On semifields of type $(q^{2n}, q^n, q^2, q^2, q)$, n odd

Giuseppe Marino* Olga Polverino Rocco Tromebtti

Abstract

A semifield of type $(q^{2n}, q^n, q^2, q^2, q)$ (with $n > 1$) is a finite semifield of order q^{2n} (q a prime power) with left nucleus of order q^n, right and middle nuclei both of order q^2 and center of order q. Semifields of type (q^6, q^3, q^2, q^2, q) have been completely classified by the authors and N. L. Johnson in [10]. In this paper we determine, up to isotopy, the form of any semifield of type $(q^{2n}, q^n, q^2, q^2, q)$ when n is an odd integer, proving that there exist $\frac{n-1}{2}$ non isotopic potential families of semifields of this type. Also, we provide, with the aid of the computer, new examples of semifields of type $(q^{14}, q^7, q^2, q^2, q)$, when $q = 2$.

Keywords: semifield, isotopy, linear set

MSC 2000: 51A40, 51E20, 12K10

1. Introduction

A *finite semifield* $\mathbb{S}$ is a finite algebraic structure satisfying all the axioms for a skew field except (possibly) associativity. The subsets

$$\begin{aligned}
\mathbb{N}_l &= \{a \in \mathbb{S} \mid (ab)c = a(bc),\ \forall b, c \in \mathbb{S}\}, \\
\mathbb{N}_m &= \{b \in \mathbb{S} \mid (ab)c = a(bc),\ \forall a, c \in \mathbb{S}\}, \\
\mathbb{N}_r &= \{c \in \mathbb{S} \mid (ab)c = a(bc),\ \forall a, b \in \mathbb{S}\} \text{ and} \\
\mathcal{K} &= \{a \in \mathbb{N}_l \cap \mathbb{N}_m \cap \mathbb{N}_r \mid ab = ba,\ \forall b \in \mathbb{S}\}
\end{aligned}$$

are fields and are known, respectively, as the *left nucleus*, the *middle nucleus*, the *right nucleus* and the *center* of the semifield. A finite semifield is a vector space

*This work was supported by the Research Project of MIUR (Italian Office for University and Research) "Strutture geometriche, combinatoria e loro applicazioni" and by INDAM (Istituto Nazionale di Alta Matematica "Francesco Severi".

over its nuclei and its center (for more details on semifields see e.g. [4, 9]). If $\mathbb{S}$ satisfies all the axioms of a semifield except possibly the existence of the identity element of the multiplication, then $\mathbb{S}$ is called *pre-semifield*. From now on the terms semifield and pre-semifield will be always used to denote a finite semifield and a finite pre-semifield. If $\mathbb{S} = (\mathbb{S}, +, \circ)$ is a pre-semifield, then $(\mathbb{S}, +)$ is an elementary abelian p-group (p prime); hence, $\mathbb{S}$ is an $\mathbb{F}_p$-vector space. Now, if $\mathbb{S} = (\mathbb{S}, +, \circ)$ and $\mathbb{S}' = (\mathbb{S}', +, \circ')$ are two pre-semifields whose additive groups are elementary abelian p-groups, then $\mathbb{S}$ and $\mathbb{S}'$ are *isotopic* if there exist three invertible $\mathbb{F}_p$-linear maps, f_1, f_2 and f_3 of $\mathbb{S}$ into $\mathbb{S}'$ such that

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

for each $x, y \in \mathbb{S}$. The dimensions of a semifield $\mathbb{S}$ over its nuclei and its center are invariant under the isotopy relation. From any pre-semifield it is possible to construct a semifield which is isotopic to the starting pre-semifield. The sizes of the nuclei as well as the size of the center of a semifield are invariant under isotopy.

Semifields coordinatize certain translation planes (called *semifield planes*) and two semifield planes are isomorphic if and only if the corresponding semifields are isotopic (see [1]). A semifield is isotopic to a field if and only if the corresponding semifield plane is Desarguesian.

Let b be an element of a semifield $\mathbb{S}$ with center $\mathcal{K}$; then the map φ_b mapping $x \in \mathbb{S}$ to $xb \in \mathbb{S}$ is a linear map when $\mathbb{S}$ is regarded as a left vector space over $\mathbb{N}_l$. The set $S = \{\varphi_b \mid b \in \mathbb{S}\}$ is called the *spread set of linear maps* of $\mathbb{S}$; it is closed under the sum of linear maps, $|S| = |\mathbb{S}|$ and $\lambda\varphi_b = \varphi_{\lambda b}$ for any $\lambda \in \mathcal{K}$, i.e. S is a $\mathcal{K}$-vector subspace of the vector space $\mathbb{V}$ of all $\mathbb{N}_l$-linear maps of $\mathbb{S}$.

We say that a semifield is of *type* $(q^{2n}, q^n, q^2, q^2, q)$ (q a prime power), if it has order q^{2n}, left nucleus of order q^n, right and middle nuclei both of order q^2 and center of order q.

In this paper we prove that a semifield $\mathbb{S}$ of type $(q^{2n}, q^n, q^2, q^2, q)$, n odd, is isotopic to a semifield $\mathbb{S}_j = (\mathbb{F}_{q^{2n}}, +, \circ)$, $\frac{n+1}{2} \leq j < n$, with multiplication given by

$$x \circ y = (\alpha_1 + \alpha_2 a_2 + \cdots + \alpha_j a_j)x + (\beta_1 b_1 + \beta_2 b_2 + \cdots + \beta_{n-j} b_{n-j})x^{q^n}\,,$$

where $y = \alpha_1 + \alpha_2 a_2 + \cdots + \alpha_j a_j + \beta_1 b_1 + \beta_2 b_2 + \cdots + \beta_{n-j} b_{n-j}$ ($\alpha_i, \beta_i \in \mathbb{F}_{q^2}$) and $\{1, a_2, \ldots, a_j, b_1, b_2, \ldots, b_{n-j}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ such that

$$\left(\frac{\alpha_1 + \alpha_2 a_2 + \cdots + \alpha_j a_j}{\beta_1 b_1 + \beta_2 b_2 + \cdots + \beta_{n-j} b_{n-j}}\right)^{q^n+1} \neq 1\,,$$

for each $\alpha_i, \beta_i \in \mathbb{F}_{q^2}$, $(\beta_1, \ldots, \beta_{n-j}) \neq (0, \ldots, 0)$. Moreover, by using the geometric properties of the spread sets of linear maps associated with such semifields we prove that two semifields $\mathbb{S}_j$ and $\mathbb{S}_{j'}$ with $\frac{n+1}{2} \leq j, j' < n$ and $j \neq j'$

are not isotopic. Hence the semifields of type $(q^{2n}, q^n, q^2, q^2, q)$, n odd, are partitioned into $\frac{n-1}{2}$ non-isotopic families.

Some semifields of type $\mathbb{S}_{\frac{n+1}{2}}$ are constructed by the authors and N. Johnson in [11, Section 4] generalizing the cyclic semifields [8]. Moreover, semifields of type $\mathbb{S}_{n-1}$ belong to a family of semifields introduced in [16] and studied in [20]. The other classes seem to be likely places to search for new semifields. Indeed, computational results obtained using MAGMA provide some new examples of semifields of type $(q^{14}, q^7, q^2, q^2, q)$, for $q = 2$ and $j = 5$.

2. Preliminary results

Let $\mathbb{S} = (\mathbb{F}_{q^{2n}}, +, \circ)$ be a semifield two dimensional over its left nucleus $\mathbb{F}_{q^n}$, with identity element 1 and center $\mathbb{F}_q$, and let S be the spread set of $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$ defining the multiplication $\circ$, i.e. $x \circ y = \varphi_y(x)$ where φ_y is the unique element of S such that $\varphi_y(1) = y$. Since $\mathbb{S}$ has center $\mathbb{F}_q$, we have $x \circ y = xy = y \circ x$ for each $x \in \mathbb{F}_q$ and $y \in \mathbb{F}_{q^{2n}}$, and hence S contains the field of linear maps $F_q = \{x \in \mathbb{F}_{q^{2n}} \mapsto \alpha x \in \mathbb{F}_{q^{2n}} \mid \alpha \in \mathbb{F}_q\}$. An element $z \in \mathbb{F}_{q^{2n}}$ belongs to the right nucleus of $\mathbb{S}$ if $x \circ (y \circ z) = (x \circ y) \circ z$ for each $x, y \in \mathbb{F}_{q^{2n}}$, i.e. $z \in \mathbb{N}_r$ if $\varphi_{y \circ z} = \varphi_z \varphi_y$ (juxtaposition stands for the composition of maps) for each $y \in \mathbb{F}_{q^{2n}}$. So the right nucleus of $\mathbb{S}$ defines a field $N_r = \{\varphi_z \mid z \in \mathbb{N}_r\}$ of linear maps contained in S isomorphic to $\mathbb{N}_r$ with respect to which S is a left vector space, i.e. $N_r S = \{\mu\varphi \mid \mu \in N_r, \varphi \in S\} = S$ and N_r can be characterized as the maximal field of linear maps contained in S with respect to which S is a left vector space. Similarly, the middle nucleus of $\mathbb{S}$ defines a field $N_m = \{\varphi_z \mid z \in \mathbb{N}_m\}$ of linear maps contained in S isomorphic to $\mathbb{N}_m$ with respect to which S is a right vector space, i.e. $SN_m = S$ and N_m can be characterized as the maximal field of linear maps contained in S with respect to which S is a right vector space.

