Finite Semifields and Galois Geometry*

Michel Lavrauw†

and

Olga Polverino ‡

1 Introduction and preliminaries

In this article, we concentrate on the links between Galois geometry and a particular kind of non-associative algebras of finite dimension over a finite field $\mathbb{F}$, called *finite semifields*. Although in the earlier literature (predating 1965) the term semifields was not used, the study of these algebras was initiated about a century ago by Dickson [31], shortly after the classification of finite fields, taking a purely algebraic point of view. Nowadays it is common to use the term *semifields* introduced by Knuth [58] in 1965 with the following motivation:

"We are concerned with a certain type of algebraic system, called a semifield*. Such a system has several names in the literature, where it is called, for example, a "nonassociative division ring" or a "distributive quasifield". Since these terms are rather lengthy, and since we make frequent reference to such systems in this paper, the more convenient name semifield will be used."*

By now, the theory of semifields has become of considerable interest in many different areas of mathematics. Besides the numerous links with finite geometry, most of which are considered here, semifields arise in the context of difference sets, coding theory, cryptography, and group theory.

To conclude this prelude we would like to emphasize that this article should not be considered as a general survey on finite semifields, but rather an approach to the subject with the focus on its connections with Galois geometry. There are many other interesting properties and constructions of finite semifields (and links with other subjects) that are not addressed here.

---

*March 2011, available from `http://cage.ugent.be/~ml`

†The author acknowledges the support of the Fund for Scientific Research - Flanders (FWO)
(Email: ml@cage.ugent.be)

‡The author acknowledges the support of the Research Project of MIUR (Italian Office for University and Research) *Geometrie su campi di Galois, piani di traslazione e geometrie d'incidenza*
(Email: olga.polverino@unina2.it)

1.1 Definition and first properties

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 $x\in\mathbb{S}$.

An algebra satisfying all of the axioms of a semifield except (S4) is called a *pre-semifield*. By what is sometimes called Kaplansky's trick, a semifield with identity $u\circ u$ is obtained from a pre-semifield by defining a new multiplication $\hat{\circ}$ as follows

$$(x\circ u)\hat{\circ}(u\circ y)=x\circ y. \tag{1}$$

A finite field is of course a trivial example of a semifield. The first non-trivial examples of semifields were constructed by Dickson in [31]: a semifield $(\mathbb{F}_{q^k}^2,+,\circ)$ of order q^{2k} with addition and multiplication defined by

$$\begin{cases} (x,y)+(u,v) &= (x+u,y+v)\\ (x,y)\circ(u,v) &= (xu+\alpha y^q v^q, xv+yu)\end{cases} \tag{2}$$

where q is an odd prime power and α is a non-square in $\mathbb{F}_{q^k}$.

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

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

$$\mathbb{N}_m(\mathbb{S}):=\{y\ :\ y\in\mathbb{S}\mid x\circ(y\circ z)=(x\circ y)\circ z,\ \forall x,z\in\mathbb{S}\}, \tag{4}$$

$$\mathbb{N}_r(\mathbb{S}):=\{z\ :\ z\in\mathbb{S}\mid x\circ(y\circ z)=(x\circ y)\circ z,\ \forall x,y\in\mathbb{S}\}. \tag{5}$$

The intersection of the *associative center* $\mathbb{N}(\mathbb{S})$ (the intersection of the three nuclei) and the commutative center is called the *center* of $\mathbb{S}$ and denoted by $C(\mathbb{S})$. Apart from the usual representation of a semifield as a finite-dimensional algebra over its center, a semifield can also be viewed as a left vector space $V_l(\mathbb{S})$ over its left nucleus, as a left vector space $V_{lm}(\mathbb{S})$ and right vector space $V_{rm}(\mathbb{S})$ over its middle nucleus, and as a right vector space $V_r(\mathbb{S})$ over its right nucleus. Left (resp. right) multiplication in $\mathbb{S}$ by an element x is denoted by L_x (resp. R_x), i.e. $y^{L_x}=x\circ y$ (resp. $y^{R_x}=y\circ x$). It follows that L_x is an endomorphism of $V_r(\mathbb{S})$, while R_x is an endomorphism of $V_l(\mathbb{S})$.

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

$$x\circ y=\sum_{i,j=1}^{n}x_iy_j(e_i\circ e_j)=\sum_{i,j=1}^{n}x_iy_j\left(\sum_{k=1}^{n}a_{ijk}e_k\right) \tag{6}$$

for certain $a_{ijk} \in \mathbb{F}$, called the *structure constants* of $\mathbb{S}$ with respect to the basis $\{e_1, \ldots, e_n\}$. This approach was used by Dickson in 1906 to prove the following characterisation of finite fields.

Theorem 1 ([31]). *A two-dimensional finite semifield is a finite field.*

In [58] 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 $\{\mathbb{S}, \mathbb{S}^{(12)}, \mathbb{S}^{(13)}, \mathbb{S}^{(23)}, \mathbb{S}^{(123)}, \mathbb{S}^{(132)}\}$.

1.2 Projective planes and isotopism

As mentioned before, the study of semifields originated around 1900, and the link with projective planes through the coordinatisation method inspired by Hilbert's *Grundlagen der Geometrie* (1999), and generalised by Hall [39] in 1943, was a further stimulation for the development of the theory of finite semifields. Everything which is contained in this section concerning projective planes and the connections with semifields can be found with more details in [28], [44], [47], and [73]. It is in this context that the notion of isotopism is of the essence.

Two semifields $\mathbb{S}$ and $\hat{\mathbb{S}}$ are called *isotopic* if there exists 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 $x, y, z \in \mathbb{S}$. The triple (F, G, H) is called an *isotopism*. An isotopism where H is the identity is called a *principal isotopism*. The set of semifields isotopic to a semifield $\mathbb{S}$ is called the *isotopism class of* $\mathbb{S}$ and is denoted by $[\mathbb{S}]$. Note that the size of the center as well as the size of the nuclei of a semifield are invariants of its isotopism class, and since the nuclei are finite fields, it is allowed to talk about the nuclei of an isotopism class $[\mathbb{S}]$.

A *projective plane* is a geometry consisting of a set $\mathcal{P}$ of *points* and a set $\mathcal{L}$ of subsets of $\mathcal{P}$, called *lines*, satisfying the following three axioms

(PP1) Each two different points are contained in exactly one line.

(PP2) Each two different lines intersect in exactly one point.

(PP3) There exist four points, no three of which are contained in a line.

Two projective planes π and π' are *isomorphic* if there exists a one-to-one correspondence between the points of π and the points of π' preserving collinearity, i.e., a line of π is mapped onto a line of π'. A projective plane is called *Desarguesian* if it is isomorphic to $\mathrm{PG}(2, \mathbb{F})$, for some (skew) field $\mathbb{F}$. An isomorphism of a projective plane π is usually called a *collineation* and a (P, ℓ)*-perspectivity* of π is a collineation of π that fixes every line on P and every point on ℓ. Because of the self-dual property of the set of axioms $\{$(PP1),(PP2),(PP3)$\}$, interchanging points and lines of a projective plane π, one obtains another projective plane, called the *dual plane*, which we denote by π^d. If there exists a line ℓ in a projective plane π, such that for each point P on ℓ the group of (P, ℓ)-perspectivities acts transitively on the points of the affine plane $\pi \setminus \ell$, then π is called a *translation plane* , and ℓ is called a translation line of π. If both π and π^d are translation planes, then π is called a *semifield plane* . The point of a semifield plane corresponding to the translation line of the dual plane is called the *shears point*. It can be shown

that, unless the plane is Desarguesian, the translation line (shears point) of a translation plane (dual translation plane) is unique, and the shears point of a semifield plane π lies on the translation line of π. The importance of the notion of isotopism arises from the equivalence between the isomorphism classes of projective planes and the isotopism classes of finite semifields, as shown by A. A. Albert in 1960.

Theorem 2 ([1]). *Two semifield planes are isomorphic if and only if the corresponding semifields are isotopic.*

The connection between semifield planes and the notion of semifields as we introduced them (as an algebra) is given by the coordinatisation method of projective planes. Without full details here, let us give an overview using homogeneous coordinates, following Knuth [58]. Let π be a projective plane, and let (R,T) be a ternary ring coordinatising π, with respect to a frame $\mathcal{G}$ in π. The points of π are represented by $(1,a,b)$, $(0,1,a)$, or $(0,0,1)$, where $a,b \in R$ and the lines are represented by $[1,c,d]$, $[0,1,c]$, $[0,0,1]$, with $c,d \in R$, where the frame $\mathcal{G} = \{(1,0,0), (0,1,0), (0,0,1), (1,1,1)\}$. The point (a,b,c) lies on the line $[d,e,f]$ if and only if

$$dc = T(b,e,af). \tag{7}$$

Since d and a must be either 0 or 1, it is clear what dc and af means.

It follows that T satisfies certain properties, and in fact one can list the necessary and sufficient properties that a ternary ring has to satisfy in order to be a ternary ring obtained by coordinatising a projective plane (by "inverse coordinatisation", i.e. constructing the plane starting from the ternary ring). In this case (R,T) is called a *planar ternary ring* , usually abbreviated to PTR. Now define two operations $a \circ b := T(a,b,0)$, and $a+b := T(a,1,b)$, and consider the structure $(R,\circ,+)$. This turns $(R,+)$ and $(R,\circ)$ into loops, with respective identities 0 and 1. With this setup, one is able to connect the algebraic properties of the PTR with the geometric properties of the plane, or more specifically, with the properties of the automorphism group of the plane π, using the following standard terminology.

A PTR is called *linear* if $T(a,b,c) = a \circ b + c$, $\forall a,b,c \in R$. A *cartesian group* is a linear PTR with associative addition; a *(left) quasifield* is a cartesian group in which the left distributive law holds; and a *semifield* is a quasifield in which both distributive laws hold, consistent with (S1)-(S4). These algebraic properties correspond to the following geometric properties. A linear PTR is a cartesian group if and only if π is $((0,0,1),[0,0,1])$-transitive. A cartesian group is a quasifield if and only if π is $((0,1,0),[0,0,1])$-transitive, and in this case π is a translation plane with translation line $[0,0,1]$, and $(R,+)$ is abelian. A semifield plane was defined as a translation plane which is also a dual translation plane, and we leave it to the reader to check the consistency of this definition.

1.3 Spreads and linear sets

An elegant way to construct a translation plane is by using so-called *spreads* of projective spaces. This construction is often called the *André-Bruck-Bose* construction.

Let $\mathcal{S}$ be a set of $(t-1)$-dimensional subspaces of $\mathrm{PG}(n-1,q)$. Then $\mathcal{S}$ is called a $(t-1)$-*spread* of $\mathrm{PG}(n-1,q)$ if every point of $\mathrm{PG}(n-1,q)$ is contained in exactly one element of $\mathcal{S}$. If $\mathcal{S}$ is a set of subspaces of $V(n,q)$ of rank t, then $\mathcal{S}$ is called a *t-spread* of $V(n,q)$ if every vector of $V(n,q) \setminus \{0\}$ is contained in exactly one element of $\mathcal{S}$.

Theorem 3 ([88]). *There exists a $(t-1)$-spread in $\mathrm{PG}(n-1,q)$ if and only if t divides n.*

Suppose t divides n, and put $n = rt$. The $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$ obtained by considering the points of $\mathrm{PG}(r-1,q^t)$ as $(t-1)$-dimensional subspaces over $\mathbb{F}_q$ is called a *Desarguesian spread* . This correspondence between the points of $\mathrm{PG}(r-1,q^t)$ and the elements of a Desarguesian $(t-1)$-spread will often be used in this article, and if the context is clear, we will identify the elements of the Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$ with the points of $\mathrm{PG}(r-1,q^t)$. If T is any subset of $\mathrm{PG}(rt-1,q)$ endowed with a Desarguesian spread $\mathcal{D}$, then by $B_{\mathcal{D}}(T)$ (or $B(T)$ if there is no confusion) we denote the set of elements of $\mathcal{D}$ that intersect T non-trivially.

