is clear that any subspace of Λ_2 which is skew to Σ_2 intersects U' in at most one point. In particular, $\langle S_{\mathcal{D}_2}(R_i)\rangle$ intersects U' in exactly one point, say t_i $(i = 1, 2)$. Since the line $\langle t_1, t_2\rangle$ is contained in U' it must intersect U in a point, say $u \in U$, and hence $B_{\mathcal{D}_2}(u) \subset \langle B_{\mathcal{D}_2}(t_1), B_{\mathcal{D}_2}(t_2)\rangle$. But then by (6) it follows that

$$B_{\mathcal{D}_2}(u) \subset \langle B_{\mathcal{D}_2}(t_1), B_{\mathcal{D}_2}(t_2)\rangle \cap \Sigma_2 \subset \langle S_{\mathcal{D}_2}(R_1), S_{\mathcal{D}_2}(R_2)\rangle \cap \Sigma_2 = \langle S_{\mathcal{D}_2}(B_{\mathcal{D}_1}(x))\rangle,$$

and hence $B_{\mathcal{D}_1}(x)$ contains a point of $B_{\mathcal{D}_2}(U)$. This contradicts our assumption that no element of $\mathcal{D}_1$ intersects both W and $L = B_{\mathcal{D}_2}(U)$. We conclude that each pair of elements of $\mathcal{S}(\mathcal{D}, U, W)$ intersect trivially.

Counting the number of elements of $\mathcal{S}(\mathcal{D}, U, W)$, taking into account the previous remark that any subspace of Λ_2 which is skew to Σ_2 intersects A in at most one point, we obtain q^{sn} different elements of $\mathcal{S}(\mathcal{D}, U, W)$, induced by elements of $\mathcal{D}_1$ that intersect $L'\backslash L$. Since for each element $R \in \mathcal{D}_1$, intersecting L, we have that $\langle R, W\rangle/W = \Sigma_1/W$, we conclude that the set $\mathcal{S}(\mathcal{D}, U, W)$ consists of $q^{ns} + 1$ skew $(n-1)$-spaces. In other words $\mathcal{S}(\mathcal{D}, U, W)$ is an $(n-1)$-spread of $\Lambda_1/W \cong \mathrm{PG}(2n-1, q^s)$.

Let S_∞ denote the element $\Sigma_1/W \in \mathcal{S}(\mathcal{D}, U, W)$. To finish the proof we still need to show that $\mathcal{S}(\mathcal{D}, U, W)$ is a semifield spread, i.e., that there is a subgroup $G \leq \mathrm{P\Gamma L}(2n, q^s)$, fixing S_∞ pointwise such that G acts transitively on the other elements of $\mathcal{S}(\mathcal{D}, U, W)$.

Note that each element of $\mathcal{D}_1$ induces an $(ns-1)$-space in Λ_2, which is partitioned by elements of $\mathcal{D}_2$. Denote the set of these $(ns-1)$-spaces induced by the elements of

$\mathcal{D}_1$, by $\mathcal{D}_3$. Since $\mathcal{D}_1$ is a Desarguesian $(n-1)$-spread of Λ_1, it follows that $\mathcal{D}_3$ is a Desarguesian $(ns-1)$-spread of Λ_2. Again, note that each element of $\mathcal{D}_3$ intersects U' in at most one point, and hence also each element of $\mathcal{D}_1$ intersects $B_{\mathcal{D}_2}(U')$ in at most one point. Let H denote the stabiliser of $\mathcal{D}_1$ in $\mathrm{P\Gamma L}(\Lambda_1)$, and note that H contains a subgroup isomorphic to $\mathrm{P\Gamma L}(r+1, q^{ns})$. Take any two elements X and Y in $B_{\mathcal{D}_1}(B_{\mathcal{D}_2}(U')) \subset \mathcal{D}_1$, and suppose that $X \cap B_{\mathcal{D}_2}(U') = \langle x \rangle$ and $Y \cap B_{\mathcal{D}_2}(U') = \langle y \rangle$, with $x, y \in \mathbb{F}_{q^s}^{rn+n} \setminus \mathbb{F}_{q^s}^{rn}$. Let ψ be an isomorphism