If Ψ and Φ are invertible $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$ and σ is an automorphism of $\mathbb{F}_{q^{2n}}$, then the set

$$S' = \Psi S^\sigma \Phi = \{\Psi \varphi^\sigma \Phi \mid \varphi \in S\} \qquad (*)$$

(where $\varphi^\sigma : x \mapsto a^\sigma x + b^\sigma x^{q^n}$ for $\varphi : x \mapsto ax + bx^{q^n}$ and the composition of maps is to be read from right to left) is an additive spread set of linear maps that defines on $\mathbb{F}_{q^{2n}}$ a pre-semifield $\mathbb{S}'$ isotopic to $\mathbb{S}$. Conversely, any pre-semifield $\mathbb{S}' = (\mathbb{F}_{q^{2n}}, +, \circ')$ isotopic to $\mathbb{S}$ is defined by a spread set S' of type $(*)$ (see e.g. [10, 11]).

Note that $\Psi N_r^\sigma \Psi^{-1}$ is a field, isomorphic to $\mathbb{N}_r$, with respect to which S' is a left vector space, i.e. $\Psi N_r^\sigma \Psi^{-1} S' = S'$ and similarly $\Phi^{-1} N_m^\sigma \Phi$ is a field,

isomorphic to $\mathbb{N}_m$, such that $S'\Phi^{-1}N_m^\sigma\Phi = S'$. Hence we have the following property.

Property 2.1. *If $\mathbb{S}'$ is a pre-semifield, with associated spread set S', isotopic to the semifield $\mathbb{S}$, then the right (respectively, middle) nucleus of $\mathbb{S}$ is isomorphic to the maximal field K of linear maps contained in $\mathbb{V}$ with respect to which $KS' = S'$ (respectively, $S'K = S'$).*

Any element $\varphi \in \mathbb{V}$ can be uniquely written as

$$\varphi = \varphi_{a,b} \colon x \in \mathbb{F}_{q^{2n}} \mapsto ax + bx^{q^n} \in \mathbb{F}_{q^{2n}}$$

and $\varphi_{a,b}$ is non-invertible if and only if $a^{q^n+1} = b^{q^n+1}$ (see [14, p. 361]). Since $\mathbf{q}(\varphi_{a,b}) = a^{q^n+1} - b^{q^n+1}$ is a quadratic form of $\mathbb{V}$ over $\mathbb{F}_{q^n}$, the non-invertible elements of $\mathbb{V}$ define the hyperbolic quadric

$$\mathcal{Q} = \left\{ [\varphi_{a,b}]_{\mathbb{F}_{q^n}} \mid a^{q^n+1} - b^{q^n+1} = 0,\ (a,b) \neq (0,0) \right\}$$

of the 3-dimensional projective space $\mathbb{P} = \mathsf{PG}(\mathbb{V}, \mathbb{F}_{q^n}) = \mathsf{PG}(3, q^n)$. Here the symbol $[\varphi_{a,b}]_{\mathbb{F}_{q^n}}$ denotes the 1-dimensional $\mathbb{F}_{q^n}$-vector subspace of $\mathbb{V}$ generated by $\varphi_{a,b}$.

If S is the spread set of $\mathbb{F}_{q^n}$-linear maps of a pre-semifield $\mathbb{S} = (\mathbb{F}_{q^{2n}}, +, \circ)$ with center $\mathbb{F}_q$, then S is an $\mathbb{F}_q$-vector subspace of $\mathbb{V}$ of dimension $2n$ and all the non-zero elements of S are invertible maps. Therefore, the $\mathbb{F}_q$-linear set $L(\mathbb{S}) = \left\{ [\varphi]_{\mathbb{F}_{q^n}} \mid \varphi \in S,\ \varphi \neq 0 \right\}$ of $\mathbb{P}$ defined by the nonzero vectors of S is disjoint from $\mathcal{Q}$. Also, any semilinear map of $\mathbb{V}$ of type

$$\Gamma \colon \varphi \in \mathbb{V} \mapsto \Psi\varphi^\sigma\Phi \in \mathbb{V}, \qquad (\Diamond)$$

where Ψ and Φ are invertible $\mathbb{F}_{q^n}$-linear maps of $\mathbb{V}$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^{2n}})$, induces a collineation of $\mathbb{P}$ preserving the reguli of $\mathcal{Q}$, and conversely (see [3]). Hence:

Theorem 2.2 ([3]). *Two isotopic semifields two dimensional over their left nuclei define linear sets isomorphic under the action of the collineation group $G \leq \mathsf{P\Gamma O}^+(4, q^n)$ preserving the reguli of $\mathcal{Q}$.*

We say that a point $P = [\varphi]_{\mathbb{F}_{q^n}}$ of $\mathbb{P}$ has *weight* i in $L(\mathbb{S})$ if $\dim_{\mathbb{F}_q}(S \cap [\varphi]_{\mathbb{F}_{q^n}}) = i$ $(i = 0, \ldots, n)$ (see e.g. [10, 19]) and we will write $w(P) = i$. In a similar way, we say that a line $l = [\varphi, \varphi']_{\mathbb{F}_{q^n}}$ of $\mathbb{P}$ has *weight* i in $L(\mathbb{S})$ if $\dim_{\mathbb{F}_q}(S \cap [\varphi, \varphi']_{\mathbb{F}_{q^n}}) = i$ $(i = 0, \ldots, 2n)$; if $i = 0$, then the line l is external to $L(\mathbb{S})$, while, if $i = 2n$, then $L(\mathbb{S}) = l$. Also, the following properties concerning the weight of points and lines hold true.

Property 2.3 ([10, Property 3.1]). *A line l of $\mathbb{P}$ is contained in $L(\mathbb{S})$ if and only if the weight of l in $L(\mathbb{S})$ is at least $n + 1$.*

Property 2.4. *The weight of a point as well as the weight of a line in $L(\mathbb{S})$ is invariant under isotopy, i.e. if $\mathbb{S}_1$ and $\mathbb{S}_2$ are isotopic pre-semifields and $S_1^\Gamma = S_2$, where Γ is an invertible semilinear map of $\mathbb{V}$ of type ($\Diamond$), and P (respectively, r) is a point (respectively, a line) of $\mathbb{P}$ of weight i in $L(\mathbb{S}_1)$, then P^φ (respectively, r^φ) has weight i in $L(\mathbb{S}_1)^\varphi = L(\mathbb{S}_2)$ where φ is the collineation of $\mathbb{P}$ induced by Γ.*

Proof. Two pre-semifields $\mathbb{S}_1$ and $\mathbb{S}_2$ with associated spread sets S_1 and S_2, respectively, are isotopic if and only if $S_1^\Gamma = S_2$, where Γ is an invertible semilinear map of $\mathbb{V}$ of type ($\Diamond$). Now, noting that an invertible semilinear map of $\mathbb{V}$ preserves the dimension of the $\mathbb{F}_q$-vector subspaces, the result easily follows. □

Starting from a given semifield $\mathbb{S} = (\mathbb{F}_{q^{2n}}, +, \circ)$ with left nucleus $\mathbb{F}_{q^n}$, two other semifields, two dimensional over their left nuclei, can be constructed: the transpose semifield $\mathbb{S}^T$ and the translation dual semifield $\mathbb{S}^\perp$ of $\mathbb{S}$. More precisely, if $\pi_\mathbb{S}$ is the semifield plane coordinatized by the semifield $\mathbb{S}$, then $\mathbb{S}^T$ is the semifield which coordinatizes the dual plane of $\pi_\mathbb{S}$; whereas $\mathbb{S}^\perp$ is defined by using the polarity $\perp$ associated with the hyperbolic quadric $\mathcal{Q}$ of $\mathbb{P}$ as originally introduced in [15] (for more details see also [9, Chapter 85]).