A set L of points in $\mathrm{PG}(r-1,q_0)$ is called a *linear set* if there exists a subspace U in $\mathrm{PG}(rt-1,q)$, for some $t \geq 1$, $q^t = q_0$, such that L is the set of points corresponding to the elements of a Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$ intersecting U, i.e. $L = B(U)$. If we want to specify the field $\mathbb{F}_q$ over which L is linear, we call L an $\mathbb{F}_q$*-linear set*. If U has dimension d in $\mathrm{PG}(rt-1,q)$, then the linear set $B(U)$ is called a linear set *of rank* $d+1$.

The same notation and terminology is used when U is a subspace of the vector space $V(rt,q)$ instead of a projective subspace. For an overview of the use of linear sets in various other areas of Galois geometries, we refer to [59], [66], and [85].

Let $\mathcal{S}$ be a $(t-1)$-spread in $\mathrm{PG}(2t-1,q)$. Consider $\mathrm{PG}(2t-1,q)$ as a hyperplane of $\mathrm{PG}(2t,q)$. We define an incidence structure $(\mathcal{P},\mathcal{L},I)$ as follows. The pointset $\mathcal{P}$ consists of all points of $\mathrm{PG}(2t,q) \setminus \mathrm{PG}(2t-1,q)$ and the lineset $\mathcal{L}$ consists of all t-spaces of $\mathrm{PG}(2t,q)$ intersecting $\mathrm{PG}(2t-1,q)$ in an element of $\mathcal{S}$. The incidence relation I is containment.

Theorem 4 ([3], [17], [18]). *The incidence structure $(\mathcal{P},\mathcal{L},I)$ is an affine plane and its projective completion is a translation plane of order q^t. Moreover, every translation plane can be constructed in this way.*

For this reason, a $(t-1)$-spread in $\mathrm{PG}(2t-1,q)$ is sometimes called a *planar spread*. Two spreads are said to be *isomorphic* if there exists a collineation of the projective space mapping one spread onto the other.

Theorem 5 ([3], [17], [18]). *Two translation planes are isomorphic if and only if the corresponding spreads are isomorphic.*

These theorems are of fundamental importance in Galois geometry; they imply a one-to-one correspondence between translation planes and planar spreads. The construction of a translation plane from a planar spread is called the *André-Bruck-Bose construction* . If the translation plane obtained is a semifield plane, then the spread is called a *semifield spread* . It follows from the fact that a semifield plane π is a dual translation plane, that a semifield spread $\mathcal{S}$ contains a special element S_∞ (corresponding to the shears point) such that the stabiliser of $\mathcal{S}$ fixes S_∞ pointwise and acts transitively on the elements of $\mathcal{S} \setminus \{S_\infty\}$, and moreover, this property characterises a semifield spread. The next theorem motivates the choice of the term Desarguesian spread.

Theorem 6 ([88]). *A $(t-1)$-spread of $\mathrm{PG}(2t-1,q)$ is Desarguesian if and only if the corresponding translation plane is Desarguesian, i.e. isomorphic to $\mathrm{PG}(2,q^t)$.*

By a method called *derivation* , it is possible to construct a non-Desarguesian translation plane from a Desarguesian plane. This construction can in fact be applied to any translation

plane corresponding to a spread that contains a regulus. A *regulus* in $\mathrm{PG}(3,q)$ is a set of $q+1$ lines that intersect a given set of three two by two disjoint lines (see [28]). Replacing a regulus by its opposite regulus one obtains another spread, and the corresponding new translation plane is called the *derived* plane.

The spread corresponding to a translation plane π can also be constructed algebraically from the coordinatising quasifield, see e.g. [44]. In order to avoid unnecessary generality, we restrict ourselves to the case where π is a semifield plane. In this case there are essentially two approaches one can take, by considering either the endomorphisms L_x or R_x. In the literature it is common to use the endomorphism R_x. We define the following subspaces of $\mathbb{S}\times\mathbb{S}$. For each $x\in\mathbb{S}$, consider the set of vectors $S_x := \{(y,y^{R_x}) : y\in\mathbb{S}\}$, and put $S_\infty := \{(0,y) : y\in\mathbb{S}\}$. It is an easy exercise to show that $\mathcal{S} := \{S_x : x\in\mathbb{S}\}\cup\{S_\infty\}$ is a spread of $\mathbb{S}\times\mathbb{S}$. The set of endomorphisms

$$S := \{R_x \ : \ x\in\mathbb{S}\} \subset \mathrm{End}(V_l(\mathbb{S}))$$

is called the *semifield spread set* corresponding to $\mathbb{S}$. Note that by (S2) the spread set S is closed under addition and, by (S3), the non-zero elements of S are invertible.

More generally, if $\mathcal{S}$ is a t-spread of $\mathbb{F}_q^t\times\mathbb{F}_q^t$, containing $S_0=\{(y,0) : y\in\mathbb{F}_q^t\}$, and $S_\infty = \{(0,y) : y\in\mathbb{F}_q^t\}$, then we can label the elements of $\mathcal{S}$ different from S_∞ as $S_x := \{(y,y^{\phi_x}) : y\in\mathbb{F}_q^t\}$, with $\phi_x\in\mathrm{End}(\mathbb{F}_q^t)$. The set $S := \{\phi_x : x\in\mathbb{F}_q^t\}\subset\mathrm{End}(\mathbb{F}_q^t)$ of endomorphisms is called a *spread set* associated with $\mathcal{S}$. A spread set S is a semifield spread set if it forms an additive subgroup of $\mathrm{End}(\mathbb{F}_q^t)$.

Two spread sets are called *equivalent* if the corresponding spreads are isomorphic. The following theorem is well known, and should probably be credited to Maduram [74]. By lack of a reference containing the exact same statement, we include a short proof.

Theorem 7. *Two semifield spread sets S, $S'\subset\mathrm{End}(\mathbb{F}^t)$ are equivalent if and only if there exist invertible elements $\omega,\psi\in\mathrm{End}(\mathbb{F}^t)$ and $\sigma\in\mathrm{Aut}(\mathbb{F})$ such that $S' = \{\omega R_x^\sigma\psi \ : \ R_x\in S\}$.*

Proof. Using the properties of a semifield spread, we may assume that an equivalence between two semifield spread sets S and S' is induced by an isomorphism β between the corresponding spreads $\mathcal{S}$ and $\mathcal{S}'$ which fixes $S_\infty = S'_\infty$ and $S_0 = S'_0$ with the notation from above. It follows that β is of the form $(x,y)\mapsto(Ax^\sigma,By^\sigma)$, where A,B are elements of $GL(n,q)$ and $\sigma\in\mathrm{Aut}(\mathbb{F}_q)$. Calculating the effect on the elements of the spread set concludes the proof (see e.g. [63, page 908]). □

1.4 Dual and transpose of a semifield, the Knuth orbit

Knuth proved that the action of S_3, defined above, on the indices of the structure constants of a semifield $\mathbb{S}$ is well-defined with respect to the isotopism classes of $\mathbb{S}$, and by the *Knuth orbit of* $\mathbb{S}$ (notation $\mathcal{K}(\mathbb{S})$), we mean the set of isotopism classes corresponding to the S_3-orbit of $\mathbb{S}$, i.e.,

$$\mathcal{K}(\mathbb{S}) = \{[\mathbb{S}],[\mathbb{S}^{(12)}],[\mathbb{S}^{(13)}],[\mathbb{S}^{(23)}],[\mathbb{S}^{(123)}],[\mathbb{S}^{(132)}]\}. \tag{8}$$

The advantage of using Knuth's approach to the coordinatisation with homogeneous coordinates, is that we immediately notice the duality. The semifield corresponding to the dual plane $\pi(\mathbb{S})^d$ of a semifield plane $\pi(\mathbb{S})$ is the plane $\pi(\mathbb{S}^{opp})$, where $\mathbb{S}^{opp}$ is the *opposite algebra* of $\mathbb{S}$

obtained by reversing the multiplication $\circ$, or in other words, the semifield corresponding to the dual plane is $\mathbb{S}^{(12)}$, which we also denote by $\mathbb{S}^d$, i.e.,

$$\mathbb{S}^d = \mathbb{S}^{(12)} = \mathbb{S}^{opp}. \tag{9}$$

Similarly, it is easy to see that the semifield $\mathbb{S}^{(23)}$ can be obtained by transposing the matrices corresponding to the transformations L_{e_i}, $e_i \in \mathbb{S}$, with respect to some basis $\{e_1, e_2, \ldots, e_n\}$ of $V_r(\mathbb{S})$, and for this reason $\mathbb{S}^{(23)}$ is also denoted by $\mathbb{S}^t$, called the *transpose of* $\mathbb{S}$. With this notation, the Knuth orbit becomes

$$\mathcal{K}(\mathbb{S}) = \{[\mathbb{S}], [\mathbb{S}^d], [\mathbb{S}^t], [\mathbb{S}^{dt}], [\mathbb{S}^{td}], [\mathbb{S}^{dtd}]\}. \tag{10}$$

Taking the transpose of a semifield can also be interpreted geometrically as dualising the semifield spread (Maduram [74]). The resulting action on the set of nuclei of the isotopism class $\mathbb{S}$ is as follows. The permutation (12) fixes the middle nucleus and interchanges the left and right nuclei; the permutation (23) fixes the left nucleus and interchanges the middle and right nuclei. Summarising, the action of the dual and transpose generate a series of at most six isotopism classes of semifields, with nuclei according to Figure 1.

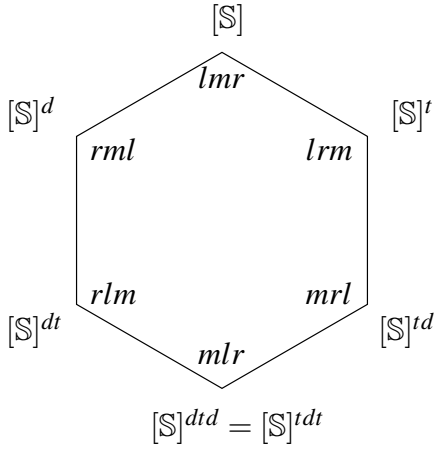

Figure 1: The Knuth orbit of a semifield $\mathbb{S}$ with nuclei lmr

2 Semifields: a geometric approach

In this section, we explain a geometric approach to finite semifields, which has been very fruitful in recent years. In what follows, we consider the set of endomorphisms corresponding to right multiplication in the semifield, and by doing so it is natural to consider the semifield as a left vector space over (a subfield of) its left nucleus. It should be clear to the reader that this is just a matter of choice and the same geometric approach can be taken by considering the set of endomorphisms corresponding to left multiplication in the semifield. The left nucleus should then be replaced by the right nucleus in what follows.

Let $\mathbb{S} = (\mathbb{S}, +, \circ)$ be a finite semifield and let S be the semifield spread set associated with $\mathbb{S}$. Clearly, for any subfield $\mathbb{F} \subset \mathbb{N}_l(\mathbb{S})$, $\mathbb{S}$ is a left vector space over $\mathbb{F}$, and S is also an additive subgroup of $\mathrm{End}(\mathbb{F}^n)$ (if $|\mathbb{S}| = |\mathbb{F}|^n$) by considering R_x as elements of $\mathrm{End}(\mathbb{F}^n)$ instead of $\mathrm{End}(V_l(\mathbb{S}))$. Conversely, any subgroup S of the additive group of $\mathrm{End}(\mathbb{F}^n)$ whose non-zero

elements are invertible defines a semifield $\mathbb{S}$ whose left nucleus contains the field $\mathbb{F}$. If S does not contain the identity map, then S defines a pre–semifield.