$$\psi : \mathbb{F}_{q^s}^{rn+n} \to \mathbb{F}_{q^{sn}}^{r+1}$$

such that

$$(\mathbb{F}_{q^s}^{rn})^\psi = \mathbb{F}_{q^{ns}}^{r}.$$

Since the pointwise stabiliser H' of $\mathbb{F}_{q^{ns}}^{r}$ in $\Gamma\mathrm{L}(r+1, q^{ns})$ acts transitively on the vectors of $\mathbb{F}_{q^{ns}}^{r+1} \setminus \mathbb{F}_{q^{ns}}^{r}$, it follows that H' contains an element φ_{xy} such that $(x^\psi)^{\varphi_{xy}} = y^\psi$, and since X and Y were arbitrary, it follows that the group H' acts transitively on $\{x^\psi : \langle x \rangle \in B_{\mathcal{D}_2}(U') \setminus B_{\mathcal{D}_2}(U)\}$. This implies that the group $\psi^{-1}H'\psi$ induces a subgroup of H, fixing Σ_1 pointwise, that acts transitively on the elements of $B_{\mathcal{D}_1}(B_{\mathcal{D}_2}(U'))$. Finally, in the quotient geometry Λ_1/W, this group induces a subgroup G of order q^{ns} fixing S_∞ pointwise such that G acts transitively on the other elements of $\mathcal{S}(\mathcal{D}, U, W)$. □

We denote by $\mathbb{S}(\mathcal{D}, U, W)$ the semifield corresponding to the semifield spread $\mathcal{S}(\mathcal{D}, U, W)$. The following theorem characterises those linear sets that correspond to a finite field.

Theorem 3.2. *If $(\mathcal{D}, U, W)$ is a BEL-configuration where L is an element of $\mathcal{D}$, then $\mathcal{S}(\mathcal{D}, U, W)$ is a Desarguesian spread and $\mathbb{S}(\mathcal{D}, U, W)$ is a finite field.*

Proof. Applying the BEL-construction to $(\mathcal{D}, U, W)$ we see that $B_{\mathcal{D}_1}(L')$ is contained in the $(2k-1)$-dimensional subspace spanned by two elements L and R of $\mathcal{D}_1$, with R an element of $B_{\mathcal{D}_1}(L' \setminus L)$. Since the restriction of a Desarguesian spread to any subspace spanned by some of its elements is again a Desarguesian spread, it follows that $B_{\mathcal{D}_1}(L')$ is a Desarguesian spread in $\langle R, L \rangle$. The projection of Λ_1 from W onto $\langle R, L \rangle$ gives a Desarguesian spread in the quotient geometry Λ_1/W. The semifield corresponding to a Desarguesian spread is a field. □

Remark 3.3. As in [2, Remark 2.3] one shows that the semifield $\mathbb{S}(\mathcal{D}, U, W)$ is independent of the choice of U' in the construction.

4 The BEL-construction for semifields with given left nucleus

In this section we give an explicit description of a BEL-configuration for a semifield with given multiplication. This BEL-configuration is different from the one in [2], depending on the size of the left nucleus. If the left nucleus is larger than the center, then the dimension of the ambient space of the BEL-configuration given here is much smaller compared to [2]. We remark that the same construction can be done with respect to the right nucleus.

Since a semifield is a vector space over each of its nuclei, the size of a nucleus is q^s, with s a divisor of n. In general, if we label the elements of $\mathbb{S}$ by the elements of $\mathbb{F}_{q^n}$, then the multiplication of a semifield $\mathbb{S}$, with center $\mathbb{F}_q$ can be written as

$$y \circ x = \sum_{i,j=0}^{n-1} d_{ij} x^{q^i} y^{q^j},$$

with $d_{ij} \in \mathbb{F}_{q^n}$.

