Available online at www.sciencedirect.com
ScienceDirect
Finite Fields and Their Applications 14 (2008) 897–910
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

On the isotopism classes of finite semifields

Michel Lavrauw

Ghent University, Department of Pure Mathematics and Computer Algebra, Krijgslaan 281, 9000 Ghent, Belgium

Received 30 January 2008; revised 8 May 2008

Available online 4 June 2008

Communicated by Gary L. Mullen

Abstract

A projective plane is called a translation plane if there exists a line L such that the group of elations with axis L acts transitively on the points not on L. A translation plane whose dual plane is also a translation plane is called a *semifield plane*. The ternary ring corresponding to a semifield plane can be made into a non-associative algebra called a *semifield*, and two semifield planes are isomorphic if and only if the corresponding semifields are *isotopic*. In [S. Ball, G. Ebert, M. Lavrauw, A geometric construction of finite semifields, J. Algebra 311 (1) (2007) 117–129] it was shown that each finite semifield gives rise to a particular configuration of two subspaces with respect to a Desarguesian spread, called a *BEL-configuration*, and vice versa that each BEL-configuration gives rise to a semifield. In this manuscript we investigate the question when two BEL-configurations determine isotopic semifields. We show that there is a one-to-one correspondence between the isotopism classes of finite semifields and the orbits of the action a subgroup of index two of the automorphism group of a Segre variety on subspaces of maximum dimension skew to a determinantal hypersurface.

Keywords: Projective planes; Finite semifields; Segre variety; Determinantal hypersurface; Spreads

1. Introduction and preliminaries

By results of Hilbert [9] and Hall [8], it is well known that to each frame of a projective plane there corresponds a ternary ring, obtained by coordinationisation. If the projective plane is non-Desarguesian and both a translation plane and a dual translation plane, then the ternary ring, associated to a frame which shares two points with the translation line, becomes a non-

E-mail address: ml@cage.ugent.be.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2008.05.002

associative algebra, called a *semifield*. In the earlier literature (predating 1965) these algebras were also called *division algebras* or *distributive quasifields*. The study of semifields was initiated about a century ago by Dickson [6], shortly after the classification of finite fields, taking a purely algebraic point of view. By now, the theory of semifields has become of considerable interest in many different areas of mathematics. Besides the numerous links with finite geometry (e.g. translation planes, generalised quadrangles, ...), semifields arise in the context of difference sets, coding theory and group theory. In this paper we will only consider finite structures.

A *finite semifield* $\mathbb{S}$ 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 $x \in \mathbb{S}$.

A finite field is a trivial example of a semifield. The first non-trivial examples were constructed by Dickson in [6]. 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 $\mathbb{S}$. Non-isomorphic semifields can coordinatise isomorphic planes. Albert [1] proved that two semifields coordinatise isomorphic planes if and only if there exists three maps (t_1, t_2, t_3), linear over some subfield of the semifields, that map elements of $\mathbb{S}_1$ to $\mathbb{S}_2$ and that satisfy, for all $x, y \in \mathbb{S}_1$,

$$t_1(x) \circ t_2(x) = t_3(x \cdot y),$$

where $\cdot$ is multiplication in $\mathbb{S}_1$ and $\circ$ is multiplication in $\mathbb{S}_2$. If such maps exist then we say that the semifields $\mathbb{S}_1$ and $\mathbb{S}_2$ are *isotopic*. For further definitions of the *nucleus*, the *left*, *middle*, and *right nucleus* of $\mathbb{S}$, etc., we refer to the excellent paper [16] (or [5, Chapter 5], [11, Chapter 8]). For an overview of the known semifields and the number of semifields of a given order up to isotopism, we refer to [14] or [12]. Recently many new semifields have been constructed, see e.g. [15,13,7,19].

In [3] a geometric construction method was given for semifields, starting from a particular configuration of subspaces in a vector space, and it was shown that all semifields can be constructed that way. One of the remarks in that paper [3, Remark 4.4] points out the problem of determining whether two such configurations give isotopic semifields or not (except when the semifield is two-dimensional over its left nucleus, in which case the BEL-configuration can be reduced to a subgeometry skew to a hyperbolic quadric [3, Final Remarks], and then the question is answered by [4, Theorem 2.1]). In other words, when considering the isotopism classes of finite semifields (or equivalently, the isomorphism classes of semifield planes), it was not clear how to determine the set of configurations corresponding to that isotopism class. We settle this question by showing that there is a one-to-one correspondence between the isotopism classes of finite semifields and the orbits of the action of a subgroup of index two of the automorphism group of a determinantal hypersurface on subspaces of maximum dimension skew to that hypersurface.

The details of the construction for finite semifields given in [3] will be recalled in Section 3. In Section 2 we establish the necessary connections between determinantal hypersurfaces, Segre varieties and Desarguesian spreads, with some interesting corollaries, in order to prove the crucial Theorem 11. Finally, in Section 4 we prove the main theorem.

We end this section with a few definitions and some notation that will be used throughout the paper.

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 of a vector space, 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 $\mathrm{PG}(d-1,q)$).

A *spread* of $V=V(d,q)$ is a set $\mathcal{S}$ of subspaces of V, all of the same dimension d', $1\leqslant d'\leqslant d$, 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]). 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 (see [5]).

Assume $n\geqslant 2$, consider $V(d,q^n)$ as a vector space $V(dn,q)$ of dimension dn over $\mathbb{F}_q$ and consider the spread of subspaces of dimension n over $\mathbb{F}_q$ in $V(dn,q)$ arising from the spread of subspaces of dimension 1 over $\mathbb{F}_{q^n}$ in $V(d,q^n)$. 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.

It should be clear to the reader that 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.