This means that semifields, n–dimensional over a subfield $\mathbb{F}_q$ of their left nucleus, can be investigated via the semifield spread sets of $\mathbb{F}_q$–linear maps of $\mathbb{F}_{q^n}$, regarded as a vector space over $\mathbb{F}_q$. An element φ of $\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ can be represented in a unique way as a q–polynomial over $\mathbb{F}_{q^n}$, that is a polynomial of the form

$$\sum_{i=0}^{n-1} a_i X^{q^i} \in \mathbb{F}_{q^n}[X],$$

and φ is invertible if and only if $\det(A) \neq 0$, where

$$A = \begin{pmatrix} a_0 & a_{n-1}^q & a_{n-2}^{q^2} & \dots & a_1^{q^{n-1}} \\ a_1 & a_0^q & a_{n-1}^{q^2} & \dots & a_2^{q^{n-1}} \\ a_2 & a_1^q & a_0^{q^2} & \dots & a_3^{q^{n-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n-1} & a_{n-2}^q & a_{n-3}^{q^2} & \dots & a_0^{q^{n-1}} \end{pmatrix}$$

(see e.g. [67, page 362]).

Hence, any spread set S of linear maps defining a semifield of order q^n can be seen as a set of q^n linearized polynomials, closed with respect to the addition, containing the zero map and satisfying the above mentioned non-singularity condition.

2.1 Linear sets and the Segre variety

Let $\mathbb{M}(n,q)$ denote the n^2-dimensional vector space of all $(n \times n)$-matrices over $\mathbb{F}_q$. The Segre variety $\mathcal{S}_{n,n}$ of the projective space $\mathrm{PG}(\mathbb{M}(n,q),\mathbb{F}_q) = \mathrm{PG}(n^2-1,q)$ is an algebraic variety corresponding to the matrices of $\mathbb{M}(n,q)$ of rank one and the $(n-2)$–th secant variety $\Omega(\mathcal{S}_{n,n})$ of $\mathcal{S}_{n,n}$ is the hypersurface corresponding to the non-invertible matrices of $\mathbb{M}(n,q)$ (also called a *determinantal hypersurface*). There are two systems $\mathcal{R}_1$ and $\mathcal{R}_2$ of maximal subspaces contained in $\mathcal{S}_{n,n}$ and each element of $\mathcal{R}_i$ has dimension $n-1$. If $n=2$, then $\mathcal{S}_{2,2}$ is a hyperbolic quadric $Q^+(3,q)$ of a 3-dimensional projective space and $\mathcal{R}_1$ and $\mathcal{R}_2$ are the reguli of $Q^+(3,q)$.

By the well-known isomorphism between the vector spaces $\mathbb{M}(n,q)$ and $\mathbb{V} = \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$, we have that the elements of $\mathbb{V}$ with kernel of rank $n-1$ correspond to a Segre variety $\mathcal{S}_{n,n}$ of the projective space $\mathrm{PG}(\mathbb{V}) = \mathrm{PG}(n^2-1,q)$ and the non–invertible elements of $\mathbb{V}$ correspond to the $(n-2)$–th secant variety $\Omega(\mathcal{S}_{n,n})$ of $\mathcal{S}_{n,n}$.

Also, the collineations of $\mathrm{PG}(\mathbb{V})$ induced by the semilinear maps

$$\Gamma_{\psi\sigma\omega} : \varphi \mapsto \psi\varphi^\sigma\omega, \tag{11}$$

(where ω and ψ are invertible elements of $\mathbb{V}$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$) form the automorphism group $\mathcal{H}(\mathcal{S}_{n,n})$ of $\mathcal{S}_{n,n}$ preserving the systems $\mathcal{R}_1$ and $\mathcal{R}_2$ of $\mathcal{S}_{n,n}$ (see [41]). The group $\mathcal{H}(\mathcal{S}_{n,n})$ has index two in the stabiliser $\mathcal{G}(\mathcal{S}_{n,n})$ of $\mathcal{S}_{n,n}$ inside $\mathrm{P\Gamma L}(n^2,q)$.

Now, let $\mathbb{S}$ be a semifield and let S be its semifield spread set consisting of $\mathbb{F}_q$–linear maps of $\mathbb{F}_{q^n}$. Since S is an additive subgroup of $\mathbb{V}$, it is an $\mathbb{F}_s$–subspace of $\mathbb{V}$, for some subfield $\mathbb{F}_s$ of $\mathbb{F}_q$ (say $q = s^t$), of dimension nt. This implies that (using the terminology of linear sets from above) $\mathbb{S}$ defines an $\mathbb{F}_s$–linear set $L(\mathbb{S}) := B(S)$ in $\mathrm{PG}(n^2-1,q)$ of rank nt. Note that

$\mathbb{F}_s$ is contained in the center of $\mathbb{S}$. Since each non-zero element of S is invertible, the linear set $L(\mathbb{S})$ is disjoint from the variety $\Omega(\mathcal{S}_{n,n})$ of $\mathrm{PG}(\mathbb{V})$. Conversely, if L is an $\mathbb{F}_s$–linear set of $\mathrm{PG}(\mathbb{V}) = \mathrm{PG}(n^2-1,s^t)$ of rank nt disjoint from $\Omega(\mathcal{S}_{n,n})$, then the set S of $\mathbb{F}_q$–linear maps underlying L satisfies the properties of a semifield spread set except, possibly, the existence of the identity map and hence L defines a pre–semifield of order $q^n = s^{nt}$, whose associated semifield has left nucleus containing $\mathbb{F}_q$ and center containing $\mathbb{F}_s$. So we have the following theorem.

Theorem 8 ([64]). *To any semifield $\mathbb{S}$ of order q^n ($q = s^t$), with left (right) nucleus containing $\mathbb{F}_q$ and center containing $\mathbb{F}_s$, there corresponds an $\mathbb{F}_s$–linear set $L(\mathbb{S})$ of the projective space $\mathrm{PG}(n^2-1,q)$ of rank nt disjoint from the $(n-2)$–th secant variety $\Omega(\mathcal{S}_{n,n})$ of a Segre variety, and conversely.*

Note that, if $\mathbb{F}_q$ is a subfield of the center of the semifield (i.e., if $t = 1$), then the corresponding linear set is simply an $(n-1)$–dimensional subspace of $\mathrm{PG}(n^2-1,q)$. Now, rephrasing Theorem 7, using (11), in the projective space $\mathrm{PG}(\mathbb{V})$ we have the following theorem.

Theorem 9 ([64]). *Two semifields $\mathbb{S}_1$ and $\mathbb{S}_2$ with corresponding $\mathbb{F}_s$–linear sets $L(\mathbb{S}_1)$ and $L(\mathbb{S}_2)$ in $\mathrm{PG}(n^2-1,q)$ are isotopic if and only if there exists a collineation $\Phi \in \mathcal{H}(\mathcal{S}_{n,n})$ such that $L(\mathbb{S}_2) = L(\mathbb{S}_1)^\Phi$.*

By the previous arguments, it is clear that linear sets $L(\mathbb{S}_1)$ and $L(\mathbb{S}_2)$ having a different geometric structure with respect to the collineation group $\mathcal{H}(\mathcal{S}_{n,n})$, determine non–isotopic semifields $\mathbb{S}_1$ and $\mathbb{S}_2$, and hence non–equivalent semifield spread sets S_1 and S_2, and non–isomorphic semifield spreads $\mathcal{S}(\mathbb{S}_1)$ and $\mathcal{S}(\mathbb{S}_2)$. Theorems 8 and 9 can be found in [64]; they generalize previous results obtained in [63], and in [69] and [21] where rank two semifields are studied.

Using the geometric approach, the transpose operation $\mathbb{S} \mapsto \mathbb{S}^t$ can be read in the following way. If τ is any polarity of the projective space $\mathrm{PG}(\mathbb{S}\times\mathbb{S},\mathbb{F}_q)$, then $\mathcal{S}(\mathbb{S})^\tau$ is a semifield spread as well and the corresponding semifield is isotopic to the transpose semifield $\mathbb{S}^t$ of $\mathbb{S}$.

It can be shown that any polarity of $\mathrm{PG}(\mathbb{S}\times\mathbb{S},\mathbb{F}_q)$ fixing the subspaces S_∞ and S_0 induces in $\mathrm{PG}(n^2-1,q)$ a collineation of $\mathcal{G}(\mathcal{S}_{n,n})$ interchanging the systems of $\mathcal{S}_{n,n}$ (see [72]). Hence, since $\mathcal{H}(\mathcal{S}_{n,n})$ has index two in $\mathcal{G}(\mathcal{S}_{n,n})$, by Theorem 9 we have the following.

Theorem 10 ([72]). *If Φ is a collineation of $\mathcal{G}(\mathcal{S}_{n,n})$ not belonging to $\mathcal{H}(\mathcal{S}_{n,n})$ then the linear set $L(\mathbb{S})^\Phi$ corresponds to the isotopism class of the transpose semifield $\mathbb{S}^t$ of $\mathbb{S}$.*

2.2 BEL-construction

In this section we concentrate on a geometric construction of finite semifield spreads. The construction we give here is taken from [64], but the main idea is the slightly less general construction given in [7] (where L is a subspace, i.e. $t = 1$).

We define a *BEL-configuration* as a triple $(\mathcal{D},U,W)$, where $\mathcal{D}$ a Desarguesian $(n-1)$-spread of $\Sigma_1 := \mathrm{PG}(rn-1,s^t)$, $t \geq 1$, $r \geq 2$; U is an nt-dimensional subspace of $\mathbb{F}_s^{rnt}$ such that $L = B(U)$ is an $\mathbb{F}_s$-linear set of Σ_1 of rank nt; and W is a subspace of Σ_1 of dimension $rn-n-1$, such that no element of $\mathcal{D}$ intersects both L and W. From a BEL-configuration one can construct a semifield spread as follows.

- Embed Σ_1 in $\Lambda_1 \cong \mathrm{PG}(rn+n-1,s^t)$ and extend $\mathcal{D}$ to a Desarguesian spread $\mathcal{D}_1$ of Λ_1.

- Let $L' = B(U')$, $U \subset U'$ be an $\mathbb{F}_s$-linear set of Λ_1 of rank $nt+1$ which intersects Σ_1 in L.
- Let $\mathcal{S}(\mathcal{D},U,W)$ be the set of subspaces defined by L' in the quotient geometry $\Lambda_1/W \cong \mathrm{PG}(2n-1,s^t)$ of W, i.e.,

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

Theorem 11 ([64]). *The set $\mathcal{S}(\mathcal{D},U,W)$ is a semifield spread of $\mathrm{PG}(2n-1,s^t)$. Conversely, for every finite semifield spread $\mathcal{S}$, there exists a BEL-configuration $(\mathcal{D},U,W)$, such that $\mathcal{S}(\mathcal{D},U,W) \cong \mathcal{S}$.*

The pre-semifield corresponding to $\mathcal{S}(\mathcal{D},U,W)$ is denoted by $\mathbb{S}(\mathcal{D},U,W)$. Using this BEL-construction it is not difficult to prove the following characterisation of the linear sets corresponding to a finite field.