In the following theorem we denote the points of $\mathrm{PG}(k^2-1, q^s)$ as $\langle (x_0, x_1, \ldots, x_{k-1}) \rangle$ with $x_i \in \mathbb{F}_{q^n}$, $n = ks$. With this notation, the set

$$\mathcal{D} = \left\{ \left\{ \langle (ax_0, ax_1, \ldots, ax_{k-1}) \rangle : a \in \mathbb{F}_{q^n}^* \right\} : \overline{x} \in \mathbb{F}_{q^n}^k \setminus \{0\} \right\},$$

is a Desarguesian $(k-1)$-spread of $\mathrm{PG}(k^2-1, q^s)$.

Theorem 4.1. *For every finite semifield $\mathbb{S}$ of order q^n with left nucleus $|\mathbb{N}_l| = q^s$, $sk = n$, there exists a BEL-configuration $(\mathcal{D}, U, W)$ in $\mathrm{PG}(k^2-1, q^s)$, such that $\mathbb{S} = \mathbb{S}(\mathcal{D}, U, W)$.*

Proof. Let $\mathbb{S}$ be a semifield of order q^n with multiplication given by

$$y \circ x = \sum_{i,j=0}^{n-1} d_{ij} x^{q^i} y^{q^j},$$

with $d_{ij} \in \mathbb{F}_{q^n}$. Suppose $\mathbb{S}$ has a left nucleus of size q^s, $s = n/k$, and relabel the elements of $\mathbb{S}$, such that $\mathbb{N}_l = \mathbb{F}_{q^s} \subset \mathbb{F}_{q^n}$, and the center is $\mathbb{F}_q$. Since $(l \circ y) \circ x = l \circ (y \circ x)$, for all $l \in \mathbb{N}_l$, it follows that the map $R_x : y \mapsto y \circ x$ is linear over $\mathbb{F}_{q^s}$, and hence the multiplication in $\mathbb{S}$ may be written as

$$y \circ x = \sum_{i=0}^{n-1} \sum_{j=0}^{k-1} c_{ij} x^{q^i} y^{q^{sj}},$$

with $c_{ij} \in \mathbb{F}_{q^n}$. Define the subspace

$$\mathcal{W} = \left\{ \left\langle \left(-\sum_{i=1}^{k-1} z_i^{q^{is}}, z_1, z_2, \ldots, z_{k-1} \right) \right\rangle : \overline{z} \in \mathbb{F}_{q^n}^{k-1} \setminus \{0\} \right\} \tag{7}$$

and the Desarguesian $(k-1)$-spread

$$\mathcal{D} = \left\{ \left\{ \langle (ax_0, ax_1, \ldots, ax_{k-1}) \rangle : a \in \mathbb{F}_{q^n}^* \right\} : \overline{x} \in \mathbb{F}_{q^n}^k \setminus \{0\} \right\} \tag{8}$$

in $\mathrm{PG}(k^2-1, q^s)$. First we show that the triple $(\mathcal{D}, U, \mathcal{W})$ where the $\mathbb{F}_q$-linear set $L = B(U)$ is given by

$$L = \left\{ \left\langle \left(c_0(x), c_1(x)^{1/q^s}, \ldots, c_{k-1}(x)^{1/q^{s(k-1)}} \right) \right\rangle : x \in \mathbb{F}_{q^n}^* \right\},$$

and $c_j(x) = \sum_{i=0}^{n-1} c_{ij} x^{q^i}$ is a BEL-configuration in $\mathrm{PG}(k^2-1, q^s)$. If there is an element of $\mathcal{D}$ intersecting both L and $\mathcal{W}$ then there exist $\overline{z} \in \mathbb{F}_{q^n}^{k-1} \setminus \{0\}$, $y \in \mathbb{F}_{q^n}^*$, and $x \in \mathbb{F}_{q^n}^*$ such that