2. Higher secant varieties to Segre varieties and Desarguesian spreads

Let V_2 denote the n^2-dimensional vector space of $(n\times n)$-matrices ($n\geqslant 2$) over $\mathbb{F}_q$, and consider the set $\mathcal{S}_{n,n}$ of points in $\mathrm{PG}(V_2)$ corresponding to all the $(n\times n)$-matrices of rank one. The set $\mathcal{S}_{n,n}$ is called the *Segre variety*, see e.g. [10, Theorem 25.5.7]. The study of these varieties dates back (at least) to Segre (1891) [21], where a completely different and more general definition was given (using coordinates) (see also [10]). For our purposes the above definition suffices. Let us summarize a few well-known facts, restricted to $\mathcal{S}_{n,n}$. The proofs can be found in [10].

Theorem 1. *The Segre variety $\mathcal{S}_{n,n}$ is the intersection of quadrics of* $\mathrm{PG}(n^2-1,q)$.

Theorem 2. *There are two systems Σ_1 and Σ_2 of maximal subspaces contained in $\mathcal{S}_{n,n}$, and each point of $\mathcal{S}_{n,n}$ is contained in exactly one element of each Σ_i. Also, each element of Σ_1 has exactly one point in common with each element of Σ_2, the elements of Σ_i have dimension $n-1$, and each subspace contained in $\mathcal{S}_{n,n}$ of dimension $s>0$ is contained in a unique element of $\Sigma_1\cup\Sigma_2$.*

Theorem 3. *The subgroup $H(\mathcal{S}_{n,n})$ of* $\mathrm{PGL}(n^2,q)$ *fixing both systems Σ_1 and Σ_2 of $\mathcal{S}_{n,n}$ is isomorphic to* $\mathrm{PGL}(n,q)\times\mathrm{PGL}(n,q)$. *If $G(\mathcal{S}_{n,n})$ denotes the subgroup of* $\mathrm{PGL}(n^2,q)$ *fixing $\mathcal{S}_{n,n}$, then $H(\mathcal{S}_{n,n})$ has index two in $G(\mathcal{S}_{n,n})$.*

The set of points of $\mathrm{PG}(V_2)$ that are contained in a line generated by points of $\mathcal{S}_{n,n}$ is called the *secant variety* Ω_1 of $\mathcal{S}_{n,n}$, and corresponds to the matrices of rank at most two. Similarly, one defines the *kth secant variety* Ω_k for all $1 \leqslant k \leqslant n-1$ corresponding to matrices of rank at most $k+1$. In this way the $(n-1)$th secant variety of $\mathcal{S}_{n,n}$ consists of all the points of $\mathrm{PG}(V_2)$, while the $(n-2)$th secant variety corresponds to the singular matrices, i.e., Ω_{n-2} is *the determinantal hypersurface* in $\mathrm{PG}(V_2)$. Also note that $\Omega_0 = \mathcal{S}_{n,n}$.

Theorem 4. *The points of the Segre variety are the points of a determinantal hypersurface in* $\mathrm{PG}(V_2)$ *with multiplicity* $n-1$.

Proof. If $n=2$, then the theorem states that the Segre variety in $\mathrm{PG}(3,q)$ has no singular points, which is well known, since it is a non-singular hyperbolic quadric in $\mathrm{PG}(3,q)$. Assume $n \geqslant 3$. The points of Ω_{n-2} are the points of the algebraic variety $\mathcal{V}(F(X_0,\ldots,X_{n^2-1}))$, with

$$F(X_0,\ldots,X_{n^2-1}) := \det \begin{pmatrix} X_0 & X_1 & \cdots & X_{n-1} \\ X_n & X_{n+1} & \cdots & X_{2n-1} \\ \vdots & \vdots & \vdots & \\ X_{n^2-n} & X_{n^2-n+1} & \cdots & X_{n^2-1} \end{pmatrix}.$$

The singular points of Ω_{n-2} are those points that vanish on all partial derivatives $\partial F/\partial X_i$, $i = 0,\ldots,n^2-1$. Denote the above matrix by $\mathbf{X}$. In order to calculate the derivatives $\partial F/\partial X_i$, $i=0,\ldots,n^2-1$, we use Jacobi's formula for the differential of the determinant

$$\frac{\partial F}{\partial X_i} = \frac{\partial \det \mathbf{X}}{\partial X_i} = (\det \mathbf{X})\,\mathrm{trace}\left(\mathbf{X}^{-1}\frac{\partial \mathbf{X}}{\partial X_i}\right).$$

Since $\partial \mathbf{X}/\partial X_i$ is the matrix with a zero in every entry except on the $(\lfloor i/n \rfloor + 1)$th row and the $((i \bmod n)+1)$th column (where the entry is one), we obtain

$$\frac{\partial F}{\partial X_i} = (\det \mathbf{X})\big(\mathbf{X}^{-1}\big)_{kl} = (-1)^{k+l}\mathbf{X}_{lk},$$

where $k := i \pmod n + 1$, and $l := \lfloor i/n \rfloor + 1$, and $\mathbf{X}_{lk}$ denotes the lkth minor of $\mathbf{X}$. Since

$$\big\{\big(i \pmod n + 1,\, \lfloor i/n \rfloor + 1\big)\colon\, i \in \big\{0,1,\ldots,n^2-1\big\}\big\} = \{1,\ldots,n\}^2,$$

it follows that the set of singular points of Ω_{n-2} is the set of points contained in each of the hypersurfaces $\mathcal{V}(\mathbf{X}_{ij})$, $1 \leqslant i,j \leqslant n$. By definition this set of points equals Ω_{n-3}. In the same way one easily verifies that the singular points of Ω_{n-3} (if $n \geqslant 4$) correspond to the $(n \times n)$-matrices with all $(n-2)\times(n-2)$ minors equal to zero, which proves that the points of Ω_{n-4} are the singular points of Ω_{n-3}, and the double points of Ω_{n-2}. Continuing this process we may conclude that the points of Ω_0, i.e., the Segre variety $\mathcal{S}_{n,n}$, are the points of Ω_{n-2} with multiplicity $n-1$. □

The following corollary is an easy consequence from the last part of the proof of Theorem 4.