In [18] the following has been proved.

Theorem 2.5 ([18, Theorem 4.1])**.** *Let $\mathbb{S} = (\mathbb{F}_{q^{2n}}, +, \circ)$ be a semifield with left nucleus $\mathbb{F}_{q^n}$ and let S be the associated spread set of linear maps. Then $S^T = \{\varphi_{a,b^{q^n}} \mid \varphi_{a,b} \in S\}$ is a spread set defining the transpose semifield $\mathbb{S}^T$.*

The polar form associated with the quadratic form $\mathbf{q}(\varphi_{a,b}) = a^{q^n+1} - b^{q^n+1}$ of $\mathbb{V}$ is $\sigma(\varphi_{a,b}, \varphi_{a',b'}) = a^{q^n}a' + a'^{q^n}a - b^{q^n}b' - b'^{q^n}b$. Hence $\langle \varphi_{a,b}; \varphi_{a',b'} \rangle = \mathrm{Tr}_{q^n/q}(\sigma(\varphi_{a,b}, \varphi_{a',b'}))$, where $\mathrm{Tr}_{q^n/q}$ is the trace function of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, is a non-degenerate bilinear form of $\mathbb{V}$ over $\mathbb{F}_q$ and

$$S^\perp = \{\varphi_{a',b'} \mid \langle \varphi_{a,b}; \varphi_{a',b'} \rangle = 0 \ \ \forall\, \varphi_{a,b} \in S\}$$

is the orthogonal complement of S with respect to $\langle \cdot\ ;\ \cdot \rangle$. By [18, Section 3], $S^\perp$ is a spread set of $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$ defining a pre-semifield isotopic to the translation dual $\mathbb{S}^\perp$ of $\mathbb{S}$.

We end this section by recalling the following property.

Property 2.6. *If l is a line of $\mathbb{P}$ of weight j in $L(\mathbb{S})$, then $l^\perp$ has weight j in $L(\mathbb{S}^\perp)$ as well.*

Proof. The statement follows from Equality (3) of [19, Section 2.1] in the case $r = 4$, $t = 2n$ and $i = 1$. □

3. The main Theorem

We start by stating the following lemma.

Lemma 3.1. *Let F be a set of $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$, n odd, such that*

(i) *F is a field of order q^2 with respect to the sum and the composition of linear maps;*

(ii) *F contains the field of linear maps $F_q = \{x \in \mathbb{F}_{q^{2n}} \mapsto \alpha x \in \mathbb{F}_{q^{2n}} \mid \alpha \in \mathbb{F}_q\}$.*

Then there exists an invertible $\mathbb{F}_{q^n}$-linear map Ψ of $\mathbb{F}_{q^{2n}}$ such that

$$\Psi^{-1} F \Psi = F_{q^2} = \{x \in \mathbb{F}_{q^{2n}} \mapsto \eta x \in \mathbb{F}_{q^{2n}} \mid \eta \in \mathbb{F}_{q^2}\}.$$

Proof. A slight generalization of [11, Lemma 2.1]. □

In light of this result, we are able to prove the main Theorem of the paper.

Theorem 3.2. *Let $\mathbb{S}$ be a semifield of type $(q^{2n}, q^n, q^2, q^2, q)$, n odd. Then $\mathbb{S}$ is isotopic to a semifield $\mathbb{S}_j = (\mathbb{F}_{q^{2n}}, +, \circ)$, $\frac{n+1}{2} \leq j < n$, with multiplication given by*

$$x \circ y = (\alpha_1 + \alpha_2 a_2 + \cdots + \alpha_j a_j)x + (\beta_1 b_1 + \beta_2 b_2 + \cdots + \beta_{n-j} b_{n-j}) x^{q^n}, \quad (1)$$

where $y = \alpha_1 + \alpha_2 a_2 + \cdots + \alpha_j a_j + \beta_1 b_1 + \beta_2 b_2 + \cdots + \beta_{n-j} b_{n-j}$ ($\alpha_i, \beta_i \in \mathbb{F}_{q^2}$) and $\{1, a_2, \ldots, a_j, b_1, b_2, \ldots, b_{n-j}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ such that

$$\left(\frac{\alpha_1 + \alpha_2 a_2 + \cdots + \alpha_j a_j}{\beta_1 b_1 + \beta_2 b_2 + \cdots + \beta_{n-j} b_{n-j}} \right)^{q^n+1} \neq 1, \quad (2)$$

for each $\alpha_i, \beta_i \in \mathbb{F}_{q^2}$, $(\beta_1, \ldots, \beta_{n-j}) \neq (0, \ldots, 0)$.

Conversely, if $\{1, a_2, \ldots, a_j, b_1, b_2, \ldots, b_{n-j}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ (n odd and $\frac{n+1}{2} \leq j < n$) satisfying (2), then the algebraic structure $\mathbb{S}_j = (\mathbb{F}_{q^{2n}}, +, \circ)$ where $\circ$ is defined as in (1), is a semifield of type $(q'^{2t}, q'^t, q'^2, q'^2, q')$, where $q' = q^s$, $n = st$ and $s \mid \gcd(n, j)$.

Proof. Let $\mathbb{S}$ be a semifield of type $(q^{2n}, q^n, q^2, q^2, q)$, n odd. Since $\mathbb{S}$ has order q^{2n}, left nucleus of size q^n and center of size q, we may assume that $\mathbb{S} = (\mathbb{F}_{q^{2n}}, +, \circ)$, $\mathbb{N}_l = \mathbb{F}_{q^n}$ and hence $\mathcal{K} = \mathbb{F}_q$. Then the spread set S associated with $\mathbb{S}$ contains the field of linear maps F_q and the right and the middle nuclei of $\mathbb{S}$ determine two subsets N_r and N_m of $\mathbb{V}$ which are fields of linear maps of order q^2 containing the field F_q and such that $N_r S = S$ and $S N_m = S$. By the previous lemma there exist two invertible $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$, Φ and Ψ,

such that $\Phi^{-1}N_r\Phi = \Psi^{-1}N_m\Psi = F_{q^2}$. So the pre-semifield $\mathbb{S}' = (\mathbb{F}_{q^{2n}}, +, \circ')$ defined by the set of $\mathbb{F}_{q^n}$-linear maps $S' = \Phi^{-1}S\Psi$ is isotopic to $\mathbb{S}$, and since

$$F_{q^2}S' = \Phi^{-1}N_rS\Psi = \Phi^{-1}S\Psi = S'$$

and

$$S'F_{q^2} = \Phi^{-1}SN_m\Psi = \Phi^{-1}S\Psi = S',$$

the pre-semifield $\mathbb{S}'$ is a left and a right vector space over the field of linear maps F_{q^2}. Hence we have that, if $\bar{\beta}\colon x \mapsto \beta x$, with $\beta \in \mathbb{F}_{q^2}$, then

$$\bar{\beta}\varphi,\ \varphi\bar{\beta} \in S'\,,$$

for all $\varphi \in S'$. Therefore, if $\varphi = \varphi_{a,b}\colon x \mapsto ax + bx^{q^n}$, then

$$\bar{\beta}\varphi - \varphi\bar{\beta}\colon x \mapsto b(\beta - \beta^q)x^{q^n}$$

is an element of S' for each $\beta \in \mathbb{F}_{q^2}$. This implies that $x \mapsto bx^{q^n}$ belongs to S' as well as the map $x \mapsto ax$. Then we can write $S' = S_1 \oplus S_2$, where S_1 is an $\mathbb{F}_{q^2}$-vector subspace of

$$D = \{x \mapsto ax \mid a \in \mathbb{F}_{q^{2n}}\} = \{aI \mid a \in \mathbb{F}_{q^{2n}}\} \text{ (with } I\colon x \in \mathbb{F}_{q^{2n}} \mapsto x \in \mathbb{F}_{q^{2n}})$$

and S_2 is an $\mathbb{F}_{q^2}$-vector subspace of

$$D' = \{x \mapsto bx^{q^n} \mid b \in \mathbb{F}_{q^{2n}}\} = \{bJ \mid b \in \mathbb{F}_{q^{2n}}\}$$
$$\text{(with } J\colon x \in \mathbb{F}_{q^{2n}} \mapsto x^{q^n} \in \mathbb{F}_{q^{2n}})\,.$$