$$z_j = y c_j(x)^{1/q^{sj}}, j \neq 0$$

and

$$-\sum_{j=1}^{k-1} z_j^{q^{js}} = y c_0(x).$$

Substituting the z_j in the second equation we get

$$y \circ x = \sum_{i=0}^{n-1} \sum_{j=0}^{k-1} c_{ij} x^{q^i} y^{q^{sj}} = 0,$$

which implies $x = 0$ or $y = 0$, a contradiction. This shows that the triple $(\mathcal{D}, U, \mathcal{W})$ is a BEL-configuration. Now extend the $\mathbb{F}_q$-linear set L to the $\mathbb{F}_q$-linear set

$$L' := \left\{ \left\langle \left(t, c_0(x), c_1(x)^{1/q^s}, \ldots, c_{k-1}(x)^{1/q^{s(k-1)}}\right) \right\rangle : (t, x) \in (\mathbb{F}_q \times \mathbb{F}_{q^n}) \setminus \{(0,0)\} \right\},$$

in $\mathrm{PG}(k^2 + k - 1, q^s)$. The element of $\mathcal{D}$ containing the point

$$\left\langle \left(t, c_0(x), c_1(x)^{1/q^s}, \ldots, c_{k-1}(x)^{1/q^{s(k-1)}}\right) \right\rangle$$

is

$$D_x := \left\{ \left\langle \left(y, y c_0(x), y c_1(x)^{1/q^s}, \ldots, y c_{k-1}(x)^{1/q^{s(k-1)}}\right) \right\rangle : y \in \mathbb{F}_{q^n}^* \right\}.$$

Calculating the quotient space $\langle D_x, \mathcal{W} \rangle / \mathcal{W}$ as a projection from $\mathcal{W}$ onto the subspace with the last $k-2$ coordinates equal to zero, we obtain

$$\langle D_x, \mathcal{W} \rangle =$$
$$\left\{ \left\langle \left(y, y c_0(x) - \sum_{i=1}^{k-1} z_i^{q^{is}}, y c_1(x)^{1/q^s} + z_1, \ldots, y c_{k-1}(x)^{1/q^{s(k-1)}} + z_{k-1} \right) \right\rangle : \right.$$
$$\left. y \in \mathbb{F}_{q^n}^*, \overline{z} \in \mathbb{F}_{q^n}^{k-1} \setminus \{0\} \right\}$$

and hence

$$\langle D_x, \mathcal{W} \rangle / \mathcal{W} = \left\{ \left\langle \left(y, \sum_{j=0}^{k-1} c_j(x) y^{q^{sj}} \right) \right\rangle : y \in \mathbb{F}_{q^n}^* \right\}$$

Thus the semifield spread $\mathcal{S}(\mathcal{D}, U, \mathcal{W})$ corresponds to a semifield with multiplication $y \circ x = \sum_{j=0}^{k-1} c_j(x) y^{q^{sj}}$, i.e., the semifield $\mathbb{S} = \mathbb{S}(\mathcal{D}, L, \mathcal{W})$. □

5 On the isotopism problem

Recall that the set of semifields isotopic to a given semifield $\mathbb{S}$ is called the *isotopism class* of $\mathbb{S}$ and is denoted by $[\mathbb{S}]$. It is not difficult to see that the sizes of the nuclei of a semifield $\mathbb{S}$ are invariants of $[\mathbb{S}]$ and hence it makes sense to speak of the *size of the nuclei of an isotopism class* $[\mathbb{S}]$. Generally one is interested in the isotopism classes of semifields, since these correspond to the isomorphism classes of the corresponding projective planes (see Albert [1]). But Knuth proved that the action of S_3 is well defined on the set of isotopism classes and we call the set of isotopism classes of semifields corresponding to the S_3-orbit the *Knuth orbit*. So instead of looking at the isotopism classes of finite semifields we might also consider the Knuth orbits of finite semifields. In general the size of the Knuth orbit is not immediately clear. However, it is straightforward to see that the Knuth orbit of a finite field has size one. The size of the Knuth orbit is also known for the semifields studied in [3], but for most other semifields its size is not known. One of the issues of the isotopism problem is not having a "canonical" representative for an isotopism class (see e.g. [6]), and the same holds for the representation of a Knuth orbit. However what concerns the Knuth orbit, we know that the sizes of the nuclei are permuted under the action of S_3. Hence, as a representative of a Knuth orbit, we may always take a semifield whose isotopism class has our favourite nucleus as its largest nucleus. In what follows we will assume this largest nucleus to be the left nucleus, but the reader should keep in mind that this is just a matter of choice.