Corollary 5. *The points of the kth secant variety* Ω_k *of the Segre variety are the points of a determinantal hypersurface* Ω_{n-2} *with multiplicity* $n-k$.

Corollary 6. *Each secant variety Ω_{k-1}, $2 \leqslant k \leqslant n$, has the same automorphism group in* $\mathrm{P\Gamma L}(n^2, q)$*, namely, the automorphism group of the Segre variety $\mathcal{S}_{n,n}$.*

Proof. Denote the subgroup of $\mathrm{P\Gamma L}(n^2, q)$ fixing a set of points U by $\mathrm{Aut}(U)$. That each automorphism of Ω_{k-1}, $1 \leqslant k \leqslant n$, induces an automorphism of the Segre variety Ω_0 follows from Theorem 4 and the fact that an automorphism of an algebraic variety leaves invariant the set of points on that variety with given multiplicity. Hence we have a well-defined morphism

$$\rho : \mathrm{Aut}(\Omega_{k-1}) \to \mathrm{Aut}(\Omega_0).$$

That ρ is an epimorphism can be seen geometrically, since each point P on Ω_{k-1} is contained in the subspace spanned by k points $P_1, \ldots, P_k$ of Ω_0. This geometric interpretation also implies that the kernel of ρ consists only of the identity. This implies that $\mathrm{Aut}(\Omega_{k-1}) \cong \mathrm{Aut}(\Omega_0)$. $\square$

The following theorem concerns the structure of the secant varieties and the subspaces lying on these varieties.

Theorem 7. *Each secant variety Ω_{k-1}, $2 \leqslant k \leqslant n$, can be partitioned by elements of a Desarguesian spread of* $\mathrm{PG}(V_2)$.

Proof. Consider the tensor product $\mathbb{F}_{q^n} \otimes_q \mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$, and the isomorphism ζ between vectorspaces

$$\zeta : \mathbb{F}_{q^n} \otimes_q \mathbb{F}_{q^n} \to V_2$$
$$v = \sum_{i,j}^{n-1} x_{ij}(v_i \otimes v_j) \mapsto v^\zeta = (x_{ij}), \quad x_{ij} \in \mathbb{F}_q,$$

where $\{v_0, \ldots, v_{n-1}\}$ is some fixed basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. If, for each $v \in \mathbb{F}_{q^n} \otimes_q \mathbb{F}_{q^n}$, we define the following subspace of $\mathbb{F}_{q^n} \otimes_q \mathbb{F}_{q^n}$

$$S_n(v) := \{av \mid a \in \mathbb{F}_{q^n}\},$$

where multiplication by $a \in \mathbb{F}_{q^n}$ is defined by

$$av := \sum_{i,j}^{n-1} x_{ij}\big((av_i) \otimes v_j\big),$$

then it is straightforward (see e.g. [17]) that the set

$$\Sigma := \big\{S_n(v)^\zeta \bigm| v \in \mathbb{F}_{q^n} \otimes_q \mathbb{F}_{q^n}\big\}$$

is a Desarguesian spread of V_2. Since the image under ζ of each two tensors contained in a given element $S_n(v)$ of Σ have the same rank, it follows that the kth secant variety in $\mathrm{PG}(V_2)$ either contains the subspace $\mathrm{PG}(S_n(v)^\zeta)$, or intersects it trivially. Since Σ is a spread, the theorem follows. $\square$

Let V_1 denote the n^2-dimensional vector space of $(\mathbb{F}_{q^n})^n$ over $\mathbb{F}_q$. For any point $P \in \mathrm{PG}(V_1)$ with coordinates $(x_0, x_1, \ldots, x_{n-1})$ define the $(n-1)$-dimensional subspace

$$B(P) := \{(ax_0, ax_1, \ldots, ax_{n-1}):\ a \in \mathbb{F}_{q^n}\}, \tag{1}$$

and extend this notation to any subspace T of $\mathrm{PG}(V_1)$, i.e., put $B(T) := \{B(P):\ P \in T\}$. Define the set

$$\mathcal{D} := \{B(P):\ P \in \mathrm{PG}(V_1)\}. \tag{2}$$

Lemma 8. *The set $\mathcal{D}$ is a Desarguesian spread of* $\mathrm{PG}(V_1)$.

Proof. This is the standard construction of a Desarguesian spread. $\square$

The following lemma provides us with an explicit bijection for the well-known one-to-one correspondence between the set of linear transformations of a vector space $V(n,q)$ (represented as matrices) and the set of q-polynomials over $\mathbb{F}_{q^n}$. For a proof we refer to [20] (or [18, pp. 361–362]).

Lemma 9. *The matrix of the linear transformation induced by the q-polynomial*

$$L(x) := \sum_{i=0}^{n-1} \alpha_i x^{q^i}, \quad \alpha_i \in \mathbb{F}_{q^n},$$

on the n-dimensional vector space $V(n,q)$ over $\mathbb{F}_q$, with respect to the basis $\{u_0, \ldots, u_{n-1}\}$ of $V(n,q)$ is given by

$$M_L := U^{-1} A_\alpha U,$$

where U and A_α are defined by

$$U := \begin{pmatrix} u_0 & u_1 & \cdots & u_{n-1} \\ u_0^q & u_1^q & \cdots & u_{n-1}^q \\ \vdots & \vdots & & \vdots \\ u_0^{q^{n-1}} & u_1^{q^{n-1}} & \cdots & u_{n-1}^{q^{n-1}} \end{pmatrix} \tag{3}$$

and

$$A_\alpha := \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \alpha_{n-1}^q & \alpha_0^q & \cdots & \alpha_{n-2}^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \cdots & \alpha_0^{q^{n-1}} \end{pmatrix} \quad \big(\alpha := (\alpha_0, \ldots, \alpha_{n-1})\big). \tag{4}$$

This allows us to construct the following explicit isomorphism between V_1 and V_2.