Since S' is an n-dimensional $\mathbb{F}_{q^2}$-vector subspace of $\mathbb{V}$, then we have that if $\dim_{\mathbb{F}_{q^2}} S_1 = j$, then $\dim_{\mathbb{F}_{q^2}} S_2 = n - j$. So, if $S_1 = [a_1I, \ldots, a_jI]_{\mathbb{F}_{q^2}}$ and $S_2 = [b_1J, \ldots, b_{n-j}J]_{\mathbb{F}_{q^2}}$, we can write the spread set S' in the following way:

$$S' = \big\{x \mapsto (\alpha_1a_1 + \cdots + \alpha_ja_j)\,x + (\beta_1b_1 + \cdots + \beta_{n-j}b_{n-j})\,x^{q^n} \mid \alpha_i, \beta_i \in \mathbb{F}_{q^2}\big\}. \quad (3)$$

The linear map $\Gamma\colon \varphi_{a,b} \in \mathbb{V} \mapsto \varphi_{a,b}J = \varphi_{b,a} \in \mathbb{V}$ defines a pre-semifield isotopic to $\mathbb{S}'$. By these arguments we may assume that, up to isotopy, S' is of type (3) with $j \geq \frac{n+1}{2}$. Note that if $j = n$, then $S' = D = \{aI \mid a \in \mathbb{F}_{q^{2n}}\}$ and hence the spread set S' defines the field $\mathbb{F}_{q^{2n}}$; so in our hypothesis $\frac{n+1}{2} \leq j < n$. Also, the spread set $a_1^{-1}S' = \{a_1^{-1}\varphi \mid \varphi \in S'\}$ contains the identity map I and defines a semifield isotopic to $\mathbb{S}'$. Hence we may suppose, up to isotopy, that $a_1 = 1$. Finally, since all the non-zero maps of S' are invertible we easily get condition (2).

Now, suppose that $\{1, a_2, \ldots, a_j, b_1, b_2, \ldots, b_{n-j}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ ($\frac{n+1}{2} \leq j < n$) satisfying (2). Then the map

$$\varphi_{\alpha_1,\ldots,\alpha_j,\beta_1,\ldots,\beta_{n-j}} : x \mapsto (\alpha_1 + \alpha_2 a_2 + \cdots + \alpha_j a_j)\, x + (\beta_1 b_1 + \cdots + \beta_{n-j} b_{n-j})\, x^{q^n}$$

is non-singular for any $\alpha_i, \beta_i \in \mathbb{F}_{q^2}$ not all zero. So

$$S_j = \{\varphi_{\alpha_1,\ldots,\alpha_j,\beta_1,\ldots,\beta_{n-j}} \mid \alpha_i, \beta_i \in \mathbb{F}_{q^2}\}$$

is an additive spread set of $\mathbb{F}_{q^n}$-linear maps and it defines a semifield $\mathbb{S}_j = (\mathbb{F}_{q^{2n}}, +, \circ)$, where $\circ$ is defined as in (1), with left nucleus $\mathbb{F}_{q^n}$. Recall that by Property 2.1, the right nucleus of $\mathbb{S}_j$ is isomorphic to the maximal field K of linear maps contained in $\mathbb{V}$ such that $KS_j = S_j$. Hence, since $F_{q^2} S_j = S_j$, we have $F_{q^2} \subseteq K$. Now, let $\varphi : x \mapsto Ax + Bx^{q^n}$ be any element of K. Then $\varphi\varphi_{\alpha_1,\ldots,\alpha_j,0,\ldots,0} \in S_j$ for any $\alpha_i \in \mathbb{F}_{q^2}$, and, since $j > n - j$, this implies $B = 0$. Hence $K \subset D$ and this implies that $K = F_{q^{2s}} = \{\bar{A} : x \to Ax \mid A \in \mathbb{F}_{q^{2s}}\}$ for some $s \mid n$, so the right nucleus of $\mathbb{S}_j$ is $\mathbb{F}_{q^{2s}}$. Also, since $\bar{A}\varphi_{\alpha_1,\ldots,\alpha_j,\beta_1,\ldots,\beta_{n-j}} = A\varphi_{\alpha_0,\ldots,\alpha_j,\beta_1,\ldots,\beta_{n-j}} \in S_j$ for each $A \in \mathbb{F}_{q^{2s}}$, we get that $[1, a_2, \ldots, a_j]_{\mathbb{F}_{q^2}}$ and $[b_1, b_2, \ldots, b_{n-j}]_{\mathbb{F}_{q^2}}$ are $\mathbb{F}_{q^{2s}}$-subspaces of $\mathbb{F}_{q^{2n}}$ and hence $s \mid j$ and $s \mid (n - j)$. From these arguments we easily get that K also is the maximal field of linear maps contained in $\mathbb{V}$ such that $S_j K = S_j$, i.e. the middle nucleus of $\mathbb{S}_j$ is $\mathbb{F}_{q^{2s}}$ as well. Then the semifield $\mathbb{S}_j$ has center $\mathbb{F}_{q'}$ where $q' = q^s$ and hence, if $n = st$, $\mathbb{S}_j$ is a semifield of type $(q'^{2t}, q'^t, q'^2, q'^2, q')$. □

We will denote by $\mathbb{S}_j$ ($\frac{n+1}{2} \leq j < n$) a semifield whose multiplication is defined as in (1) and by S_j the associated spread set of $\mathbb{F}_{q^n}$-linear maps.

Remark 3.3. Note that the spread set

$$S_j = \{x \mapsto (\alpha_1 + \alpha_2 a_2 + \cdots + \alpha_j a_j)\, x + (\beta_1 b_1 + \cdots + \beta_{n-j} b_{n-j})\, x^{q^n} \mid \alpha_i, \beta_i \in \mathbb{F}_{q^2}\}$$

can be written in the following way:

$$S_j = \{x \mapsto (\alpha_1 + \alpha_2 a_2 + \cdots + \alpha_j a_j)\, x + b(\beta_1 + \beta_2 b'_2 + \cdots + \beta_{n-j} b'_{n-j})\, x^{q^n} \mid \alpha_i, \beta_i \in \mathbb{F}_{q^2}\},$$

where $b = b_1$ and $b'_k = \frac{b_k}{b_1}$ for $k = 2, \ldots, n - j$. Hence condition (2) in Theorem 3.2 can be rewritten as

$$b^{q^n+1} \notin \left\{ \left(\frac{\alpha_1 + \cdots + \alpha_j a_j}{\beta_1 + \cdots + \beta_{n-j} b'_{n-j}} \right)^{q^n+1} \;\middle|\; \alpha_i, \beta_i \in \mathbb{F}_{q^2},\ (\beta_1, \ldots, \beta_{n-j}) \neq (0, \ldots, 0) \right\}. \quad (4)$$

In what follows, we will show that two semifields $\mathbb{S}_j$ and $\mathbb{S}_{j'}$, with $j \neq j'$ ($j, j' \geq \frac{n+1}{2}$) are not isotopic. To this aim we start by proving the following lemma.

Lemma 3.4. *The linear set $L(\mathbb{S}_j)$ ($j \geq \frac{n+1}{2}$) associated with the semifield $\mathbb{S}_j$ contains a unique line of $\mathbb{P}$ and such a line has weight j in $L(\mathbb{S}_j)$.*

Proof. Let r and $r^\perp$ (where $\perp$ is the polarity induced by the quadric $\mathcal{Q}$) be the lines of $\mathbb{P}$ defined by the 2-dimensional $\mathbb{F}_{q^n}$-subspaces $D = \{aI \mid a \in \mathbb{F}_{q^{2n}}\}$ and $D' = \{bJ \mid b \in \mathbb{F}_{q^{2n}}\}$ of $\mathbb{V}$, respectively. Since

$$S_j = \{x \mapsto (\alpha_1 + \alpha_2 a_2 + \cdots + \alpha_j a_j)\, x + (\beta_1 b_1 + \cdots + \beta_{n-j} b_{n-j})\, x^{q^n} \mid \alpha_i, \beta_i \in \mathbb{F}_{q^2}\},$$

r and $r^\perp$ have weight $2j$ and $2(n-j)$ in $L(\mathbb{S}_j)$, respectively. More precisely, $S_1 = D \cap S_j = [I, a_2 I, \ldots, a_j I]_{\mathbb{F}_{q^2}}$ and $\dim_{\mathbb{F}_q} S_1 = 2j$, while $S_2 = D' \cap S_j = [b_1 J, b_2 J, \ldots, b_{n-j} J]_{\mathbb{F}_{q^2}}$ and $\dim_{\mathbb{F}_q} S_2 = 2(n-j)$.