So, we distinguish the isotopy classes of semifields of order q^n by the size of the largest nucleus, and using the action of S_3 on the indices of the structure constants, we may assume that the representative of the Knuth orbit of $\mathbb{S}$ has as largest nucleus the left nucleus, which we denote by $\mathbb{N}_l$. The isotopism classes of semifields of order q^n which have the right or middle nucleus as largest nucleus are then obtained by permuting the indices of the structure constants of the semifield. The following theorem solves the isotopism problem for semifields $\mathbb{S}(\mathcal{D}, L, \mathcal{W})$, with $\mathcal{W}$ defined by (7).

Theorem 5.1. *Two semifields $\mathbb{S}(\mathcal{D}, U_1, \mathcal{W})$ and $\mathbb{S}(\mathcal{D}, U_2, \mathcal{W})$ of order q^n and left nucleus of size q^s, $n = sk$, with $\mathcal{W}$ defined by (7), are isotopic if and only if there exists a collineation φ of $\mathrm{PG}(k^2-1, q^s)$ fixing $B(\mathcal{W})$ with $B(U_1)^\varphi = B(U_2)$.*

Proof. Suppose $\mathbb{S}(\mathcal{D}, U_1, \mathcal{W})$ and $\mathbb{S}(\mathcal{D}, U_2, \mathcal{W})$, with $\mathcal{W}$ defined by (7), are isotopic semifields with multiplication given by

$$y \circ x = \sum_{i=0}^{n-1}\sum_{j=0}^{k-1} c_{ij} x^{q^i} y^{q^{sj}} = \sum_{j=0}^{k-1} c_j(x) y^{q^{sj}} \qquad \text{and}$$

$$y \circ' x = \sum_{i=0}^{n-1}\sum_{j=0}^{k-1} c'_{ij} x^{q^i} y^{q^{sj}} = \sum_{j=0}^{k-1} c'_j(x) y^{q^{sj}}.$$

The spreads of $\mathrm{PG}(2k-1, q^s)$, $\mathcal{S}$ and $\mathcal{S}'$, corresponding to $\mathbb{S}$ and $\mathbb{S}'$, consist of the

subspace $S_\infty = S'_\infty = \{(0,y) : y \in \mathbb{F}_{q^n}^*\}$, together with the subspaces

$$S_x = \{(y, y \circ x) : y \in \mathbb{F}_{q^n}^*\}, \quad x \in \mathbb{F}_{q^n}, \qquad \text{and}$$
$$S'_x = \{(y, y \circ' x) : y \in \mathbb{F}_{q^n}^*\}, \quad x \in \mathbb{F}_{q^n},$$

respectively. The corresponding $\mathbb{F}_q$-linear sets L_1 and L_2 in $\mathrm{PG}(k^2-1, q^s)$, as in the proof of Theorem 4.1 are given by

$$L_1 = \{\langle (c_0(x), c_1(x)^{1/q^s}, \ldots, c_{k-1}(x)^{1/q^{s(k-1)}}) \rangle : x \in \mathbb{F}_{q^n}^*\}, \qquad \text{and}$$
$$L_2 = \{\langle (c'_0(x), c'_1(x)^{1/q^s}, \ldots, c'_{k-1}(x)^{1/q^{s(k-1)}}) \rangle : x \in \mathbb{F}_{q^n}^*\},$$

respectively. As in the proof of [7, Theorem 17], we use the collineation Ψ between $\mathrm{PG}(k^2-1,q^s)$ and $\mathrm{PG}(M_k(\mathbb{F}_{q^s}))$ induced by the isomorphism between $V(k^2,q^s)$ and $M_k(\mathbb{F}_{q^s})$ defined by

$$(x_0, x_1, \ldots, x_{k-1}) \mapsto U^{-1} A_{(x_0, x_1^{q^s}, \ldots, x_{k-1}^{q^{sk-1}})} U,$$