Lemma 10. *The map $V_1 \to V_2$ that maps the vector $(x_0, x_1, \ldots, x_{n-1})$ to the matrix $U^{-1}A_{(x_0, x_1^q, \ldots, x_{n-1}^{q^{n-1}})}U$ defines an isomorphism between V_1 and V_2.*

Proof. One easily verifies that

$$U^{-1}A_{(ax_0, (ax_1)^q, \ldots, (ax_{n-1})^{q^{n-1}})}U = aU^{-1}A_{(x_0, x_1^q, \ldots, x_{n-1}^{q^{n-1}})}U,$$

$\forall a \in \mathbb{F}_q$, $\forall x_0, \ldots, x_{n-1} \in \mathbb{F}_{q^n}$, and

$$\begin{aligned} &U^{-1}A_{(x_0, x_1^q, \ldots, x_{n-1}^{q^{n-1}})}U + U^{-1}A_{(y_0, y_1^q, \ldots, y_{n-1}^{q^{n-1}})}U \\ &\quad = U^{-1}A_{(x_0+y_0, (x_1+y_1)^q, \ldots, (x_{n-1}+y_{n-1})^{q^{n-1}})}U, \end{aligned}$$

$\forall x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1} \in \mathbb{F}_{q^n}$. $\square$

The next theorem links the subspace $\mathcal{W}$ used in [3] to the Segre variety.

Theorem 11. *The set of points contained in the spread elements of the Desarguesian spread $\mathcal{D}$ intersecting*

$$\mathcal{W} := \left\{ \left\langle \left(-\sum_{i=1}^{n-1} z_i^{q^i}, z_1, z_2, \ldots, z_{n-1} \right) \right\rangle : z_i \in \mathbb{F}_{q^n} \right\} \subset \mathrm{PG}(V_1) \tag{5}$$

is projectively equivalent to the set of points of the $(n-2)$th secant variety Ω_{n-2} to a Segre variety.

Proof. Consider the collineation Ψ between the corresponding projective spaces

$$\Psi : \mathrm{PG}(V_1) \to \mathrm{PG}(V_2), \tag{6}$$

induced by the isomorphism from Lemma 10

$$V_1 \to V_2: \quad (x_0, x_1, \ldots, x_{n-1}) \mapsto U^{-1}A_\alpha U, \quad \alpha = \left(x_0, x_1^q, \ldots, x_{n-1}^{q^{n-1}}\right).$$

Let $P = \langle (x_0, \ldots, x_{n-1}) \rangle$ be a point of $\mathrm{PG}(V_1)$. It follows from Lemma 9 that P^Ψ corresponds to the matrix M_L, where $L(Y)$ is the q-polynomial given by

$$L(Y) := \sum_{i=0}^{n-1} x_i^{q^i} Y^{q^i}. \tag{7}$$

This implies that P^Ψ is a point of Ω_{n-2} if and only if M_L is singular if and only if there exists an $a \in \mathbb{F}_{q^n}^*$ such that

$$\sum_{i=0}^{n-1}(x_i a)^{q^i} = 0,$$

or equivalently, there exists an $a \in \mathbb{F}_{q^n}^*$ such that

$$\langle (ax_0, ax_1, \dots, ax_{n-1}) \rangle \in \mathcal{W}.$$

It follows that the matrix corresponding to P^Ψ is singular if and only if $B(P) \in B(\mathcal{W})$. This provides us with a one-to-one correspondence between the set of points

$$\{P \in \mathrm{PG}(n^2-1,q)\colon B(P) \in B(\mathcal{W})\}$$

and the points of the secant variety Ω_{n-2}. $\square$

An immediate corollary of the proof of Theorem 11 and Lemma 9 is the following.

Corollary 12. *The secant variety Ω_k, $1 \leqslant k \leqslant n-2$, can be partitioned by elements of $B(\mathcal{W})^\Psi$, where Ψ is defined by* (6). *In particular, the elements of $\mathcal{D}$ intersecting $\mathcal{W}$ partition the pointset of a determinantal hypersurface in* $\mathrm{PG}(V_1)$.

Proof. In order to show that the elements of $B(\mathcal{W})$ partition Ω_k, $1 \leqslant k \leqslant n-2$, as in the proof of Theorem 7, it suffices to show that any two points of an arbitrary $B(P)^\Psi$ have the same rank. Let P have coordinates $(x_0, x_1, \dots, x_{n-1})$ and consider a second point P' in $B(P)$, say with coordinates $(ax_0, ax_1, \dots, ax_{n-1})$ for some $a \in \mathbb{F}_{q^n}^*$. By Lemma 9, the rank of P^Ψ equals the codimension of the solution space of the linear transformation given by the q-polynomial $L(Y)$ defined in (7). Similarly the rank of P'^Ψ equals the codimension of the solution space of the linear transformation given by the q-polynomial

$$\sum_{i=0}^{n-1}(ax_i)^{q^i} Y^{q^i}.$$

Since these solution spaces have the same dimension (use the substitution $Y \mapsto a^{-1}Y$), it follows that P^Ψ and P'^Ψ have the same rank. $\square$