Theorem 12 ([63]). *The linear set $L(\mathbb{S})$ of $\mathrm{PG}(n^2-1,q)$ disjoint from $\Omega(\mathcal{S}_{n,n})$ corresponds to a pre–semifield isotopic to a field if and only if there exists a Desarguesian $(n-1)$–spread of $\mathrm{PG}(n^2-1,q)$ containing $L(\mathbb{S})$ and a system of $\mathcal{S}_{n,n}$.*

If $r=2$ and $s=1$, then we can use the symmetry in the definition of a BEL-configuration to construct two semifields, namely $\mathbb{S}(\mathcal{D},U,W)$ and $\mathbb{S}(\mathcal{D},W,U)$, and in this way we can extend the Knuth orbit by considering the operation

$$\kappa := \mathbb{S}(\mathcal{D},U,W) \mapsto \mathbb{S}(\mathcal{D},W,U). \tag{12}$$

Except in the case where the semifield is a rank two semifield, in which case κ becomes the translation dual (see Section 4), it is not known whether κ is well defined on the set of isotopism classes (see [7], [54]).

3 Rank two semifields

Semifields of dimension two over (a subfield of) their left nucleus (*rank two semifields*) correspond to semifield spreads of 3–dimensional projective spaces, as explained in Section 1. In the last years, the connection between semifields and linear sets described in Section 2 has been intensively used to construct and characterize families of rank two semifields.

If $\mathbb{S} = (\mathbb{F}_{q^2},+,\circ)$ is a semifield with left nucleus containing $\mathbb{F}_q$ and center containing $\mathbb{F}_s$, $q=s^t$, then by Theorem 8 its semifield spread set S defines an $\mathbb{F}_s$-linear set $L(S)$ of rank $2t$ in the 3-dimensional projective space $\Sigma = \mathrm{PG}(\mathbb{V},\mathbb{F}_q) = \mathrm{PG}(3,q)$, where $\mathbb{V} = \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^2})$, disjoint from the hyperbolic quadric $Q^+(3,q)$ of Σ defined by the non–invertible elements of $\mathbb{V}$, and conversely. Also, by Theorem 9 the study up to isotopy of semifields of order q^2 with left nucleus containing $\mathbb{F}_q$ and center containing $\mathbb{F}_s$ corresponds to the study of $\mathbb{F}_s$-linear sets of rank $2t$ of Σ with respect to the action of the collineation group of Σ fixing the reguli of the hyperbolic quadric $Q^+(3,q)$.

In this case the Knuth orbit of $\mathbb{S}$ can be extended in the following way. If $b(X,Y)$ is the bilinear form associated with $Q^+(3,q)$, then by field reduction we can use the bilinear form

$$b_s(X,Y) := Tr_{q/s}(b(X,Y)),$$

where $Tr_{q/s}$ is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_s$, to obtain another linear set $L(\mathbb{S})^\perp$ disjoint from $Q^+(3,q)$ induced by the semifield spread set

$$S^\perp := \{x \in \mathbb{V} \ : \ b_s(x,y) = 0, \forall y \in \mathbb{V}\}.$$

Theorem 13. *The set $S^\perp$ is a semifield spread set of $\mathbb{F}_q$–linear maps of $\mathbb{F}_{q^2}$.*

The pre–semifield arising from the semifield spread set $S^\perp$ is called the *translation dual* $\mathbb{S}^\perp$ of the semifield $\mathbb{S}$. The translation dual of a rank two semifield has been introduced in [69] in terms of translation ovoids of $Q^+(5,q)$ generalizing the relationship between semifield flocks and translation ovoids of $Q(4,q)$ that will be detailed in Section 5. In [61], it was shown that this operation links the two sets of three semifields associated with a semifield flock from [6], and that this operation is a special case of the semifield operation κ (see (12)) from [7] (see (12) at the end of Section 2). The translation dual operation is well defined on the set of isotopism classes and leaves invariant the sizes of the nuclei of a semifield $\mathbb{S}$, as proven in [71, Theorem 5.3]. This implies that in general $[\mathbb{S}^\perp]$ is not contained in the Knuth orbit $\mathcal{K}(\mathbb{S})$ and hence in the 2–dimensional case we have a chain of possibly twelve isotopism classes $\mathcal{K}(\mathbb{S}) \cup \mathcal{K}(\mathbb{S}^\perp)$, with nuclei as illustrated by Figure 2.

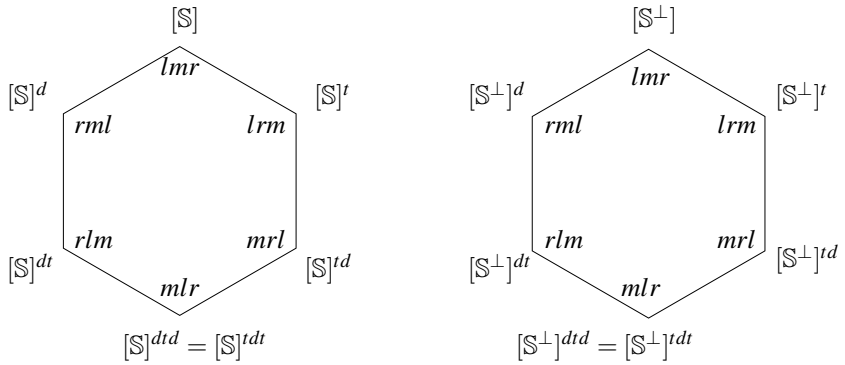

Figure 2: The isotopism classes $\mathcal{K}(\mathbb{S}) \cup \mathcal{K}(\mathbb{S}^\perp)$ of a rank two semifield $\mathbb{S}$ with nuclei *lmr*

To our knowledge, the known examples of semifields $\mathbb{S}$ for which $\mathbb{S}^\perp$ is not isotopic to $\mathbb{S}$ are: the symplectic semifield of order $q = 3^{2t}$ ($t > 2$) from Cohen-Ganley [23], and Thas-Payne [92], the symplectic semifield of order 3^{10} from Penttila–Williams [84], the HMO–semifields of order q^4 (for $q = p^k$, k odd, $k \geq 3$ and p prime with $p \equiv 1 \pmod 4$) exhibited in [54, Example 5.8] and their translation duals. But, in all of these cases, the size of $\mathcal{K}(\mathbb{S}) \cup \mathcal{K}(\mathbb{S}^\perp)$ is six, since these are self-transpose semifields, i.e. $[\mathbb{S}] = [\mathbb{S}^t]$.

Using the geometric approach from Section 2, in [21], the authors classify all semifields of order q^4 with left nucleus of order q^2 and center of order q (see Theorem 26).

In [75], [48] and [34], semifields of order q^6, with left nucleus of order q^3 and center of order q, are studied using the same geometric approach, giving the following result.

Theorem 14 ([75], [48])**.** *Let $\mathbb{S}$ be a semifield of order q^6 with left nucleus of order q^3 and center of order q. Then there are eight possible geometric configurations for the corresponding linear set $L(\mathbb{S})$ in* $\mathrm{PG}(3,q^3)$*. The corresponding classes of semifields are partitioned into eight non-isotopic families, labeled $\mathcal{F}_0$, $\mathcal{F}_1$, $\mathcal{F}_2$, $\mathcal{F}_3$, $\mathcal{F}_4^{(a)}$, $\mathcal{F}_4^{(b)}$, $\mathcal{F}_4^{(c)}$ and $\mathcal{F}_5$.*

The families $\mathcal{F}_i$, $i = 0,1,2$, are completely characterized: the family $\mathcal{F}_0$ contains only Generalized Dickson/Knuth semifields with the given parameters; the family $\mathcal{F}_1$ contains only the symplectic semifield associated with the Payne–Thas ovoid of $Q^+(4,3^3)$; the family $\mathcal{F}_2$ contains only the semifield associated with the Ganley flock of the quadratic cone of $\mathrm{PG}(3,3^3)$.

So far, only few examples of semifields belonging to $\mathcal{F}_3$ and $\mathcal{F}_4^{(b)}$ are known for small values of q. These were obtained by using a computer algebra software package.

A further investigation of families $\mathcal{F}_4^{(a)}$ and $\mathcal{F}_4^{(c)}$ led to the construction of new infinite families of semifields (Section 6, EMPT2 semifields).

Moreover, all semifields of order q^6 with left nucleus of order q^3, right and middle nuclei of order q^2, and center of order q fall in family $\mathcal{F}_4^{(c)}$ and they are completely classified (see Section 6, Theorem 27).

Finally, semifields belonging to the family $\mathcal{F}_5$ are called *scattered semifields* , because their associated linear sets are of maximum size $q^5+q^4+\cdots+q+1$, i.e., are scattered following [14]. In [75], it has been proved that to any semifield $\mathbb{S}$ belonging to $\mathcal{F}_5$ is associated an $\mathbb{F}_q$*–pseudoregulus* $\mathcal{L}(\mathbb{S})$ of $\mathrm{PG}(3,q^3)$, which is a set of q^3+1 pairwise disjoint lines with exactly two transversal lines. An $\mathbb{F}_q$-pseudoregulus of $\mathrm{PG}(3,q^3)$ defines a *derivation set* in a similar way as the pseudoregulus of $\mathrm{PG}(3,q^2)$ defined by Freeman [37]. The known examples of semifields belonging to the family $\mathcal{F}_5$ are the Generalized twisted fields and the two families of Knuth semifields of type III and IV with the involved parameters. In [75], they are also characterized in terms of the associated $\mathbb{F}_q$–pseudoreguli. Precisely, in the case of Knuth semifields the transversal lines of the associated pseudoregulus are contained in a regulus of $Q^+(3,q)$; whereas in the case of Generalized twisted fields the transversal lines of the associated pseudoregulus are pairwise polar external lines of $Q^+(3,q)$ and the set of lines of the pseudoregulus is preserved by the polarity $\perp$ induced by $Q^+(3,q)$.

Recent results obtained in [65] have shown that various other possible geometric configurations of the transversal lines of a pseudoregulus of $\mathrm{PG}(3,q^3)$ can produce new semifields in family $\mathcal{F}_5$.

The results obtained in the case q^6 inspired a more general construction method that led to the discovery of new infinite families of rank two semifields of size q^{2t} for arbitrary values of q and t (see Section 6, EMPT1 semifields).

Some other existence and classification results for rank two semifields obtained by the geometric approach of linear sets can be found in [49], [76] and [77].

4 Symplectic semifields and commutative semifields

A semifield spread $\mathcal{S}$ of the projective space $\mathrm{PG}(2n-1,q)$ is *symplectic* when all subspaces of $\mathcal{S}$ are totally isotropic with respect to a symplectic polarity of $\mathrm{PG}(2n-1,q)$.

Starting from a semifield $\mathbb{S}$, we can construct a family of semifield spreads; precisely, we can associate to $\mathbb{S}$ a semifield spread $\mathcal{S}_{\mathbb{F}}$ for any subfield $\mathbb{F}$ of its left nucleus (see Section 1.3). By [53] and [70], if $\mathcal{S}_{\mathbb{F}}$ is a symplectic semifield spread then any other semifield spread arising from $\mathbb{S}$ is symplectic. Hence, it makes sense to define a *symplectic semifield* as a semifield whose associated semifield spread is symplectic.

In terms of the associated linear set, a symplectic semifield can be characterized in the following way.

Theorem 15 ([72]). *The semifield $\mathbb{S}$ with corresponding linear set $L(\mathbb{S})$ in $\mathrm{PG}(\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n}))$ is symplectic if and only if there is a subspace Γ of $\mathrm{PG}(\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n}))$ of dimension $\frac{n(n+1)}{2}-1$ such that $\Gamma \cap \mathcal{S}_{n,n}$ is a quadric Veronesean and $L(\mathbb{S}) \subset \Gamma$.*

Symplectic semifields and commutative semifields are related via the S_3-action in the following way.