with

$$U := \begin{pmatrix} u_0 & u_1 & \ldots & u_{k-1} \\ u_0^{q^s} & u_1^{q^s} & \ldots & u_{k-1}^{q^s} \\ \vdots & \vdots & & \vdots \\ u_0^{q^{sk-1}} & u_1^{q^{sk-1}} & \ldots & u_{k-1}^{q^{sk-1}} \end{pmatrix}, \qquad \text{and}$$

$$A_{(y_0,y_1,\ldots,y_{k-1})} := \begin{pmatrix} y_0 & y_1 & \ldots & y_{k-1} \\ y_{k-1}^{q^s} & y_0^{q^s} & \ldots & y_{k-2}^{q^s} \\ \vdots & \vdots & & \vdots \\ y_1^{q^{sk-1}} & y_2^{q^{sk-1}} & \ldots & y_0^{q^{sk-1}} \end{pmatrix}.$$

To conclude the proof, apply exactly the same reasoning as in the proof of [7, Theorem 17]. □

The following theorem is a refinement of two results proved in [7] and links the set of points of $B_{\mathcal{D}}(\mathcal{W})$ to the Segre variety $\mathcal{S}_{k,k}(q^s)$.

Theorem 5.2. *The set of points $B_{\mathcal{D}}(\mathcal{W})$ with $\mathcal{D}$ and $\mathcal{W}$ as in (8) and (7), respectively, is projectively equivalent to the set of points of the $(k-2)$-th secant variety to a Segre variety $\mathcal{S}_{k,k}(q^s)$ in $\mathrm{PG}(k^2-1,q^s)$, and the elements of $B_{\mathcal{D}}(\mathcal{W})$ contain a subset that is projectively equivalent to one of the two families of maximal subspaces contained in $\mathcal{S}_{k,k}(q^s)$.*

Proof. The first part of the statement is [7, Theorem 11]. Let Ψ denote the associated collineation, i.e. $B_{\mathcal{D}}(\mathcal{W})^\Psi$ covers the $(k-2)$-th secant variety to a Segre variety $\mathcal{S}_{k,k}(q^s)$ in $\mathrm{PG}(k^2-1,q^s)$. Let $\mathcal{F}_1$ and $\mathcal{F}_2$ denote the two families of maximal subspaces contained

in $\mathcal{S}_{k,k}(q^s)$. It follows from the proof of [7, Corollary 12] that a $(k-1)$-space R^Ψ with $R \in B_\mathcal{D}(\mathcal{W})$ is either contained in $\mathcal{S}_{k,k}(q^s)$ or is skew to $\mathcal{S}_{k,k}(q^s)$. Since $B_\mathcal{D}(\mathcal{W})^\Psi$ consists of $(k-1)$-dimensional subspaces and each two elements of $B_\mathcal{D}(\mathcal{W})^\Psi$ are skew, $B_\mathcal{D}(\mathcal{W})^\Psi$ contains a subset that coincides with one of the two families $\mathcal{F}_1$ or $\mathcal{F}_2$. □

We denote the subgroup of $\mathrm{P\Gamma L}(k^2, q^s)$ fixing both families of maximal subspaces contained in $\mathcal{S}_{k,k}(q^s)$ by $H(\mathcal{S}_{k,k}(q^s))$. The above link between the set of points of $B_\mathcal{D}(\mathcal{W})$ to the Segre variety $\mathcal{S}_{k,k}(q^s)$ gives the equivalence between the algebraic and geometric approach to the isotopism problem for finite semifields. In case the semifield is symplectic, the Segre variety in this equivalence becomes a Veronesean variety, because of the extra symmetry; for more on the symplectic case we refer to [9].