3. Finite semifields and the BEL-construction

The geometric construction method for finite semifields given in [3] gives a correspondence between finite semifields and particular configurations of subspaces with respect to a Desarguesian spread of a projective space (which we will refer to as a *BEL-configuration*). In the original BEL-configuration of a semifield of order q^n, apart from q and n, there is an extra parameter r involved. In particular, starting from a Desarguesian $(n-1)$-spread $\mathcal{D}$, and any two subspaces U and W of $\mathrm{PG}(rn-1,q)$, $r \geqslant 2$, of dimension $n-1$ and $rn-n-1$, respectively, such that $B(U) \cap B(W) = \emptyset$, one obtains a semifield $\mathbb{S}(U,W)$ of order q^n. As before, we use the notation $B(T)$ to denote the set of elements of the Desarguesian spread that intersect the subspace (or subset) T. The construction goes as follows:

- Embed $\mathrm{PG}(rn-1,q)$ in $\mathrm{PG}(rn+n-1,q)$ and extend $\mathcal{D}$ to a Desarguesian spread $\mathcal{D}'$ of $\mathrm{PG}(rn+n-1,q)$.
- Let A be an n-dimensional subspace of $\mathrm{PG}(rn+n-1,q)$ which intersects $\mathrm{PG}(rn-1,q)$ in U.
- Let $\mathcal{S}(U,W)$ be the set of subspaces defined by $B(A)$ in the quotient geometry $\mathrm{PG}(2n-1,q)$ of W, i.e.,

$$\mathcal{S}(U,W)=\{\langle R,W\rangle/W:\ R\in B(A)\}.$$

In [3, Theorem 2.2] it was shown that $\mathcal{S}(U,W)$ is a semifield spread of $\mathrm{PG}(2n-1,q)$. The corresponding semifield is denoted by $\mathbb{S}(U,W)$. Also in [3] it was proved that each finite semifield can be obtained this way.

Theorem 13. *(See [3, Theorem 4.1].) For every finite semifield $\mathbb{S}$, there exist $n\geqslant 1$, a prime p and subspaces U and W in $\mathrm{PG}(n^2-1,p)$, of dimension $n-1$ and n^2-n-1, respectively, such that $\mathbb{S}$ is isotopic to $\mathbb{S}(U,W)$.*

4. Isotopism and the BEL-construction

When dealing with semifields, one is often confronted with the problem of determining whether two semifields are *isotopic*, or equivalently (by [1]), when the corresponding projective planes are isomorphic, or equivalently when the corresponding spreads are isomorphic (by [2]) (sometimes called *equivalent*). In [3] the following theorem was proved.

Theorem 14. *Let $\mathbb{S}(U,W)$ and $\mathbb{S}(U',W')$ be two semifields constructed from subspaces U, U', W, W' of $\mathrm{PG}(rn-1,q)$. If there exists an element φ of $\mathrm{P\Gamma L}(rn,q)$, fixing the Desarguesian spread $\mathcal{D}$, and such that $U^\varphi=U'$ and $W^\varphi=W'$, then $\mathbb{S}(U,W)$ and $\mathbb{S}(U',W')$ are isotopic semifields.*

This theorem still leaves open the possibility for two BEL-configurations to give isotopic semifields, although they do not allow a semilinear collineation of $\mathrm{PG}(rn-1,q)$ as in Theorem 14. That this also happens, was one of the problems unresolved in the original paper, see [3, Remark 4.4]. We investigate this problem here.

Although the parameter r might be useful to construct new examples (by keeping it small), it is an obstacle when we want to deal with the isotopism issue. Let us illustrate the second part of this statement.

Suppose we have a BEL-configuration (U,W) in $\Lambda_{rn-1}:=\mathrm{PG}(rn-1,q)$. Denote the $(rn+n-1)$-dimensional space used to construct the semifield spread $\mathcal{S}(U,W)$ by Λ_{rn+n-1}; so $\mathcal{D}'$ is a Desarguesian spread of Λ_{rn+n-1}. Let Λ'_{rn+n-1} denote a $\mathrm{PG}(rn+n-1,q)$ that intersects Λ_{rn+n-1} in Λ_{rn-1}, and denote $\langle\Lambda_{rn+n-1},\Lambda'_{rn+n-1}\rangle$ by $\Lambda_{rn+2n-1}$. Extend $\mathcal{D}'$ to a Desarguesian spread $\mathcal{D}_{rn+2n-1}$ of $\Lambda_{rn+2n-1}$ in such a way that Λ'_{rn+n-1} is partitioned by elements of $\mathcal{D}_{rn+2n-1}$.

Now define $W'=\langle W,T\rangle$, for some $T\in\mathcal{D}_{rn+2n-1}\setminus\mathcal{D}$, with $T\subset\Lambda'_{rn+n-1}$.

Theorem 15. *The pair (U,W') forms a BEL-configuration in Λ'_{rn+n-1} and the semifields $\mathbb{S}(U,W)$ and $\mathbb{S}(U,W')$ are isotopic.*

Proof. Clearly we obtain a BEL-configuration (U, W') in Λ'_{rn+n-1}: each element of $B(U)$ is skew to each element of $B(W')$, since an element of $B(W')$ is either in $B(W)$ or skew to Λ_{rn-1}. In order two show that the semifields $\mathbb{S}(U, W)$ and $\mathbb{S}(U, W')$ are isotopic, consider the map defined on the points of $\Lambda_{rn+2n-1}/W'$:

$$\begin{aligned}&\gamma : \Lambda_{rn+2n-1}/W' \to \Lambda_{rn+n-1}/W\\&\bar{P} = \langle P, W'\rangle/W' \mapsto \big(\langle P, W'\rangle \cap \Lambda_{rn+n-1}\big)/W.\end{aligned}$$