Theorem 16 ([52]). *A pre–semifield $\mathbb{S}$ is isotopic to a commutative semifield if and only if the pre–semifield $\mathbb{S}^{td}$ is symplectic.*

It follows from the above that the Knuth orbit $\mathcal{K}(\mathbb{S})$ of a symplectic semifield consists of the isotopism classes $\{[\mathbb{S}] = [\mathbb{S}^t], [\mathbb{S}^d] = [\mathbb{S}^{td}], [\mathbb{S}^{dt}] = [\mathbb{S}^{tdt}]\}$ (see Figure 3).

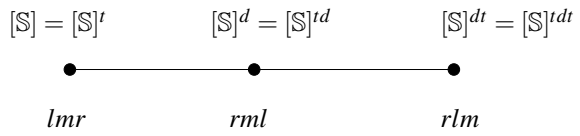

Figure 3: The Knuth orbit $\mathcal{K}(\mathbb{S})$ of a symplectic semifield $\mathbb{S}$ with nuclei *lmr*

Using this connection, in [52], a large number of commutative semifields of even order are constructed starting from the symplectic *semifield scions of the Desarguesian spreads*. These spreads were introduced and investigated in [56]. There the study of symplectic semifield spreads in characteristic 2 having odd dimension over $\mathbb{F}_2$ was motivated by their connections with extremal $\mathbb{Z}_4$-linear codes and extremal line sets in Euclidean spaces (see [20]).

In odd characteristic, commutative pre–semifields are related to the notion of planar DO polynomial. A *Dembowski-Ostrom (DO) polynomial* $f \in \mathbb{F}_q[x]$ ($q = p^e$) is a polynomial of the shape

$$f(x) = \sum_{i,j=0}^{k} a_{ij} x^{p^i+p^j};$$

whereas a polynomial $f \in \mathbb{F}_q[x]$ is *planar* or *perfect nonlinear (PN for short)* if the difference polynomial $f(x+a)-f(x)-f(a)$ is a permutation polynomial for each $a \in \mathbb{F}_q^*$. If $f(x) \in \mathbb{F}_q[x]$, q odd, is a planar DO polynomial, then $\mathbb{S}_f = (\mathbb{F}_q, +, \circ)$ is a commutative pre–semifield with multiplication $\circ$ defined by $a \circ b = f(a+b) - f(a) - f(b)$. Conversely, if $\mathbb{S} = (\mathbb{F}_q, +, \circ)$ is a commutative pre–semifield of odd order, then the polynomial given by $f(x) = \frac{1}{2}(x \circ x)$ is a planar DO polynomial and $\mathbb{S} = \mathbb{S}_f$ (see [25], and [27]).

Perfect nonlinear functions are differentially 1-uniform functions and they are of special interest in differential cryptanalysis (see [12], [80]).

For the known examples of symplectic or commutative (pre)semifields, see semifields of type D, A, K, G, CG/TP, CM-DY, PW/BLP, KW/K, CHK, BH, ZKW, Bi and LMPT listed in Section 6.

5 Rank two commutative semifields

In this section, we turn our attention to commutative semifields that are of rank at most two over their middle nucleus, which we will call *rank two commutative semifields* or *RTCS* for short. Note that with this definition, finite fields are examples of RTCS. These semifields deserve special attention because of their importance in Galois geometry. They are connected to many of the central objects in the field, such as flocks of a quadratic cone, translation generalized quadrangles, ovoids, eggs, ... see e.g. [8].

As seen in the previous section, commutative semifields are linked with symplectic semifields, and the study of RTCS is equivalent to the study of symplectic semifields that are of rank two over their left nucleus. Figure 4 diplays the six isotopism classes corresponding to a RTCS, consisting of two Knuth orbits (see [6] and [61] for more details).

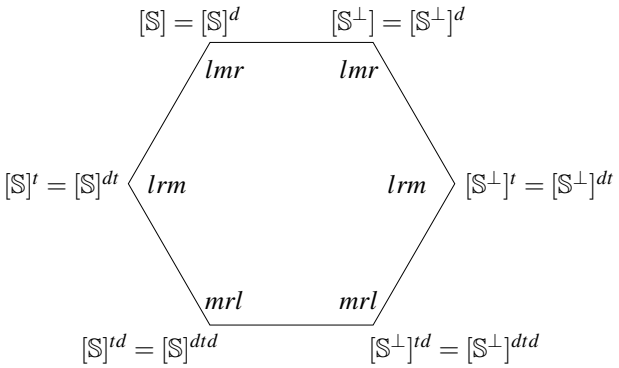

Figure 4: The isotopism classes $\mathcal{K}(\mathbb{S}) \cup \mathcal{K}(\mathbb{S}^\perp)$ corresponding to a RTCS $\mathbb{S}$ with nuclei *lmr*

Rewriting the example (2) from Dickson [31], we have the following construction of an RTCS. Let σ be an automorphism of $\mathbb{F}_q$, q odd, and define the following multiplication on $\mathbb{F}_q^2$:

$$(x,y) \circ (u,v) = (xv + yu, yv + mx^\sigma u^\sigma), \tag{13}$$

where m is a non-square in $\mathbb{F}_q$. Cohen and Ganley made significant progress in the investigation of RTCS. They put Dickson's construction in the following more general setting. Let $\mathbb{S}$ be an RTCS of order q^2 with middle nucleus $\mathbb{F}_q$, and let $\alpha \in \mathbb{S} \setminus \mathbb{F}_q$ be such that $\{1, \alpha\}$ is a basis for $\mathbb{S}$. Addition in $\mathbb{S}$ is component-wise and multiplication is defined as

$$(x,y) \circ (u,v) = (xv + yu + g(xu), yv + f(xu)), \tag{14}$$

where f and g are additive functions from $\mathbb{F}_q$ to $\mathbb{F}_q$, such that $x\alpha^2 = g(x)\alpha + f(x)$. We denote this semifield by $\mathbb{S}(f,g)$. Verifying that this multiplication has no zero divisors leads to the following theorem which comes from [23].

Theorem 17. *Let $\mathbb{S}$ be a RTCS of order q^2 and characteristic p. Then there exist $\mathbb{F}_p$-linear functions f and g such that $\mathbb{S} = \mathbb{S}(f,g)$, with multiplication as in (14) and such that $zw^2 + g(z)w - f(z) = 0$ has no solutions for all w, $z \in \mathbb{F}_q$, and $z \neq 0$.*

For q even, Cohen and Ganley obtained the following remarkable theorem proving the non-existence of proper RTCS in even characteristic. To our knowledge, there is no obvious geometric reason why this should be so.

Theorem 18 ([23]). *For q even the only RTCS of order q^2 is the finite field $\mathbb{F}_{q^2}$.*

If q is odd, then the quadratic $zw^2+g(z)w-f(z)=0$ in w will have no solutions in $\mathbb{F}_q$ if and only if $g(z)^2+4zf(z)$ is a non-square for all $z\in\mathbb{F}_q^*$. In [23], Cohen and Ganley prove that in odd characteristic, in addition to the example with multiplication (13) by Dickson, there is just one other infinite family of proper RTCS, namely of order 3^{2r}, with multiplication given by:

$$(x,y)\circ(u,v)=(xv+yu+x^3u^3, yv+\eta x^9u^9+\eta^{-1}xu), \tag{15}$$

with η a non-square in $\mathbb{F}_{3^r}$ ($r\geq 2$).

Theorem 19 ([23]). *Suppose that f and g are linear polynomials of degree less than q over $\mathbb{F}_q$, q odd, such that for infinitely many extensions $\mathbb{F}_{q^e}$ of $\mathbb{F}_q$, the functions*

$$f^*:\mathbb{F}_{q^e}\to\mathbb{F}_{q^e}\ :\ x\mapsto f(x), \text{ and}$$

$$g^*:\mathbb{F}_{q^e}\to\mathbb{F}_{q^e}\ :\ x\mapsto g(x),$$

define an RTCS $\mathbb{S}(f^*,g^*)$ of order q^{2e}. Then $\mathbb{S}(f,g)$ is a semifield with multiplication given by (13) or (15), or $\mathbb{S}(f,g)$ is a field.

The only other example of an RTCS was constructed from a translation ovoid of $Q(4,3^5)$, first found by computer in 1999 by Penttila and Williams ([84]). The associated semifield has order 3^{10} and multiplication

$$(x,y)\circ(u,v)=(xv+yu+x^{27}u^{27}, yv+x^9u^9). \tag{16}$$

Summarising, the only known examples of RTCS which are not fields are of *Dickson type* (13), of *Cohen-Ganley type* (15), or of *Penttila-Williams type* (16).

The existence of RTCS was further examined in [15] and [62] obtaining the following theorems which show that there is little room for further examples.

Theorem 20 ([62]). *Let $\mathbb{S}$ be an RTCS of order p^{2n}, p an odd prime. If $p>2n^2-(4-2\sqrt{3})n+(3-2\sqrt{3})$, then $\mathbb{S}$ is either a field or a RTCS of Dickson type.*

Theorem 21 ([15]). *Let $\mathbb{S}$ be an RTCS of order q^{2n}, q an odd prime power, with center $\mathbb{F}_q$. If $q\geq 4n^2-8n+2$, then $\mathbb{S}$ is either a field or a RTCS of Dickson type.*

In combination with a computational result by Bloemen, Thas, and Van Maldeghem [13], the above implies a complete classification of RTCS of order q^6, with centre of order q.

Theorem 22 ([15]). *Let $\mathbb{S}$ be an RTCS of order q^6 with centre of order q, then either $\mathbb{S}$ is a field, or q is odd and $\mathbb{S}$ is of Dickson type.*

We end this section with the connections between RTCS and some interesting objects in Galois geometry.

5.1 Translation generalized quadrangles and eggs

Let $\mathbb{S}(f,g)$ be an RTCS of order q^{2n} such that f and g are $\mathbb{F}_q$-linear, and for $(a,b) \in \mathbb{F}_{q^n}^2$ define

$$g_t(a,b) := a^2 t + g(t)ab - f(t)b^2. \tag{17}$$

Then the set $\mathcal{E}(f,g) := \{E(a,b) \ : \ a,b \in \mathbb{F}_{q^n}\} \cup \{E(\infty)\}$, with

$$E(a,b) := \{\langle (t, -g_t(a,b), -2at - bg(t), ag(t) - 2bf(t))\rangle \ : \ t \in \mathbb{F}_{q^n}^*\} \tag{18}$$

$$\text{and } E(\infty) := \{\langle (0,t,0,0)\rangle \ : \ t \in \mathbb{F}_{q^n}^*\}, \tag{19}$$

is a set of $q^{2n}+1$ $(n-1)$-dimensional subspaces of $\mathrm{PG}(4n-1,q)$ satisfying the following properties:

(E1) each three different elements of $\mathcal{E}(f,g)$ span a $(3n-1)$-dimensional subspace of $\mathrm{PG}(4n-1,q)$;

(E2) each element of $\mathcal{E}(f,g)$ is contained in a $(3n-1)$-dimensional subspace of $\mathrm{PG}(4n-1,q)$ that is disjoint from the other elements of $\mathcal{E}(f,g)$.

Such a set of $q^{2n}+1$ $(n-1)$-dimensional subspaces in $\mathrm{PG}(4n-1,q)$, satisfying (E1) and (E2) is called a *pseudo-ovoid*, *generalized ovoid*, or *egg* of $\mathrm{PG}(4n-1,q)$. These notions can be defined in more generality and were first studied in [89]. A more recent reference containing the general definition is [59]. Analogously to the relationship between planar spreads and translation planes, there is a one-to-one correspondence between eggs and translation generalized quadrangles (TGQ) (see [83]). It is far beyond the scope of this article to give a complete overview of the theory of eggs and TGQ here, and we refer the reader to [59], [83], or [93] for more details. However, we do want to mention the remarkable fact that all known examples of eggs (and hence of TGQ) are either obtained by field reduction from an ovoid or an oval, or they arise from an RTCS, i.e., they correspond to an egg $\mathcal{E}(f,g)$ (or its dual) constructed from an RTCS $\mathbb{S}(f,g)$ as above (see [59, Section 3.8] for more details).