We first prove that any point of r has weight at most j in $L(\mathbb{S}_j)$. Indeed, let $P = [vI]_{\mathbb{F}_{q^n}}$ (with $v \in \mathbb{F}^*_{q^{2n}}$) be a point of r with weight i in $L(\mathbb{S}_j)$, i.e., $\dim_{\mathbb{F}_q}([vI]_{\mathbb{F}_{q^n}} \cap S_1) = i$ and hence $S_v = S_1 \cap [vI]_{\mathbb{F}_{q^n}}$ is an $\mathbb{F}_q$-vector subspace of D of dimension i over $\mathbb{F}_q$. So we can write $S_v = [\lambda_1 vI, \ldots, \lambda_i vI]_{\mathbb{F}_q} \subseteq [vI]_{\mathbb{F}_{q^n}}$, where $\lambda_1, \ldots, \lambda_i \in \mathbb{F}_{q^n}$ are linearly independent over $\mathbb{F}_q$. Since $S_v \subseteq S_1$ and S_1 is an $\mathbb{F}_{q^2}$-subspace, we get $[S_v]_{\mathbb{F}_{q^2}} = [\lambda_1 vI, \ldots, \lambda_i vI]_{\mathbb{F}_{q^2}} \subseteq S_1$; moreover, since n is odd, $\lambda_1, \ldots, \lambda_i$ are linearly independent over $\mathbb{F}_{q^2}$, as well. This implies that

$$2i = \dim_{\mathbb{F}_q} [S_v]_{\mathbb{F}_{q^2}} \leq \dim_{\mathbb{F}_q} S_1 = 2j\,,$$

i.e. $i \leq j$. In a similar way we get that the weight of any point of $r^\perp$ in $L(\mathbb{S}_j)$ is at most $n - j$.

Now, as the line r has weight $2j$ in $L(\mathbb{S}_j)$ and $2j \geq n+1$, by Property 2.3, r is contained in $L(\mathbb{S}_j)$. By way of contradiction suppose that there exists a line $\ell = \mathsf{PG}(W, \mathbb{F}_{q^n})$ of $\mathbb{P}$ different from r contained in $L(\mathbb{S}_j)$. Then, by Property 2.3, ℓ has weight $t = \dim_{\mathbb{F}_q}(S_j \cap W) \geq n+1$ in $L(\mathbb{S}_j)$. If $\ell \cap r = \emptyset$,

$$2n = \dim_{\mathbb{F}_q} S_j \geq \dim_{\mathbb{F}_q} [S_j \cap W, S_j \cap D]_{\mathbb{F}_q} = t + 2j \geq 2n + 2\,,$$

a contradiction. Hence $\ell \cap r \neq \emptyset$. Let $\pi = \mathsf{PG}(U, \mathbb{F}_{q^n})$ be the plane of $\mathbb{P}$ containing $\ell = \mathsf{PG}(W, \mathbb{F}_{q^n})$ and $r = \mathsf{PG}(D, \mathbb{F}_{q^n})$ and let $P = l \cap r$. From the previous arguments it follows that $w(P) = \dim_{\mathbb{F}_q}(S_j \cap D \cap W) \leq j$ and if $Q = r^\perp \cap \pi$, then $w(Q) = \dim_{\mathbb{F}_q}(S_j \cap D' \cap U) \leq n - j$. Since

$$\begin{aligned}\dim_{\mathbb{F}_q}(S_j \cap U) &\geq \dim_{\mathbb{F}_q}[S_j \cap D, S_j \cap W]_{\mathbb{F}_q} \\ &= \dim_{\mathbb{F}_q}(S_j \cap D) + \dim_{\mathbb{F}_q}(S_j \cap W) - w(P) = 2j + t - w(P)\,,\end{aligned}$$

we have

$$\begin{aligned} 2n = \dim_{\mathbb{F}_q} S_j &= \dim_{\mathbb{F}_q}[S_j \cap U, S_j \cap D']_{\mathbb{F}_q} \\ &= \dim_{\mathbb{F}_q}(S_j \cap U) + \dim_{\mathbb{F}_q}(S_j \cap D') - w(Q) \\ &\geq 2j + t - w(P) + 2(n-j) - w(Q) \\ &\geq 2j + n + 1 - j + 2(n-j) - n + j = 2n + 1\,, \end{aligned}$$

a contradiction. □

We are now able to prove the following theorem.

Theorem 3.5. *Two semifields $\mathbb{S}_j$ and $\mathbb{S}_{j'}$, with $j \neq j'$ $(j, j' \geq \frac{n+1}{2})$ are not isotopic.*

Proof. By way of contradiction, suppose that $\mathbb{S}_j$ and $\mathbb{S}_{j'}$, with $j \neq j'$ (where $j, j' \geq \frac{n+1}{2}$) are isotopic. Then there exists an invertible semilinear map Γ of type $(\Diamond)$ such that $S_j^\Gamma = S_{j'}$. If φ is the collineation of $\mathbb{P}$ induced by Γ, then $L(\mathbb{S}_j)^\varphi = L(\mathbb{S}_{j'})$ and by Lemma 3.4 φ fixes the line r. This means that, by Property 2.4, the line $r^\varphi = r$ has weight j in $L(\mathbb{S}_j)^\varphi = L(\mathbb{S}_{j'})$, a contradiction. □

By Theorems 3.2 and 3.5 the semifields of type $(q^{2n}, q^n, q^2, q^2, q)$, n odd, are partitioned into $\frac{n-1}{2}$ not isotopic (potential) families: $\mathcal{G}_{\frac{n+1}{2}}(q,n), \mathcal{G}_{\frac{n+3}{2}}(q,n), \ldots, \mathcal{G}_{n-1}(q,n)$, according with the form of their multiplication as explained in Theorem 3.2.

Theorem 3.6. *The families $\mathcal{G}_j(q,n)$, $\frac{n+1}{2} \leq j \leq n-1$, are closed under the transpose and the translation dual operations.*

Proof. Let $\mathbb{S}_j = (\mathbb{F}_{q^{2n}}, +, \circ)$ be a semifield belonging to $\mathcal{G}_j(q,n)$ $(\frac{n+1}{2} \leq j \leq n-1)$. Since the transpose operation leaves invariant the order of the left nucleus and interchanges the order of the right and middle nuclei [17], while the translation dual operation leaves invariant the order of the nuclei [18, Theorem 5.3], then $\mathbb{S}_j^T$ and $\mathbb{S}_j^\perp$ are semifields of type $(q^{2n}, q^n, q^2, q^2, q)$ as well. Also, by Theorem 3.2 and by Theorem 2.5 we get that $\mathbb{S}_j^T$ belongs to the family $\mathcal{G}_j(q,n)$. Similarly, by Property 2.6 and Lemma 3.4, $L(\mathbb{S}_j^\perp)$ contains a unique line of $\mathbb{P}$ and such a line has weight j in $L(\mathbb{S}_j^\perp)$. Thus $\mathbb{S}_j^\perp$ belongs to the family $\mathcal{G}_j(q,n)$ as well. □

In the case $n = 3$, it turns out that we have a unique family of semifields of type $(q^{2n}, q^n, q^2, q^2, q)$, namely, $\mathcal{G}_2(q,3)$. There exist examples of such semifields for any value of q; moreover semifields belonging to $\mathcal{G}_2(q,3)$ were completely classified in [10].

By Theorem 3.2 and by Remark 3.3, there exists a semifield of type $\mathbb{S}_j = (\mathbb{F}_{q^{2n}}, +, \circ)$ (n odd) if there exists an $\mathbb{F}_{q^2}$-basis $\{1, a_2, \ldots, a_j, b, bb'_2, \ldots, bb'_{n-j}\}$ of $\mathbb{F}_{q^{2n}}$ satisfying condition (4). In [11], it has been proven that if u is an element of $\mathbb{F}_{q^n}$ not belonging to any proper subfield of $\mathbb{F}_{q^n}$ and b is an element of $\mathbb{F}_{q^{2n}}$ such that $b^{q^n+1} = A + Bu + Cu^2$ $(A, B, C \in \mathbb{F}_q)$ with either $C = 0$ and $B \neq 0$ or $C \neq 0$ and the polynomial $f(x) = A + Bx + Cx^2 \in \mathbb{F}_q[x]$ having two distinct roots in $\mathbb{F}_q$, then $\{1, u, u^2, \ldots, u^{\frac{n-1}{2}}, b, bu, bu^2, \ldots, bu^{\frac{n-3}{2}}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ satisfying condition (4) and the corresponding semifield $\mathbb{S}_{\frac{n+1}{2}}$ has center $\mathbb{F}_q$. Hence we have the following theorem.