The map γ is well defined since each subspace $\langle P, W'\rangle$, for a point $P \in \Lambda_{rn+2n-1} \setminus W$, meets Λ_{rn+n-1} in a subspace of dimension $rn-n$ which contains W. Next, suppose $\bar{P}^\gamma = \bar{Q}^\gamma$, i.e.,

$$\big(\langle P, W'\rangle \cap \Lambda_{rn+n-1}\big)/W = \big(\langle Q, W'\rangle \cap \Lambda_{rn+n-1}\big)/W,$$

for some P and Q in $\Lambda_{rn+2n-1} \setminus W$. This implies that

$$\big\langle\big(\langle P, W'\rangle \cap \Lambda_{rn+n-1}\big), W\big\rangle = \big\langle\big(\langle Q, W'\rangle \cap \Lambda_{rn+n-1}\big), W\big\rangle,$$

and hence

$$\big\langle\big(\langle P, W'\rangle \cap \Lambda_{rn+n-1}\big), W'\big\rangle = \big\langle\big(\langle Q, W'\rangle \cap \Lambda_{rn+n-1}\big), W'\big\rangle.$$

Since

$$\big\langle\big(\langle P, W'\rangle \cap \Lambda_{rn+n-1}\big), W'\big\rangle = \langle P, W'\rangle,$$

for each point $P \in \Lambda_{rn+2n-1} \setminus W$, it follows that $\langle P, W'\rangle = \langle Q, W'\rangle$, and hence $\bar{P} = \bar{Q}$. This shows that γ is injective. It follows that γ is a bijection between the $(2n-1)$-dimensional projective spaces $\Lambda_{rn+2n-1}/W'$ and Λ_{rn+n-1}/W. In order to show that γ is a collineation, consider three collinear points $\bar{P}_1$, $\bar{P}_2$, and $\bar{P}_3$ in $\Lambda_{rn+2n-1}/W'$. The subspace spanned by P_1, P_2, and W' then contains $\langle P_3, W'\rangle$, and this means that

$$\langle P_3, W'\rangle \cap \Lambda_{rn+n-1} \subset \big\langle\langle P_1, W'\rangle \cap \Lambda_{rn+n-1}, \langle P_2, W'\rangle \cap \Lambda_{rn+n-1}\big\rangle.$$

This is equivalent to saying that $\bar{P}_1^\gamma$, $\bar{P}_2^\gamma$ and $\bar{P}_3^\gamma$ are collinear points. It follows that γ is a bijection between the $(2n-1)$-dimensional projective spaces $\Lambda_{rn+2n-1}/W'$ and Λ_{rn+n-1}/W mapping collinear points to collinear points, i.e., a collineation. It is easy to see that γ maps the spread $\mathcal{S}(U, W')$ onto the spread $\mathcal{S}(U, W)$, i.e., $\mathbb{S}(U, W)$ and $\mathbb{S}(U, W')$ are isotopic. □

Note that increasing the parameter r without changing the isotopism class of the semifield, as illustrated by Theorem 15, can also be reversed until we reach a W that equals $\langle B(U)\rangle \cap W$. We know that $\langle B(U)\rangle$ is partitioned by spread elements, and so if W is larger than $\langle B(U)\rangle \cap W$, we can continue picking a T from the elements of $B(W)$ which do not belong to $\langle B(U)\rangle$, and reverse the arguments used in Theorem 15, in order to obtain a BEL-configuration with a W satisfying $W = \langle B(U)\rangle \cap W$.

Theorem 15 shows that it is impossible to give a satisfactory solution to the isotopism problem for BEL-configurations without specifying the parameter r. In fact, even for a specific r, there are too many parameters in the BEL-configuration in order to solve the isotopism problem as illustrated by [3, Remark 4.4] (also pointed out in [15]).

We can remove the excess of freedom as follows. As mentioned before, in [3] it was proved that a finite semifield can be constructed from a BEL-configuration (U, W) with $r = n$. Also, the parameters q and n are effectively only one parameter (namely the order of the semifield), since two semifields can only be isotopic if they have the same order q^n and hence the same characteristic p. Together with the proof of Theorem 4.1 in [3] this guaranties us that it suffices to restrict ourselves to BEL-configurations $(U, \mathcal{W})$ in a projective space $\mathrm{PG}(n^2 - 1, p)$, where p is prime, and where $\mathcal{W}$ is defined by (5) (with $q = p$).

It should be noted that we could have made a different choice here. Instead of restricting ourselves to BEL-configurations in $\mathrm{PG}(n^2 - 1, p)$, p prime, when dealing with an isotopism problem for semifields of order p^n, we could have restricted ourselves to BEL-configurations $(U, \mathcal{W})$ in $\mathrm{PG}(n^2 - 1, q)$, where $\mathbb{F}_q$ is contained in the nucleus of the semifields of order q^n. The reason for this is that if one replaces the characteristic p of the semifield $\mathbb{S}$ in the proof of Theorem 4.1 in [3] by the size of the nucleus of $\mathbb{S}$, one obtains a proof for the following theorem.

Theorem 16. *For every semifield $\mathbb{S}$, there exist subspaces U and W of $\mathrm{PG}(n^2 - 1, q)$, where $\mathbb{F}_q$ is contained in the nucleus of $\mathbb{S}$, such that $\mathbb{S}(U, W)$ is isotopic to $\mathbb{S}$.*

Proof. Replace p by q in the proof of Theorem 4.1 of [3], and start with the multiplication given by

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

with $c_{i,j} \in \mathbb{F}_{q^n}$. $\square$

The following theorem solves the isotopism-problem for BEL-configurations in $\mathrm{PG}(n^2 - 1, q)$, with $\mathcal{W}$ given by (5).