5.2 Semifield flocks and translation ovoids

A *flock of a quadratic cone* $\mathcal{K}$ of $\mathrm{PG}(3,q)$ with vertex v is a partition of $\mathcal{K} \setminus \{v\}$ into irreducible conics. The planes containing the conics of the flock are called the *planes of the flock*. In [90], Thas shows that a flock of a quadratic cone coexists with a set of upper triangular two by two matrices (sometimes called a *q-clan*) for which the difference of any two matrices is anisotropic, i.e. $v(A-B)v^t = 0$ implies $v = 0$ for $A \neq B$. Previous work, by Kantor [51] and Payne [81] [82], shows that such a set of two by two matrices gives rise to a generalized quadrangle of order (q^2,q).

If $\mathcal{K}$ is the quadratic cone in $\mathrm{PG}(3,q^n)$, q odd, with vertex $v = (0,0,0,1)$ and base the conic $\mathcal{C}$ with equation $X_0X_1 - X_2^2 = 0$ in the plane $X_3 = 0$, then the planes of a flock of $\mathcal{K}$ may be written as

$$\pi_t : tX_0 - f(t)X_1 + g(t)X_2 + X_3 = 0, \ t \in \mathbb{F}_{q^n}, \tag{20}$$

for some $f, g : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$. We denote this flock by $\mathcal{F}(f,g)$. The associated set of two by two matrices consists of the matrices

$$\begin{pmatrix} t & g(t) \\ 0 & -f(t) \end{pmatrix}, t \in \mathbb{F}_{q^n}. \tag{21}$$

If f and g are linear over a subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^n}$, then $\mathcal{F}(f,g)$ is called a *semifield flock* . Using Theorem 17 and the above, one may conclude that $\mathcal{F}(f,g)$ is a semifield flock if and only if $\mathbb{S}(f,g)$ is an RTCS.

Another well studied object in Galois geometry connected to RTCS are translation ovoids of the generalized quadrangle $Q(4,q)$, consisting of points and lines that are contained in the projective algebraic variety $V(X_0X_1 - X_2^2 + X_3X_4)$ in PG$(4,q)$. An *ovoid* of $Q(4,q)$ is a set Ω of points such that each line of $Q(4,q)$ contains exactly one point of Ω. An ovoid Ω is called a *translation ovoid* if there exists a group H of automorphisms of $Q(4,q)$, fixing Ω, a point $x \in \Omega$ and every line through x, acting transitively on the points of Ω not collinear with x. The correspondence between semifield flocks and translation ovoids of $Q(4,q)$ was first explained by Thas in [91], and later by Lunardon [68] with more details. The explicit calculations of what follows can be found in [60, Section 3]. Let $\mathbb{S}(f,g)$ be an RTCS of order q^{2n}, with f and g $\mathbb{F}_q$-linear, i.e. there exist $b_i, c_i \in \mathbb{F}_{q^n}$ such that $g(t) = \sum b_i t^{q^i}$, and $f(t) = \sum c_i t^{q^i}$. The corresponding ovoid $\Omega(f,g)$ of $Q(4,q^n)$ is then given by the set of points

$$\{(u, F(u,v), v, 1, v^2 - uF(u,v)) \ : \ (u,v) \in \mathbb{F}_{q^n}^2\} \cup \{(0,0,0,0,1)\},$$

with

$$F(u,v) = \sum_{i=0}^{n-1} (c_i u + b_i v)^{1/q^i}.$$

6 Known examples and classification results

In this section, we list the known finite non-associative semifields and some of the known classification results.

In the sequel, p and q will denote a prime and a prime power, respectively. Also, we will say that a semifield $\mathbb{S}'$ is a *Knuth derivative* of a semifield $\mathbb{S}$ if the isotopism class $[\mathbb{S}']$ of $\mathbb{S}'$ belongs to the Knuth orbit of $\mathbb{S}$. Recall that, by Theorem 16, a pre-semifield $\mathbb{S}$ is isotopic to a commutative semifield if and only if its Knuth derivative $\mathbb{S}^{td}$ is symplectic.

1. (**D**) *Dickson commutative semifields* of order p^{2e} with p odd and $e > 1$ [32].
2. (**HK**) *Hughes–Kleinfeld semifields* of order p^{2e} with $e > 1$ [43].
3. (**A**) *Albert Generalized twisted fields* of order q^n with center of order q ($q > 2$ and $n > 2$) [2]. For q odd some Generalized twisted fields are symplectic [4] and their Knuth commutative derivatives are Generalized twisted fields as well. Indeed, the family of the Generalized twisted fields is closed under the Knuth operations (see [52]).
4. (**S**) *Sandler semifields* of order q^{mn} with center of order q and $1 < n \leq m$ [87].

5. (**K**) In [58], Knuth generalizes the Dickson commutative semifields ([58, (7.16)] *Generalized Dickson semifields*) and constructs four types of semifields: *families I, II, III, and IV* of order p^{2e}, with $e > 1$ [58, (7.17)]; semifields of type II are Hughes-Kleinfeld semifields and families II, III and IV belong to the same Knuth orbit (see [9]). Some Generalized Dickson semifields are symplectic semifields (see [50]) and their commutative Knuth derivatives are Dickson semifields (see [52]). In the same paper Knuth also provides a family of commutative semifields of order 2^{mn}, n odd and $mn > 3$: the *Knuth binary semifields* [58, (6.10)].

6. (**G**) *Ganley commutative semifields* [38] of order 3^{2r}, with $r \geq 3$ odd, and their symplectic Knuth derivatives [52, (5.14)].

7. (**CG**/**TP**) *Cohen–Ganley commutative semifields* of order 3^{2r}, $r \geq 2$ [23, Example 3], their symplectic derivatives (*Thas–Payne symplectic semifields*) and the corresponding semifields associated with a flock [92].

8. (**BL**) *Boerner-Lantz semifield* of order 81 [16].

9. (**JJ**) *Jha–Johnson cyclic semifields of type* (q,m,n), of order q^l where $l = \mathrm{lcm}(n,m)$, $m,n > 1$ and $l > \max\{m,n\}$ [45, Theorem 2]. Jha–Johnson cyclic semifields generalize the Sandler semifields.

10. (**HJ**) *Huang–Johnson semifields*: 7 non-isotopic semifields of order 8^2 (classes II, III, ...,VIII) [42].

11. (**CM** $-$ **DY**) *Coulter–Matthews/Ding–Yuang commutative pre–semifields* of order 3^n, $n > 1$ odd [27], [33], and their symplectic Knuth derivatives (see [52]).

12. (**PW**/**BLP**) *Penttila–Williams symplectic semifield* of order 3^{10} [84], its commutative Knuth derivative and the related *Bader-Lunardon-Pinneri semifield* associated with a flock [5].

13. (**KW**/**K**) *Kantor–Williams symplectic pre-semifields* of order q^m, for q even and $m > 1$ odd [56], and their commutative Knuth derivatives (*Kantor commutative pre-semifields*) [52, (4.2)]. Kantor commutative pre-semifields generalize the Knuth binary semifields.

14. (**CHK**) *Coulter–Henderson–Kosick commutative pre–semifield* of order 3^8 [26].

15. (**CF**) *Cordero–Figueroa semifield* of order 3^6 [47, 37.10].

16. (**De**) *Dempwolff semifields* of order 3^4 [30]. The author in [30] completes the classification of semifields of order 81 and determines 4 Knuth orbits of semifields not previously known (classes I, II, III and V). He also discusses the embedding of semifields of type III and V in an infinite series.

17. (**BH**) *Budaghyan–Helleseth commutative pre-semifields* $\mathbb{B}_{s,k}$ of order p^{2k}, p odd, constructed from PN DO–polynomials of type (i*) with s and k integers such that $0 < s < 2k$, $\gcd(p^s+1, p^k+1) \neq \gcd(p^s+1, (p^k+1)/2)$ and $\gcd(k+s, 2k) = \gcd(k+s, k)$; and of type (i**) with s and k integers such that $0 < s < 2k$ and $\gcd(k+s, 2k) = \gcd(k+s, k)$ [19].

18. (**MPT**) *Marino–Polverino–Trombetti semifields*: 4 non-isotopic semifields of order 2^{14} [76, Theorem 5.3].

19. (**JMPT**) *Johnson–Marino–Polverino–Trombetti semifields* of order q^{2n} with $n > 1$ odd [49, Theorem 1]. JMPT semifields generalize the Jha–Johnson cyclic semifields of type $(q,2,n)$, n odd. Also, the Huang–Johnson semifield of class VI belongs to this family.

20. (**JMPT**$(\mathbf{4^5},\mathbf{16^5})$) *Johnson–Marino–Polverino–Trombetti non-cyclic semifields* of order 4^5 and order 16^5 [49, Theorem 7].

21. (**ZKW**) *Zha–Kyureghyan–Wang commutative pre-semifields* $\mathbb{Z}_{s,k}$ of order p^{3k}, p odd where s and k are integers such that $\gcd(3,k)=1$, $0<s<3k$, $k\equiv s \pmod 3$, $k\neq s$ and $\frac{3k}{\gcd(s,3k)}$ odd, constructed in [95] from PN DO–polynomials.

22. (**EMPT2**) *Ebert–Marino–Polverino–Trombetti semifields* of order q^6 for q odd [36, Theorems 2.7, 2.8].

23. (**EMPT1**) *Ebert–Marino–Polverino–Trombetti semifields* of order q^{2n} with either $n\geq 3$ odd, or $n>2$ even and q odd [35, Theorem 1.1]. The Huang–Johnson semifields of type VII and VIII belong to this family.

24. (**MT**) *Marino–Trombetti semifield* of order 2^{10} [77].

25. (**Bi**) *Bierbrauer commutative pre-semifields* from PN DO–polynomials [10] and [11].

26. (**RCR**) *Rúa–Combarro–Ranilla semifields* of order 2^6 [86]. The authors in [86] classify all semifields of order 64 and determine 67 Knuth orbits of semifields with 64 elements not previously known.

27. (**LaMPT**) *Lavrauw–Marino–Polverino–Trombetti rank two scattered semifields* of order q^6 for q odd, $q\equiv 1 \pmod 3$ and for $q=2^{2h}$, $h\equiv 1 \pmod 3$ from [65]. These semifields belong to family $\mathcal{F}_5$.

28. (**LuMPT**) *Lunardon–Marino–Polverino–Trombetti* symplectic semifields of order q^6 for q odd, and their commutative Knuth derivatives [72].

Apart from the Knuth cubical array (see Section 1), the translation dual construction and the BEL geometric model (see Section 2), some other "construction processes" are known to produce semifields starting from a given one: the *lifting construction* (or *HMO construction*) and the *symplectic dual construction*.

The lifting construction produces semifields of order q^4 with left nucleus of order q^2 starting from rank two semifields of order q^2. Note that this process may be iterated producing semifields of order q^{2^i} for any integer $i\geq 2$. Also, the lifting construction is not closed under the isotopy relation, indeed isotopic semifields can produce non-isotopic lifted semifields. This construction method has been introduced by Hiramine, Matsumoto and Oyama in [40], for q odd, and then generalized by Johnson in [46] for any value of q. Semifields lifted from a field are completely determined (see [16], [24] and [21]). For further details on lifting see e.g. [47, Chapter 93] and [54].