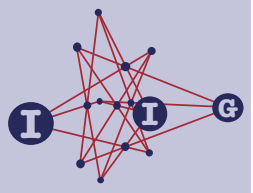
Theorem 3.7. *The family $\mathcal{G}_{\frac{n+1}{2}}(q, n)$ is not empty for any odd n and for any value of q.*

The examples exhibited above (JMPT semifields of List **(L)**) are obtained in [11] generalizing the cyclic semifields (JJ semifields of List **(L)**), and they are either cyclic semifields or isotopic to cyclic semifields. However, in the same paper, by using the computer algebra software MAGMA, two new examples of semifields of type $\mathbb{S}_{\frac{n+1}{2}}$ for $n = 5$ of orders 2^{10} and 4^{10} with centers $\mathbb{F}_2$ and $\mathbb{F}_4$, respectively, have been exhibited (JMPT(4^5,16^5) semifields of **(L)**). Such examples are neither cyclic nor isotopic to cyclic semifields.

In [16] a potential family of semifields of type $(q^{2n}, q^n, q^2, q^2, q)$, n odd, has been introduced and in [20, Section 2] it has been proved that such semifields are of type $\mathbb{S}_{n-1}$. Also in [20], examples of semifields belonging to $\mathcal{G}_{n-1}(q, n)$ for $n = 5$ and $q = 2$ are exhibited (MT semifields of List **(L)**).

If $n \geq 7$, Theorem 3.2 provides other potential families of new semifields of type $(q^{2n}, q^n, q^2, q^2, q)$, n odd. Indeed, we will prove that any possible semifield belonging to $\mathcal{G}_{\frac{n+3}{2}}, \mathcal{G}_{\frac{n+5}{2}}, \ldots, \mathcal{G}_{n-2}$ would be new. More precisely, we show any such semifield would not be isotopic to any known semifield nor isotopic to any derivative of a known semifield. Here, a derivative of a semifield $\mathbb{S}$ is, up to isotopy, a semifield obtained from $\mathbb{S}$ either by a Knuth operation (see [13]) or by the translation dual operation.

Below we list the known examples of semifields (the classes are not necessarily disjoint, see C and D). This list comes from [9, Chapter 37].



(L) LIST OF KNOWN SEMIFIELDS

B Knuth binary commutative semifields

F Flock semifields and their 5th cousins:

- **F_1** Kantor-Knuth
- **F_2** Cohen-Ganley, 5th cousin: Payne-Thas.
- **F_3** Penttila-Williams symplectic semifield order 3^5, 5th cousin, Bader, Lunardon, Pinneri flock semifield

C Commutative semifields/symplectic semifields.

- **C_1** Kantor-Williams Desarguesian Scions (symplectic), Kantor-Williams commutative semifields
- **C_2** Ganley commutative semifields and symplectic cousins
- **C_3** Coulter-Matthews commutative semifields and symplectic cousins

D Generalized Dickson/Knuth/Hughes-Kleinfeld semifields

S Sandler semifields

JJ Jha-Johnson cyclic semifields (gen. Sandler, also of type $S(\omega, m, n)$)

JMPT Johnson-Marino-Polverino-Trombetti semifields (generalizes Jha-Johnson type $S(\omega, 2, n)$-semifields)

JMPT$(4^5, 16^5)$ Johnson-Marino-Polverino-Trombetti non-cyclic semifields of order 4^5 and order 16^5

T Generalized twisted fields

JH Johnson-Huang 8 semifields of order 8^2

CF Cordero-Figueroa semifield of order 3^6

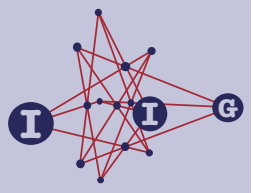
Recently, in [5], [6], [7] and [20] the following semifields have been constructed.

EMPT of order q^{2n}, n odd Ebert-Marino-Polverino-Trombetti semifields of type (q^{2n}, q^n, q, q, q) for any odd integer $n > 2$ and any prime power q

EMPT of order q^{2n}, n even Ebert-Marino-Polverino-Trombetti semifields of type $(q^{2n}, q^n, q^2, q^2, q)$ for any even integer $n > 2$ and any odd prime power q

EMPT of order q^6 Ebert-Marino-Polverino-Trombetti semifields of type (q^6, q^3, q^2, q, q) and semifields of type (q^6, q^3, q, q^2, q) for any odd prime power q

MT Marino-Trombetti semifield of order 2^{10}



We notice that the last example belongs to the family $\mathcal{G}_{n-1}(q,n)$ for $q=2$ and $n=5$.

Theorem 3.8. *Semifields belonging to* $\mathcal{G}_{\frac{n+3}{2}}(q,n)$, $\mathcal{G}_{\frac{n+5}{2}}(q,n)$, $\ldots$, $\mathcal{G}_{n-2}(q,n)$ *(with* n *odd* ≥ 5*) are new, if they exist.*

Proof. First we prove that no semifield of the previous list nor any derivative of such a semifield is of type (q^{2n},q^n,q^2,q^2,q), $n\geq 5$ odd, apart from the JJ, JMPT, JMPT$(4^5,16^5)$ and MT semifields.

Recall that the Knuth operations permute the nuclei of a given semifield with certain rules as shown in [17] and that the translation dual operation leaves the sizes of the nuclei invariant [18]. A symplectic semifield and hence a flock semifield (which is the translation dual of a symplectic semifield two-dimensional over its left nucleus) has right and middle nuclei both isomorphic to the center [12, 17]; whereas a semifield isotopic to a commutative semifield has left and right nuclei both isomorphic to the center. Hence no semifield of type B, F, C listed above nor any of their derivatives is of type (q^{2n},q^n,q^2,q^2,q).

Since a Knuth semifield D of type (17), (18) or (19) (see [4, p. 241]) is 2-dimensional over at least two of its nuclei and since a Knuth semifield of type (20) (see [4, p. 242]) has the three nuclei equal to the center, no Knuth semifield of type (17), (18), (19) or (20) nor any of their derivatives is of type (q^{2n},q^n,q^2,q^2,q).

Straightforward computations show that the Knuth operations map a generalized Dickson semifield (see [4, p. 241, multiplication (15)]) to a generalized Dickson semifield. So, to prove that none of the derivatives of a generalized Dickson semifield is of type (q^{2n},q^n,q^2,q^2,q) (n odd), it suffices to show that a generalized Dickson semifield which is two dimensional over its left nucleus, is not of type (q^{2n},q^n,q^2,q^2,q) (n odd). To this aim, observe that a generalized Dickson semifield of order q^2 is 2-dimensional over its left nucleus $\mathbb{F}_q$ when $\alpha=\mathrm{id}$. If $\sigma=\beta$ and $\sigma=\beta^{-1}$ then multiplication (15) coincides with the multiplication of a Knuth semifield of type (18). Hence, let either $\sigma\neq\beta$ or $\sigma\neq\beta^{-1}$. In this case, we easily get that the nuclei of the generalized Dickson semifield are as follows: $\mathbb{N}_r=\mathrm{Fix}(\sigma\beta)\leqslant\mathbb{N}_l=\mathbb{F}_q$, $\mathbb{N}_m=\mathrm{Fix}(\beta\sigma^{-1})\leqslant\mathbb{N}_l=\mathbb{F}_q$ and $\mathcal{K}=\mathbb{F}_q\cap\mathrm{Fix}(\sigma)\cap\mathrm{Fix}(\beta)$. Such a semifield can not be of type $(q'^{2n},q'^n,q'^2,q'^2,q')$ for any n odd.

Next, a Sandler semifield has order q^{m^2}, with left nucleus and center of order q (see [4, p. 243] and [21, Thm. 1]); hence, again by comparing the nuclei, one can see that Sandler semifields and their derivatives are not of type (q^{2n},q^n,q^2,q^2,q) (n odd).