Corollary 5.3. *There is a one-to-one correspondence between the isotopism classes of finite semifields of order q^n, with center $\mathbb{F}_q$ and left nucleus of order q^s, $n = ks$, and the orbits of the action of $H(\mathcal{S}_{k,k}(q^s))$ on the $\mathbb{F}_q$-linear sets of rank n in $\mathrm{PG}(k^2-1, q^s)$ skew to the $(k-2)$-th secant variety $\Omega_{k-2}(q^s)$ of $\mathcal{S}_{k,k}(q^s)$.*

Proof. Combine Theorem 5.1 and Theorem 5.2. □

As an application of the BEL-construction we have the following characterisation of the isotopism class of a finite field.

Theorem 5.4. *The $H(\mathcal{S}_{k,k}(q^s))$-orbit, corresponding to the isotopism class of a finite field, is the orbit of a $(k-1)$-dimensional subspace, skew to the $(k-2)$-th secant variety $\Omega_{k-2}(q^s)$ of $\mathcal{S}_{k,k}(q^s)$, that belongs to a Desarguesian spread, containing one of the two families of maximal subspaces of $\mathcal{S}_{k,k}(q^s)$.*

Proof. Let $L = B(U)$ be a $(k-1)$-dimensional subspace belonging to the Desarguesian spread $\mathcal{D}$ containing one of the two families of maximal subspaces of $\mathcal{S}_{k,k}(q^s)$, and let W be any (k^2-k-1)-dimensional subspace contained in the $(k-2)$-th secant variety to a Segre variety $\mathcal{S}_{k,k}(q^s)$. This subspace exists because of Theorem 5.2. Then $(\mathcal{D}, U, W)$ is a BEL-configuration with $B(U) \in \mathcal{D}$. It follows from Theorem 3.2 that $\mathbb{S}(\mathcal{D}, U, W)$ is a field. □

References

[1] A. A. Albert, Finite division algebras and finite planes. In: *Proc. Sympos. Appl. Math., Vol. 10*, 53–70, Amer. Math. Soc. 1960. MR0116036 (22 #6831) Zbl 0096.15003

[2] S. Ball, G. Ebert, M. Lavrauw, A geometric construction of finite semifields. *J. Algebra* **311** (2007), 117–129. MR2309880 (2008d:51001) Zbl 1125.12002

[3] S. Ball, M. Lavrauw, On the Hughes-Kleinfeld and Knuth's semifields two-dimensional over a weak nucleus. *Des. Codes Cryptogr.* **44** (2007), 63–67. MR2336394 (2008g:12007) Zbl 1123.51009

[4] I. Cardinali, O. Polverino, R. Trombetti, Semifield planes of order q^4 with kernel F_{q^2} and center F_q. *European J. Combin.* **27** (2006), 940–961. MR2226429 (2007c:51010) Zbl 1108.51010

[5] L. E. Dickson, Linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc.* **7** (1906), 370–390. MR1500755 Zbl 37.0111.06

[6] D. E. Knuth, Finite semifields and projective planes. *J. Algebra* **2** (1965), 182–217. MR0175942 (31 #218) Zbl 0128.25604

[7] M. Lavrauw, On the isotopism classes of finite semifields. *Finite Fields Appl.* **14** (2008), 897–910. MR2457536 (2009k:12006) Zbl 1167.51005

[8] G. Lunardon, Normal spreads. *Geom. Dedicata* **75** (1999), 245–261. MR1689271 (2000i:51033) Zbl 0944.51004

[9] G. Lunardon, G. Marino, O. Polverino, R. Trombetti, Symplectic spreads and quadric Veronesean. Preprint.

[10] G. Marino, O. Polverino, R. Trombetti, On $\mathbb{F}_q$-linear sets of $\mathrm{PG}(3, q^3)$ and semifields. *J. Combin. Theory Ser. A* **114** (2007), 769–788. MR2333132 (2008f:51017) Zbl 1118.51006

[11] O. Polverino, Linear sets in finite projective spaces. *Discrete Math.* **310** (2010), 3096–3107. MR2684078 Zbl pre05807480

Received 3 April, 2009

M. Lavrauw, Department of Pure Mathematics and Computer Algebra, Ghent University, Building S22, Krijgslaan 281, 9000 Gent, Belgium
Email: ml@cage.ugent.be