The symplectic dual construction has been recently introduced in [72] and produces a symplectic semifield of order q^3 (q odd) with left nucleus containing $\mathbb{F}_q$ starting from a symplectic semifield $\mathbb{S}$ with the same data. As the translation dual construction, the symplectic dual construction is an involutary operation, (i.e., if $\mathbb{S}^\tau$ denotes the symplectic dual of the semifield $\mathbb{S}$, then $(\mathbb{S}^\tau)^\tau=\mathbb{S}$). Indeed the symplectic dual of a semifield is obtained by dualizing the associated linear set with respect to a suitable polarity.

6.1 Classification results for any q

We have already seen that all two-dimensional finite semifields are fields. In 1977, G. Menichetti classified all three-dimensional finite semifields proving the following result.

Theorem 23 ([78]). *A semifield of order q^3 with center containing $\mathbb{F}_q$ either is a field or is isotopic to a Generalized twisted field.*

Later on Menichetti generalized the previous result proving the following theorem.

Theorem 24 ([79]). *Let $\mathbb{S}$ be a semifield of prime dimension n over the center $\mathbb{F}_q$. Then there exists an integer $\nu(n)$ depending only on n, such that if $q > \nu(n)$ then $\mathbb{S}$ is isotopic to a Generalized twisted field.*

As a corollary we have that *a semifield of order p^3 is a field or a Generalized twisted field* and that *a semifield of order p^n, n prime, if p is "large enough", is a field or a Generalized twisted field.*

All the other classification results for semifields of given order involve conditions on one or more of their nuclei. In fact, all of them deal with rank two semifields.

The first result in this direction is the following theorem that can be found in [43] (case (a)) and in [58, Theorem 7.4.1].

Theorem 25. *Let $\mathbb{S}$ be a semifield which is not a field and which is a 2-dimensional vector space over a finite field $\mathbb{F}$. Then*
(a) *$\mathbb{F} = \mathbb{N}_r = \mathbb{N}_m$ if and only if $\mathbb{S}$ is a Knuth semifield of type II.*
(b) *$\mathbb{F} = \mathbb{N}_l = \mathbb{N}_m$ if and only if $\mathbb{S}$ is a Knuth semifield of type III.*
(c) *$\mathbb{F} = \mathbb{N}_l = \mathbb{N}_r$ if and only if $\mathbb{S}$ is a Knuth semifield of type IV.*

More recently, using the geometric approach of the linear sets the following results for rank two semifields of order q^4 and q^6 have been obtained in [21] and [49], respectively.

Theorem 26 ([21]). *A semifield $\mathbb{S}$ of order q^4 with left nucleus $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$ is isotopic to one of the following semifields: Generalized Dickson/Knuth semifields (q odd), Hughes-Kleinfeld semifields, semifields lifted from Desarguesian planes or Generalized twisted fields.*

Theorem 27 ([49]). *Each semifield $\mathbb{S}$ of order q^6, with left nucleus of order q^3 and middle and right nuclei of order q^2 and center of order q is isotopic to a JMPT semifield, precisely $\mathbb{S}$ is isotopic to a semifield $(\mathbb{F}_{q^6}, +, \circ)$ with multiplication given by*

$$x \circ y = (\alpha + \beta u)x + b\gamma x^{q^3}, \ \text{where} \ \ y = \alpha + \beta u + \gamma b \ (\alpha, \beta, \gamma \in \mathbb{F}_{q^2}),$$

with u a fixed element of $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and b an element of $\mathbb{F}_{q^6}$ such that $b^{q^3+1} = u$.

Finally, for classification results concerning rank two commutative semifields (RTCS) we refer to Section 5.

6.2 Classification results for small values of q

All semifields of order $q \leq 125$ are classified. By [58, Theorem 6.1], a non-associative semifield has order p^n, where $n \geq 3$ and $p^n \geq 16$, and by Menichetti's classification result (Theorem 23), semifields of order 27 and 125 are fields or Generalized twisted fields.

Semifields of order 16 and order 32 have been classified in the sixties; those of order 16 form three isotopism classes (see [57]) and those of order 32 form six isotopism classes (see [94]).

Recently in [30] with the aid of the computer algebra software package GAP, Dempwolff has completed the classification of semifields of order 81 proving that there are 27 non-isotopic semifields with 81 elements, partitioned into 12 Knuth orbits.

Finally, in [86], Rúa, Combarro and Ranilla have obtained a computer assisted classification of all semifields of order 64. They have determined 332 non-isotopic semifields with 64 elements, partitioned into 80 Knuth orbits.

7 Open Problems

We conclude this overview of finite semifields with some open problems, at least one problem from every section.

In this article we have encountered a number of different invariants of the isotopism classes of finite semifields, such as the size of semifield, and the size of its nuclei, or the characteristic. Of course, since the isotopism classes for semifields correspond to the isomorphism classes of the corresponding semifield planes, each invariant of the isomorphism classes of projective planes (e.g. the *fingerprint*, *Kennzahl*, *Leitzahl* defined in [22] and [29]) serves as an invariant of the isotopism class of semifields. However, these invariants can sometimes only be computed for semifields of small order, and it often remains very difficult to determine whether a semifield is "new" or not, where "new" means not isotopic to a semifield that was already known before. Moreover, these invariants are perhaps too general, as they apply to general translation planes and not just to semifield planes. As we saw in this article, the geometric approach can sometimes be used in order to distinguishing between isotopism classes of semifield, but there is still no guarantee that different isotopism classes are represented by linear sets that are distinguishable by their geometric properties. This leads us to the following problem.

Problem 1 (Section 1) Find new invariants of isotopism classes of finite semifields, or even better: find a unique representative for each isotopism class.

The following two problems are related to the geometric construction for semifields (from [7]) explained in Section 2.

Problem 2 (Section 2) Find examples of semifields $\mathbb{S}$ that are not 2-dimensional over their left nucleus, having $r = 2$ (r is the integer in the BEL-construction), and such that the semifield $\mathbb{S}^\kappa$ is new.

Problem 3 (Section 2) Does the operation κ that interchanges U and W extend to an operation on the isotopism classes, and if so, how many isotopism classes of semifields does this operation produce in conjunction with the Knuth orbit?

The following problem is also related to the Knuth orbit. As pointed out in Section 3, all known examples of rank two semifields $\mathbb{S}$ for which $\mathbb{S}^\perp$ is not isotopic to $\mathbb{S}$ have the property that the size of $\mathcal{K}(\mathbb{S}) \cup \mathcal{K}(\mathbb{S}^\perp)$ is six.

Problem 4 (Section 3) Find examples of rank two semifields $\mathbb{S}$ for which the set of isotopism classes $\mathcal{K}(\mathbb{S}) \cup \mathcal{K}(\mathbb{S}^\perp)$ has size twelve.

Theorem 15 gives a characterisation of symplectic semifields, which in combination with Theorem 16 gives an indirect characterisation of commutative semifields. Can we find a more direct characterisation without using the S_3-action?

Problem 5 (Section 4) Find a geometric characterisation of linear sets associated with a commutative semifield without using Theorem 16.

A longstanding open problem is the classification of RTCS. This would have many interesting corollaries in Galois geometry, for instance in the theory of semifield flocks, translation ovoids, eggs and translation generalized quadrangles.

Problem 6 (Section 5) Improve on the bounds from [15] and [62], or classify RTCS up to isotopism.

In Section 6, we have listed many examples of finite semifields. Some are contained in infinite families, others are standalone examples. Here is a list of examples that might be embeddable in an infinite family.

Problem 7 (Section 6) Find infinite families (if they exist) of semifields containing the sporadic examples listed in Section 6 (BL, HJ, PW/BLP, CHK, CF, De, MPT, JMPT($4^5, 16^5$), MT, RCR).

During the last decade a lot of data has been produced including a lot of infinite families of finite semifields. In order to make any progress in the classification of finite semifields, it is important to have strong characterisations for the known families.

Problem 8 (Section 6) Find characterisations of known families of semifields.

Another classification problem for which progress has already been made concerns rank two semifields of order q^6 that are 6-dimensional over their center (see Theorem 27).

Problem 9 (Section 6) Complete the classification of semifields of order q^6, 2-dimensional over the left nucleus and 6-dimensional over the center.

References

[1] A. A. ALBERT, *Finite division algebras and finite planes*, in Proc. Sympos. Appl. Math., Vol. 10, American Mathematical Society, Providence, R.I., 1960, pp. 53–70.

[2] ——, *Generalized twisted fields*, Pacific J. Math., 11 (1961), pp. 1–8.

[3] J. ANDRÉ, *Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe*, Math. Z., 60 (1954), pp. 156–186.

[4] L. BADER, W. M. KANTOR, AND G. LUNARDON, *Symplectic spreads from twisted fields*, Boll. Un. Mat. Ital. A (7), 8 (1994), pp. 383–389.

[5] L. BADER, G. LUNARDON, AND I. PINNERI, *A new semifield flock*, J. Combin. Theory Ser. A, 86 (1999), pp. 49–62.

[6] S. BALL AND M. R. BROWN, *The six semifield planes associated with a semifield flock*, Adv. Math., 189 (2004), pp. 68–87.

[7] S. BALL, G. EBERT, AND M. LAVRAUW, *A geometric construction of finite semifields*, J. Algebra, 311 (2007), pp. 117–129.

[8] S. BALL AND M. LAVRAUW, *Commutative semifields of rank 2 over their middle nucleus*, in Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), Springer, Berlin, 2002, pp. 1–21.

[9] ——, *On the Hughes-Kleinfeld and Knuth's semifields two-dimensional over a weak nucleus*, Des. Codes Cryptogr., 44 (2007), pp. 63–67.

[10] J. BIERBRAUER, *New semifields, PN and APN functions*, Des. Codes Cryptogr., to appear. doi: 10.1007/s10623-009-9318-7.

[11] ——, *New commutative semifields and their nuclei*. manuscript, 2010.

[12] E. BIHAM AND A. SHAMIR, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptology, 4 (1991), pp. 3–72.

[13] I. BLOEMEN, J. A. THAS, AND H. VAN MALDEGHEM, *Translation ovoids of generalized quadrangles and hexagons*, Geom. Dedicata, 72 (1998), pp. 19–62.

[14] A. BLOKHUIS AND M. LAVRAUW, *Scattered spaces with respect to a spread in* $\mathrm{PG}(n,q)$, Geom. Dedicata, 81 (2000), pp. 231–243.

[15] A. BLOKHUIS, M. LAVRAUW, AND S. BALL, *On the classification of semifield flocks*, Adv. Math., 180 (2003), pp. 104–111.

[16] V. BOERNER-LANTZ, *A class of semifields of order* q^4, J. Geom., 27 (1986), pp. 112–118.

[17] R. H. BRUCK AND R. C. BOSE, *The construction of translation planes from projective spaces*, J. Algebra, 1 (1964), pp. 85–102.

[18] ——, *Linear representations of projective planes in projective spaces*, J. Algebra, 4 (1966), pp. 117–172.

[19] L. BUDAGHYAN AND T. HELLESETH, *New perfect nonlinear multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime p.* Golomb, Solomon W. (ed.) et al., Sequences and their applications – SETA 2008. 5th international conference, Lexington, KY, USA, September 14–18, 2008 Proceedings. Springer. Lect. Notes Comput. Sci. 5203, 403-414 (2008)., 2008.

[20] A. R. CALDERBANK, P. J. CAMERON, W. M. KANTOR, AND J. J. SEIDEL, *Z_4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets*, Proc. London Math. Soc. (3), 75 (1997), pp. 436–480.