Also, the multiplication of a generalized twisted field of order q depends on two automorphisms of $\mathbb{F}_q$, say S and T with $S\neq\mathrm{id}$, $T\neq\mathrm{id}$ and $S\neq T$

and $|\mathbb{N}_l| = |\mathrm{Fix}\ T|$, $|\mathbb{N}_r| = |\mathrm{Fix}\ S|$ and $|\mathbb{N}_m| = |\mathrm{Fix}\ ST^{-1}|$ (see [1, Lemma 1]). If either a generalized twisted field or any of its derivatives were of type $(q^{2n}, q^n, q^2, q^2, q)$ (n odd), it would have order s^{2n} (n odd), two of its nuclei would have order s^2 and the third nucleus would have order s^n; and this is not possible. Finally, JH and CF semifields are not of type $(q^{2n}, q^n, q^2, q^2, q)$ with ($n \geq 5$ odd) because of their orders.

Now, recall that JJ, JMPT and JMPT$(4^5, 16^5)$ semifields belong to $\mathcal{G}_{\frac{n+1}{2}}(q, n)$ and that the MT semifield belongs to $\mathcal{G}_{n-1}(q, n)$. So, by these arguments and by Theorems 3.2 and 3.6, the assertion now follows. □

4. The question of isotopisms

From Lemma 3.4, it follows that if $\mathbb{S}_j$ and $\mathbb{S}'_j$ ($\frac{n+1}{2} \leq j \leq n-1$) are two isotopic semifields of the family $\mathcal{G}_j(q, n)$, then there exists an element φ of the group G such that $L(\mathbb{S}_j)^\varphi = L(\mathbb{S}'_j)$ and $r^\varphi = r$, where r is the line of $\mathbb{P}$ defined by $D = \{aI \mid a \in \mathbb{F}_{q^{2n}}\}$. Hence, as in [5, Prop. 5.2 and Prop. 5.4], we get the following result.

Theorem 4.1. *The spread sets*

$$S_j = \{x \mapsto (\alpha_1 + \alpha_2 a_2 + \cdots + \alpha_j a_j)\, x + b(\beta_1 + \beta_2 b_2 + \cdots + \beta_{n-j} b_{n-j})\, x^{q^n} \mid \alpha_i, \beta_i \in \mathbb{F}_{q^2}\}$$

and

$$S'_j = \{x \mapsto (\alpha_1 + \alpha_2 a'_2 + \cdots + \alpha_j a'_j)\, x + b'(\beta_1 + \beta_2 b'_2 + \cdots + \beta_{n-j} b'_{n-j})\, x^{q^n} \mid \alpha_i, \beta_i \in \mathbb{F}_{q^2}\}$$

define isotopic semifields if and only if there exist $\lambda \in \mathbb{F}^*_{q^{2n}}$, $M \in \mathbb{F}^*_{q^{2n}}$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^{2n}})$ such that

$$\lambda[1, a_2^\sigma, \ldots, a_j^\sigma]_{\mathbb{F}_{q^2}} = [1, a'_2, \ldots, a'_j]_{\mathbb{F}_{q^2}} \quad \text{and}$$
$$\lambda b^\sigma M^{q^n-1}[1, b_2^\sigma, \ldots, b_{n-j}^\sigma]_{\mathbb{F}_{q^2}} = b'[1, b'_2, \ldots, b'_{n-j}]_{\mathbb{F}_{q^2}}.$$ □

5. Computational results

In this final section we prove that there exist examples of semifields of type $(q^{2n}, q^n, q^2, q^2, q)$, n odd, not belonging to $\mathcal{G}_{\frac{n+1}{2}}$ and $\mathcal{G}_{n-1}$; indeed we will provide some examples of semifields belonging to $\mathcal{G}_{n-2}(q, n)$ for $q = 2$ and $n = 7$.

By Theorem 3.2 and Remark 3.3, if $n = 7$ a semifield belonging to the family $\mathcal{G}_5(q, 7)$ is of type $\mathbb{S}_5 = (\mathbb{F}_{q^{14}}, +, \circ)$ with multiplication given by

$$x \circ y = (\alpha_1 + \alpha_2 a_2 + \alpha_3 a_3 + \alpha_4 a_4 + \alpha_5 a_5)x + b(\beta_1 + \beta_2 B)x^{q^7}, \tag{5}$$

where $a_i, b, B \in \mathbb{F}_{q^{14}}$ such that

$$\begin{cases} \{1, a_2, \ldots, a_5, b, bB\} \text{ is an } \mathbb{F}_{q^2}\text{-basis of } \mathbb{F}_{q^{14}}, \\ N(b) = b^{q^7+1} \notin P(1, a_2 \ldots a_5, B), \end{cases} \tag{6}$$

where

$$P(1, a_2, \ldots, a_5, B) = \left\{ \left(\frac{\alpha_1 + \alpha_2 a_2 + \cdots + \alpha_5 a_5}{\beta_1 + \beta_2 B} \right)^{q^7+1} \;\middle|\; \alpha_i, \beta_i \in \mathbb{F}_{q^2}, \; (\beta_1, \beta_2) \neq (0, 0) \right\}.$$

Let $B' = \frac{\alpha+\beta B}{\gamma+\delta B}$ with $\alpha, \beta, \gamma, \delta \in \mathbb{F}_{q^2}$ such that $\alpha\delta - \beta\gamma \neq 0$. If $\lambda \in \mathbb{F}_{q^2}^*$, $\sigma = \mathrm{id}$ and $b' = b(\gamma + \delta B)$, we get

$$\lambda[1, a_2, a_3, \ldots, a_5]_{\mathbb{F}_{q^2}} = [1, a_2, a_3, \ldots, a_5]_{\mathbb{F}_{q^2}}$$

and

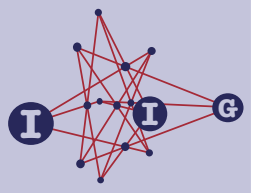
$$\lambda b[1, B] = \lambda b(\gamma + \delta B)\left[1, \frac{\alpha + \beta B}{\gamma + \delta B}\right]_{\mathbb{F}_{q^2}} = b'[1, B']_{\mathbb{F}_{q^2}}.$$

Hence it follows from Theorem 4.1 that a semifield $\mathbb{S}_5'$ defined by the basis $\{1, a_2, \ldots, a_5, b', b'B'\}$, if it exists, would be isotopic to the semifield $\mathbb{S}_5$ defined by the basis $\{1, a_2, \ldots, a_5, b, bB\}$.

Now let $q = 2$ and ω be a primitive element of $\mathbb{F}_{2^7}$ with minimal polynomial $x^7 + x + 1 \in \mathbb{F}_2[x]$ and let z be a primitive element of $\mathbb{F}_{2^{14}}$ with minimal polynomial $x^{14} + x^7 + x^5 + x^3 + 1 \in \mathbb{F}_2[x]$. We look for elements $B \in \mathbb{F}_{2^{14}} \setminus \mathbb{F}_{2^2}$ for which there exists $b \in \mathbb{F}_{2^{14}}^*$ such that $N(b) \notin P(1, \omega, \omega^2, \omega^3, \omega^4, B)$. If B is such an element and $b \in \mathbb{F}_{2^{14}}^*$ with $N(b) \notin P(1, \omega, \omega^2, \omega^3, \omega^4, B)$, we denote by $\mathbb{S}_{\omega,b,B}$ the corresponding semifield. By the previous arguments, for any $B' = \frac{\alpha+\beta B}{\gamma+\delta B}$, with $\alpha, \beta, \gamma, \delta \in \mathbb{F}_{2^2}$ and $\alpha\delta - \beta\gamma \neq 0$, the semifield $\mathbb{S}_{\omega,b',B'}$, with $b' = b(\gamma + \delta B)$, is isotopic to $\mathbb{S}_{\omega,b,B}$.

Given two elements $B, B' \in \mathbb{F}_{2^{14}} \setminus \mathbb{F}_{2^2}$, we say that B and B' are $\mathbb{F}_{2^2}$-*equivalent* if there exist $\alpha, \beta, \gamma, \delta \in \mathbb{F}_{2^2}$ with $\alpha\delta - \beta\gamma \neq 0$ such that $B' = \frac{\alpha+\beta B}{\gamma+\delta B}$. Note that such a relation is an equivalence relation.

In light of these remarks, MAGMA computations [2] show that the elements $B \in \mathbb{F}_{2^{14}} \setminus \mathbb{F}_{2^2}$ producing a semifield $\mathbb{S}_{\omega,b,B}$ for some $b \in \mathbb{F}_{2^{14}}^*$, up to the above



equivalence relation, are those listed in Table 1. For each such B there exists exactly one element $\eta \in \mathbb{F}_{2^7} \setminus P(1, \omega, \omega^2, \omega^3, \omega^4)$ and such an element is listed in the second column of Table 1. So, for each element $b \in \mathbb{F}_{2^{14}}$ such that $N(b) = \eta$, we get a semifield of type $\mathbb{S}_{\omega,b,B}$.