Theorem 17. *Two semifields $\mathbb{S}(\mathcal{U}, \mathcal{W})$ and $\mathbb{S}(\mathcal{U}', \mathcal{W})$, with $\mathcal{W}$ defined by (5), are isotopic if and only if there exists a collineation ϕ of $\mathrm{PG}(V_1)$ fixing $B(\mathcal{W})$ with $\mathcal{U}^\phi = \mathcal{U}'$.*

Proof. Suppose $\mathbb{S} = \mathbb{S}(\mathcal{U}, \mathcal{W})$ and $\mathbb{S}' = \mathbb{S}(\mathcal{U}', \mathcal{W})$, with $\mathcal{W}$ defined by (5), are isotopic semifields, with multiplication given by

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

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

$x, y \in \mathbb{F}_{q^n}$, respectively. The subspaces $\mathcal{U}$ and $\mathcal{U}'$ corresponding to the semifields $\mathbb{S}$ and $\mathbb{S}'$, as in the BEL-construction, are given by

$$\mathcal{U} := \{\langle (c_0(x), c_1(x)^{1/q}, \ldots, c_{n-1}(x)^{1/q^{n-1}})\rangle\colon x \in \mathbb{F}_{q^n}^*\}$$

and

$$\mathcal{U}' := \{\langle (c_0'(x), c_1'(x)^{1/q}, \ldots, c_{n-1}'(x)^{1/q^{n-1}})\rangle\colon x \in \mathbb{F}_{q^n}^*\},$$

respectively. The corresponding semifield spreads of $\mathrm{PG}(2n-1,q)$, $\mathcal{S}$ and $\mathcal{S}'$, consist of the subspace

$$S_\infty = S_\infty' = \{(0,y) \mid y \in \mathbb{F}_{q^n}^*\},$$

together with the subspaces

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

respectively. The image of $\mathcal{U}$, respectively $\mathcal{U}'$, under the collineation $\Psi : \mathrm{PG}(V_1) \to \mathrm{PG}(V_2)$ defined by (6), is given by

$$\mathcal{U}^\Psi = \mathrm{PG}(\{R_x \mid x \in \mathbb{F}_{q^n}^*\}) \subset \mathrm{PG}(V_2),$$

with $R_x = U^{-1}A_\alpha U$, $\alpha = (c_0(x), \ldots, c_{n-1}(x))$, and

$$\mathcal{U}'^\Psi = \mathrm{PG}(\{R_x' \mid x \in \mathbb{F}_{q^n}^*\}) \subset \mathrm{PG}(V_2),$$

with $R_x' = U^{-1}A_\alpha' U$, $\alpha' = (c_0'(x), \ldots, c_{n-1}'(x))$. The matrices R_x, respectively R_x', are the matrices induced by right multiplication in the semifield $\mathbb{S}$, respectively $\mathbb{S}'$. Since the semifields $\mathbb{S}$ and $\mathbb{S}'$ are isotopic if and only if the spreads are isomorphic, and since the automorphism group of a semifield spread (if the semifield is not a field), fixes one special element (in this case the element S_∞, see [5]) and acts transitively on the other elements of the spread, we may assume that the isomorphism β between the two spreads $\mathcal{S}$ and $\mathcal{S}'$, induced by the isotopy between $\mathbb{S}$ and $\mathbb{S}'$, also fixes $S_0 = S_0'$. With the representation of the semifield spreads $\mathcal{S}$ and $\mathcal{S}'$ of $\mathrm{PG}(2n-1,q)$ as above, it follows that β is of the form

$$(x,y) \mapsto (Ax^\sigma, By^\sigma), \tag{8}$$

where A and B are elements of $\mathrm{GL}(n,q)$, and $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$. It follows that the image of S_x under β can be written as

$$S_x^\beta = \{(Ay^\sigma, B(y \circ x)^\sigma) \mid y \in \mathbb{F}_{q^n}^*\} = \{(z, B((A^{-\sigma^{-1}} z^{\sigma^{-1}}) \circ x)^\sigma) \mid z \in \mathbb{F}_{q^n}^*\}.$$

If $S_x^\beta = S_y'$ for some $y \in \mathbb{F}_{q^n}$, then $R_y' = BR_x^\sigma A^{-1}$, which shows that the two semifields $\mathbb{S}$ and $\mathbb{S}'$ are isotopic if and only if there exist non-singular matrices C (corresponding to B) and D (corresponding to A^{-1}) such that the two sets of matrices R_x and R_x', are related by

$$\{R_x' \mid x \in \mathbb{F}_{q^n}^*\} = \{CR_x^\sigma D \mid x \in \mathbb{F}_{q^n}^*\}.$$

This is if and only if there exists a collineation φ of $\mathrm{PG}(V_2)$ such that $\mathcal{U}^{\Psi\varphi} = \mathcal{U}'^{\Psi}$ (where φ is induced by the isomorphism $X \mapsto CX^{\sigma}D$ of V_2), if and only if there exists a collineation $\phi = \Psi\varphi\Psi^{-1}$ of $\mathrm{PG}(V_1)$ such that $\mathcal{U}^{\phi} = \mathcal{U}'$. Since C, D are both non-singular, X and $CX^{\sigma}D$ have the same rank, which implies that φ fixes the kth secant variety, $1 \leqslant k \leqslant n-2$. In particular φ fixes both families of maximal subspaces of the Segre variety, and hence, by Corollary 12, ϕ fixes $B(\mathcal{W})$.

Conversely, suppose ϕ is a collineation of $\mathrm{PG}(V_1)$ fixing $B(\mathcal{W})$, such that $\mathcal{U}^{\phi} = \mathcal{U}'$. By Theorem 11, $\Psi^{-1}\phi\Psi$ fixes the determinantal hypersurface Ω_{n-2}, and in particular $\Psi^{-1}\phi\Psi$ fixes the Segre variety, by Corollary 6. Moreover, since ϕ not only fixes the set of points contained in the elements of $B(\mathcal{W})$, but also the elements of $B(\mathcal{W})$, $\Psi^{-1}\phi\Psi$ also will fix both families of maximal subspaces of the Segre variety (by Corollary 12). By [10] we find an automorphism $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$, and non-singular $(n \times n)$-matrices C and D over $\mathbb{F}_q$ which relate the sets of matrices R_x and R'_x as in the first part of the proof. This is equivalent to an isotopy between the two semifields $\mathbb{S}(\mathcal{U}, \mathcal{W})$ and $\mathbb{S}(\mathcal{U}', \mathcal{W})$. □

We denote the subgroup of $\mathrm{P\Gamma L}(n^2, q)$ fixing both systems Σ_1 and Σ_2 of a Segre variety $\mathcal{S}_{n,n}$ by $H(\mathcal{S}_{n,n})$.