[21] I. CARDINALI, O. POLVERINO, AND R. TROMBETTI, *Semifield planes of order q^4 with kernel F_{q^2} and center F_q*, European J. Combin., 27 (2006), pp. 940–961.

[22] C. CHARNES, *Quadratic matrices and the translation planes of order* 5^2, in Coding theory, design theory, group theory (Burlington, VT, 1990), Wiley-Intersci. Publ., Wiley, New York, 1993, pp. 155–161.

[23] S. D. COHEN AND M. J. GANLEY, *Commutative semifields, two-dimensional over their middle nuclei*, J. Algebra, 75 (1982), pp. 373–385.

[24] M. CORDERO AND R. FIGUEROA, *On some new classes of semifield planes*, Osaka J. Math., 30 (1993), pp. 171–178.

[25] R. S. COULTER AND M. HENDERSON, *Commutative presemifields and semifields*, Adv. Math., 217 (2008), pp. 282–304.

[26] R. S. COULTER, M. HENDERSON, AND P. KOSICK, *Planar polynomials for commutative semifields with specified nuclei*, Des. Codes Cryptogr., 44 (2007), pp. 275–286.

[27] R. S. COULTER AND R. W. MATTHEWS, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr., 10 (1997), pp. 167–184.

[28] P. DEMBOWSKI, *Finite geometries*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44, Springer-Verlag, Berlin, 1968.

[29] U. DEMPWOLFF, *Translation planes of order* 27, Des. Codes Cryptogr., 4 (1994), pp. 105–121.

[30] ——, *Semifield planes of order 81*, J. Geom., 89 (2008), pp. 1–16.

[31] L. E. DICKSON, *On commutative linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc., 7 (1906), pp. 514–522.

[32] ——, *Linear algebras with associativity not assumed*, Duke Math. J., 1 (1935), pp. 113–125.

[33] C. DING AND J. YUAN, *A family of skew Hadamard difference sets*, J. Combin. Theory Ser. A, 113 (2006), pp. 1526–1535.

[34] G. L. EBERT, G. MARINO, O. POLVERINO, AND R. TROMBETTI, *On the multiplication of some semifields of order q^6*, Finite Fields Appl., 15 (2009), pp. 160–173.

[35] ——, *Infinite families of new semifields*, Combinatorica, to appear, (2010).

[36] G. L. EBERT, G. MARINO, O. POLVERINO, AND R. TROMBETTI, *Semifields in class $\mathcal{F}_4^{(a)}$*, Electron. J. Combin., 16 (2009), pp. Research Paper 53, 20.

[37] J. W. FREEMAN, *Reguli and pseudoreguli in* $\mathrm{PG}(3, s^2)$, Geom. Dedicata, 9 (1980), pp. 267–280.

[38] M. J. GANLEY, *Central weak nucleus semifields*, European J. Combin., 2 (1981), pp. 339–347.

[39] M. HALL, *Projective planes*, Trans. Amer. Math. Soc., 54 (1943), pp. 229–277.

[40] Y. HIRAMINE, M. MATSUMOTO, AND T. OYAMA, *On some extension of* 1*-spread sets*, Osaka J. Math., 24 (1987), pp. 123–137.

[41] J. W. P. HIRSCHFELD AND J. A. THAS, *General Galois geometries*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1991. Oxford Science Publications.

[42] H. HUANG AND N. L. JOHNSON, 8 *semifield planes of order* 8^2, Discrete Math., 80 (1990), pp. 69–79.

[43] D. R. HUGHES AND E. KLEINFELD, *Seminuclear extensions of Galois fields*, Amer. J. Math., 82 (1960), pp. 389–392.

[44] D. R. HUGHES AND F. C. PIPER, *Projective planes*, Springer-Verlag, New York, 1973. Graduate Texts in Mathematics, Vol. 6.

[45] V. JHA AND N. L. JOHNSON, *An analog of the Albert-Knuth theorem on the orders of finite semifields, and a complete solution to Cofman's subplane problem*, Algebras Groups Geom., 6 (1989), pp. 1–35.

[46] N. L. JOHNSON, *Sequences of derivable translation planes*, Osaka J. Math., 25 (1988), pp. 519–530.

[47] N. L. JOHNSON, V. JHA, AND M. BILIOTTI, *Handbook of finite translation planes*, vol. 289 of Pure and Applied Mathematics (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2007.

[48] N. L. JOHNSON, G. MARINO, O. POLVERINO, AND R. TROMBETTI, *Semifields of order q^6 with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$*, Finite Fields Appl., 14 (2008), pp. 456–469.

[49] ——, *On a generalization of cyclic semifields*, J. Algebraic Combin., 29 (2009), pp. 1–34.

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

[51] ——, *Some generalized quadrangles with parameters q^2, q*, Math. Z., 192 (1986), pp. 45–50.

[52] ——, *Commutative semifields and symplectic spreads*, J. Algebra, 270 (2003), pp. 96–114.

[53] ——, *Isomorphisms of symplectic planes*, Adv. Geom., 7 (2007), pp. 553–557.

[54] ——, *HMO-planes*, Adv. Geom., 9 (2009), pp. 31–43.

[55] W. M. KANTOR AND R. A. LIEBLER, *Semifields arising from irreducible semilinear transformations*, J. Aust. Math. Soc., 85 (2008), pp. 333–339.

[56] W. M. KANTOR AND M. E. WILLIAMS, *Symplectic semifield planes and $\mathbb{Z}_4$-linear codes*, Trans. Amer. Math. Soc., 356 (2004), pp. 895–938 (electronic).

[57] E. KLEINFELD, *Techniques for enumerating Veblen-Wedderburn systems*, J. Assoc. Comput. Mach., 7 (1960), pp. 330–337.

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

[59] 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.

[60] ——, *Semifield flocks, eggs, and ovoids of $Q(4,q)$*, Adv. Geom., 5 (2005), pp. 333–345.

[61] ——, *The two sets of three semifields associated with a semifield flock*, Innov. Incidence Geom., 2 (2005), pp. 101–107.

[62] ——, *Sublines of prime order contained in the set of internal points of a conic*, Des. Codes Cryptogr., 38 (2006), pp. 113–123.

[63] ——, *On the isotopism classes of finite semifields*, Finite Fields Appl., 14 (2008), pp. 897–910.

[64] ——, *Finite semifields with a large nucleus and higher secant varieties to segre varieties*, Adv. Geom., to appear, (2010).

[65] M. LAVRAUW, G. MARINO, O. POLVERINO, AND R. TROMBETTI, *$\mathbb{F}_q$-pseudoreguli of $PG(3,q^3)$ and scattered semifields of order q^6*. In preparation.

[66] M. LAVRAUW AND G. VAN DE VOORDE, *On linear sets on a projective line* Des. Codes Cryptogr., to appear.

[67] R. LIDL AND H. NIEDERREITER, *Finite fields*, vol. 20 of Encyclopedia of Mathematics and its Applications, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983. (Now distributed by Cambridge University Press).

[68] G. LUNARDON, *Flocks, ovoids of* $\mathrm{Q}(4,q)$ *and designs*, Geom. Dedicata, 66 (1997), pp. 163–173.

[69] ——, *Translation ovoids*, J. Geom., 76 (2003), pp. 200–215. Combinatorics, 2002 (Maratea).

[70] ——, *Symplectic spreads and finite semifields*, Des. Codes Cryptogr., 44 (2007), pp. 39–48.

[71] G. LUNARDON, G. MARINO, O. POLVERINO, AND R. TROMBETTI, *Translation dual of a semifield*, J. Combin. Theory Ser. A, 115 (2008), pp. 1321–1332.

[72] ——, *Symplectic semifield spreads of* $\mathrm{PG}(5,q)$ *and the Veronese surface*. Submitted, 2010.

[73] H. LÜNEBURG, *Translation planes*, Springer-Verlag, Berlin, 1980.

[74] D. M. MADURAM, *Transposed translation planes*, Proc. Amer. Math. Soc., 53 (1975), pp. 265–270.

[75] G. MARINO, O. POLVERINO, AND R. TROMBETTI, *On* $\mathbb{F}_q$*-linear sets of* $\mathrm{PG}(3,q^3)$ *and semifields*, J. Combin. Theory Ser. A, 114 (2007), pp. 769–788.

[76] ——, *On semifields of type* (q^{2n},q^n,q^2,q^2,q)*, n odd*, Innov. Incidence Geom., 6/7 (2007/08), pp. 271–289.

[77] G. MARINO AND R. TROMBETTI, *A new semifield of order* 2^{10}, Discrete Math., to appear. doi:10.1016/j.disc.2009.05.013.

[78] G. MENICHETTI, *On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field*, J. Algebra, 47 (1977), pp. 400–410.

[79] ——, *n-dimensional algebras over a field with a cyclic extension of degree n*, Geom. Dedicata, 63 (1996), pp. 69–94.

[80] K. NYBERG, *Differentially uniform mappings for cryptography.* Helleseth, Tor (ed.), Advances in cryptology - EUROCRYPT '93. Workshop on the theory and application of cryptographic techniques, Lofthus, Norway, May 23-27, 1993. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 765, 55-64 (1994)., 1994.

[81] S. E. PAYNE, *Generalized quadrangles as group coset geometries*, in Proceedings of the Eleventh Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1980), Vol. II, vol. 29, 1980, pp. 717–734.

[82] ——, *A new infinite family of generalized quadrangles*, in Proceedings of the sixteenth Southeastern international conference on combinatorics, graph theory and computing (Boca Raton, Fla., 1985), vol. 49, 1985, pp. 115–128.

[83] S. E. PAYNE AND J. A. THAS, *Finite generalized quadrangles*, EMS Series of Lectures in Mathematics, European Mathematical Society (EMS), Zürich, second ed., 2009.

[84] T. PENTTILA AND B. WILLIAMS, *Ovoids of parabolic spaces*, Geom. Dedicata, 82 (2000), pp. 1–19.

[85] O. POLVERINO, *Linear sets in Finite Projective Spaces*, Discrete Math., to appear. doi:10.1016/j.disc.2009.04.007.

[86] I. F. RÚA, E. F. COMBARRO, AND J. RANILLA, *Classification of* 64*-element finite semifields*, J. Algebra, 322 (2009), pp. 4011–4029.

[87] R. SANDLER, *Autotopism groups of some finite non-associative algebras*, Amer. J. Math., 84 (1962), pp. 239–264.

[88] B. SEGRE, *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane*, Ann. Mat. Pura Appl. (4), 64 (1964), pp. 1–76.

[89] J. A. THAS, *The m-dimensional projective space $S_m(M_n(\mathrm{GF}(q)))$ over the total matrix algebra $M_n(\mathrm{GF}(q))$ of the $n \times n$-matrices with elements in the Galois field* $\mathrm{GF}(q)$, Rend. Mat. (6), 4 (1971), pp. 459–532.

[90] ——, *Generalized quadrangles and flocks of cones*, European J. Combin., 8 (1987), pp. 441–452.

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

[92] J. A. THAS AND S. E. PAYNE, *Spreads and ovoids in finite generalized quadrangles*, Geom. Dedicata, 52 (1994), pp. 227–253.

[93] J. A. THAS, K. THAS, AND H. VAN MALDEGHEM, *Translation generalized quadrangles*, vol. 26 of Series in Pure Mathematics, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2006.

[94] R. J. WALKER, *Determination of division algebras with* 32 *elements*, in Proc. Sympos. Appl. Math., Vol. XV, Amer. Math. Soc., Providence, R.I., 1963, pp. 83–85.

[95] Z. ZHA, G. M. KYUREGHYAN, AND X. WANG, *Perfect nonlinear binomials and their semifields*, Finite Fields Appl., 15 (2009), pp. 125–133.