B	$N(b)$
$B_1 = z^{1647}$	$\eta_1 = \omega^{21}$
$B_2 = z^{106}$	$\eta_2 = \omega^{40}$
$B_3 = z^{122}$	$\eta_3 = \omega^{50}$
$B_4 = z^{441}$	$\eta_4 = \omega^{19}$

Table 1

Also, if $B_i \neq B_j$ $(i, j \in \{1, 2, 3, 4\})$, then B_i and B_j are not $\mathbb{F}_{2^2}$-equivalent. Note that, if $b, b' \in \mathbb{F}_{2^{14}}^*$ such that $N(b) = N(b')$, then there exists $\overline{M} \in \mathbb{F}_{2^{14}}^*$ with $b' = \overline{M}^{2^7-1} b$ and, hence, $\mathbb{S}_{\omega,b,B}$ and $\mathbb{S}_{\omega,b',B}$ are isotopic (see Theorem 4.1 with $\lambda = 1$, $\sigma = \mathrm{id}$ and $M = \overline{M}$). Then, for any $i \in \{1, 2, 3, 4\}$, the pair (B_i, η_i) defines, up to isotopy, a unique semifield of type $\mathbb{S}_{\omega,b_i,B_i}$, where $N(b_i) = \eta_i$. Hence there exist at most 4 semifields of type $\mathbb{S}_{\omega,b,B}$, up to isotopy.

Now suppose that the two semifields of type $\mathbb{S}_{\omega,b,B}$ and $\mathbb{S}_{\omega,b',B'}$ are isotopic. Then there exist $\lambda \in \mathbb{F}_{2^{14}}^*$, $M \in \mathbb{F}_{2^{14}}^*$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{2^{14}})$ such that

$$\lambda[1, \omega^\sigma, \omega^{2\sigma}, \omega^{3\sigma}, \omega^{4\sigma}]_{\mathbb{F}_{q^2}} = [1, \omega, \omega^2, \omega^3, \omega^4]_{\mathbb{F}_{2^2}} \tag{7}$$

and

$$\lambda b^\sigma M^{2^{14}-1}[1, B]_{\mathbb{F}_{q^2}} = b'[1, B']_{\mathbb{F}_{2^2}} . \tag{8}$$

If $\sigma : x \mapsto x^2$, condition (7) becomes

$$\lambda[1, \omega^2, \omega^4, \omega^6, \omega^8]_{\mathbb{F}_{2^2}} = [1, \omega, \omega^2, \omega^3, \omega^4]_{\mathbb{F}_{2^2}} ,$$

and since $\omega^7 + \omega + 1 = 0$ it is equivalent to say that

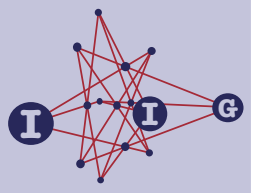
$$\lambda[1, \omega, \omega^2, \omega^4, \omega^6]_{\mathbb{F}_{2^2}} = [1, \omega, \omega^2, \omega^3, \omega^4]_{\mathbb{F}_{2^2}} ,$$

and this easily implies that $\lambda = 0$, a contradiction. In a similar way, we get a contradiction for any $\sigma \in \mathrm{Aut}(\mathbb{F}_{2^{14}})$ with $\sigma \neq \mathrm{id}$.

On the other hand, if $\sigma = \mathrm{id}$, straightforward computations show that if conditions (7) and (8) are satisfied then

$$\lambda \in \mathbb{F}_{2^2}^* , \quad B' = \frac{\alpha + \beta B}{\gamma + \delta B} , \quad b' = bM^{2^{14}-1}(\gamma + \delta B) ,$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{F}_{2^2}$ and $\alpha\delta - \beta\gamma \neq 0$, i.e. B and B' are $\mathbb{F}_{2^2}$-equivalent. So we get the following result.



Theorem 5.1. *The semifields* $\mathbb{S}_{\omega,b,B} = (\mathbb{F}_{2^{14}}, +, \circ)$ *and* $\mathbb{S}_{\omega,b',B'} = (\mathbb{F}_{2^{14}}, +, \circ)$ *with multiplication*

$$x \circ y = (\alpha_1 + \alpha_2\omega + \cdots + \alpha_5\omega^4)\, x + b(\beta_1 + \beta_2 B)\, x^{2^7} \quad \textit{and}$$
$$x \circ y = (\alpha_1 + \alpha_2\omega + \cdots + \alpha_5\omega^4)\, x + b'(\beta_1 + \beta_2 B')\, x^{2^7},$$

respectively, are isotopic if and only if

$$B' = \frac{\alpha + \beta B}{\gamma + \delta B} \quad \textit{and} \quad b' = bM^{2^{14}-1}(\gamma + \delta B),$$

for some $M \in \mathbb{F}_{2^{14}}^*$, *where* $\alpha, \beta, \gamma, \delta \in \mathbb{F}_{2^2}$ *and* $\alpha\delta - \beta\gamma \neq 0$. □

As a corollary we have:

Corollary 5.2. *The semifields* $\mathbb{S}_{\omega,b_i,B_i}$, $i \in \{1, 2, 3, 4\}$, *are pairwise non-isotopic.* □

Also, by the previous arguments and by Theorem 3.8, we get the following result.

Theorem 5.3. *In the family* $\mathcal{G}_5(2, 7)$ *there exist at least four non-isotopic semifields, and they are new.* □

References

[1] **A.A. Albert**, Finite division algebras and finite planes, *Proc. Sympos. Appl. Math.* **10** (1960), 53–70.

[2] **J. Cannon** and **C. Playoust**, *An introduction to MAGMA*, University of Sydney Press, Sydney (1993).

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

[4] **P. Dembowski**, *Finite Geometries*, Springer Verlag, Berlin (1968).

[5] **G. Ebert**, **G. Marino**, **O. Polverino** and **R. Trombetti**, New infinite families of semifields, submitted.

[6] _____, On the multiplication of some semifields of order q^6, *Finite Fields Appl.*, to appear.

[7] _____, Semifields in class $\mathcal{F}_4^{(a)}$, submitted.

[8] **N.L. Johnson** and **V. Jha**, 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** no. 1 (1989), 1–35.

[9] **N.L. Johnson**, **V. Jha** and **M. Biliotti**, *Handbook of Finite Translation Planes*, Pure and Applied Mathematics, Taylor Books, 2007.

[10] **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** no. 2 (2008), 456–469

[11] _____, On a generalization of cyclic semifields, *J. Algebraic Combin.*, to appear (available on line DOI 10.1007/s10801-007-0116-x).

[12] **N.L. Johnson** and **O. Vega**, Symplectic spreads and symplectically paired spreads, *Note Mat.* **26** (2006), 105–111.

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

[14] **R. Lidl** and **H. Niederreiter**, *Finite fields*, Encyclopedia Math. Appl. **20**, Addison-Wesley, Reading (1983) (Now distributed by Cambridge University Press).

[15] **G. Lunardon**, Translation ovoids, *J. Geom.* **76** (2003), 200–215.

[16] _____, Semifields and linear sets of $\mathrm{PG}(1, q^t)$, *Quad. Mat.*, to appear.

[17] _____, Symplectic spreads and finite semifields, *Des. Codes Cryptogr.* **44** no. 1–3 (2007), 39–48.

[18] **G. Lunardon**, **G. Marino**, **O. Polverino** and **R. Trombetti**, Translation dual of a semifield, *J. Combin. Theory Ser. A* **115** (2008), no. 8, 1321–1332.

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

[20] **G. Marino** and **R. Trombetti**, A new semifield of order 2^{10}, submitted.

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

Giuseppe Marino

Dipartimento di Matematica, Seconda Università degli Studi di Napoli, Via Vivaldi, 43, 81100 Caserta, Italy

e-mail: giuseppe.marino@unina2.it

Olga Polverino

Dipartimento di Matematica, Seconda Università degli Studi di Napoli, Via Vivaldi, 43, 81100 Caserta, Italy

e-mail: olga.polverino@unina2.it

Rocco Tromebtti

Dipartimento di Matematica e Applicazioni, Università degli Studi di Napoli "Federico II", Via Cintia, 80126 Napoli, Italy,

e-mail: rtrombet@unina.it