Theorem 18. *There is a one-to-one correspondence between the isotopism classes of finite semifields of order q^n, with nucleus containing $\mathbb{F}_q$, and the orbits of the action of $H(\mathcal{S}_{n,n})$ on the $(n-1)$-dimensional subspaces of $\mathrm{PG}(n^2-1, q)$ skew to the $(n-2)$th secant variety Ω_{n-2} of $\mathcal{S}_{n,n}$.*

Proof. Combine Theorems 17 and 11. □

Theorem 19. *There is a one-to-one correspondence between the isotopism classes of finite semifields of order q^n, with nucleus containing $\mathbb{F}_q$, and the orbits of the action of a subgroup of index two of the automorphism group of a determinantal hypersurface $\mathcal{V}$ on the subspaces of maximum dimension skew to $\mathcal{V}$.*

Proof. It follows from Theorems 3 and 11 that the group $H(\mathcal{S}_{n,n})$ is a subgroup of index two of the automorphism group of a determinantal hypersurface $\mathcal{V}$ in $\mathrm{PG}(n^2-1, q)$. That a subspace skew to $\mathcal{V}$ has dimension $\leqslant n-1$ follows from Theorem 11 and $\dim(\mathcal{W}) = n^2-n-1$. Now apply Theorem 18. □

Note that the involution corresponding to this subgroup of index two is induced by matrix transposition in V_2. The following theorem determines the $H(\mathcal{S}_{n,n})$-orbit corresponding to the isotopy class of a finite field.

Theorem 20. *The $H(\mathcal{S}_{n,n})$-orbit corresponding the isotopy class of a finite field is the orbit of a subspace T skew to the $(n-2)$th secant variety Ω_{n-2} of $\mathcal{S}_{n,n}$, where $T^{\Psi^{-1}}$ is an element of the Desarguesian spread D.*

Proof. Put $U = T^{\Psi^{-1}}$ and apply the BEL-construction with the notation as in Section 3. Since U is an element of $\mathcal{D}$, the elements of the Desarguesian spread $\mathcal{D}'$ of $\mathrm{PG}(n^2+n-1, q)$, intersecting the n-dimensional subspace A are the elements of $\mathcal{D}'$ contained in $\langle U, R\rangle$, with R is an arbitrary element of $B(A) \setminus \{U\}$. This implies that the spread $\mathcal{S}(U, W)$ is Desarguesian. Consequently the semifield $\mathbb{S}(U, \mathcal{W})$ is a field. Combining Theorems 17 and 11 concludes the proof. $\square$

References

[1] A.A. Albert, Finite division algebras and finite planes, in: Proc. Sympos. Appl. Math., vol. 10, Amer. Math. Soc., Providence, RI, 1960, pp. 53–70.

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

[3] S. Ball, G. Ebert, M. Lavrauw, A geometric construction of finite semifields, J. Algebra 311 (1) (2007) 117–129.

[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 (6) (2006) 940–961.

[5] P. Dembowski, Finite Geometries, Classics Math., Springer-Verlag, Berlin, 1997, reprint of the 1968 original.

[6] L.E. Dickson, Linear algebras in which division is always uniquely possible, Trans. Amer. Math. Soc. 7 (3) (1906) 370–390.

[7] G. Ebert, G. Marino, O. Polverino, R. Trombetti, Infinite families of new semifields, submitted for publication.

[8] M. Hall, Projective planes, Trans. Amer. Math. Soc. 54 (1943) 229–277.

[9] D. Hilbert, Probleme der Grundlegung der Mathematik, Math. Ann. 102 (1) (1930) 1–9.

[10] J.W.P. Hirschfeld, J.A. Thas, General Galois Geometries, Oxford Math. Monogr., The Clarendon Press, Oxford Univ. Press, New York, 1991, Oxford Sci. Publ.

[11] D.R. Hughes, F.C. Piper, Projective Planes, Grad. Texts in Math., vol. 6, Springer-Verlag, New York, 1973.

[12] N.L. Johnson, V. Jha, M. Biliotti, Handbook of Finite Translation Planes, Pure Appl. Math. (Boca Raton), vol. 289, Chapman & Hall/CRC, Boca Raton, FL, 2007.

[13] N.L. Johnson, G. Marino, O. Polverino, R. Trombetti, On a generalization of cyclic semifields, J. Algebraic Combin., in press.

[14] W.M. Kantor, Finite semifields, in: Finite Geometries, Groups, and Computation, Walter de Gruyter GmbH & Co. KG, Berlin, 2006, pp. 103–114.

[15] W.M. Kantor, Hmo-planes, Adv. Geom., in press.

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

[17] M. Lavrauw, Scattered spaces with respect to spreads, and eggs in finite projective spaces, Eindhoven University of Technology, Eindhoven, 2001 (Dissertation, Technische Universiteit Eindhoven, Eindhoven, 2001).

[18] R. Lidl, H. Niederreiter, Finite Fields, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997, with a foreword by P.M. Cohn.

[19] G. Marino, O. Polverino, R. Trombetti, On semifields of type (q^{2n}, q^n, q^2, q), n odd, Innov. Incidence Geom., in press.

[20] G. Menichetti, n-Dimensional algebras over a field with a cyclic extension of degree n, Geom. Dedicata 63 (1) (1996) 69–94.

[21] C. Segre, Sulle varietà che rappresentano le coppie di punti di due piani o spazi, Rend. Circ. Mat. Palermo 5 (1891) 192–204.