A generalization of some Huang–Johnson semifields

N.L. Johnson
Mathematics Dept.
University of Iowa
Iowa City, Iowa 52242, USA
njohnson@math.uiowa.edu

Giuseppe Marino*
Dipartimento di Matematica
Seconda Università degli Studi di Napoli
I– 81100 Caserta, Italy
giuseppe.marino@unina2.it

Olga Polverino*
Dipartimento di Matematica
Seconda Università degli Studi di Napoli
I– 81100 Caserta, Italy
olga.polverino@unina2.it

Rocco Trombetti*
Dipartimento di Matematica e Applicazioni
Università degli Studi di Napoli "Federico II"
I– 80126 Napoli, Italy
rtrombet@unina.it

Submitted: May 19, 2010; Accepted: Jan 25, 2011; Published: Feb 4, 2011
Mathematics Subject Classification: 12K10 51A40 51E99

Abstract

In [H. Huang, N.L. Johnson: Semifield planes of order 8^2, *Discrete Math.*, **80** (1990)], the authors exhibited seven sporadic semifields of order 2^6, with left nucleus $\mathbb{F}_{2^3}$ and center $\mathbb{F}_2$. Following the notation of that paper, these examples are referred as the Huang–Johnson semifields of type II, III, IV, V, VI, VII and $VIII$. In [N. L. Johnson, V. Jha, M. Biliotti: *Handbook of Finite Translation Planes*, Pure and Applied Mathematics, Taylor Books, 2007], the question whether these semifields are contained in larger families, rather then sporadic, is posed. In this paper, we first prove that the Huang–Johnson semifield of type VI is isotopic to a cyclic semifield, whereas those of types VII and $VIII$ belong to infinite families recently constructed in [N.L. Johnson, G. Marino, O. Polverino, R. Trombetti: Semifields of order q^6 with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$, *Finite Fields Appl.*, **14** (2008)] and [G.L. Ebert, G. Marino, O. Polverino, R. Trombetti: Infinite families of new semifields, *Combinatorica*, **6** (2009)]. Then, Huang–Johnson semifields of type II and III are extended to new infinite families of semifields of order q^6, existing for every prime power q.

*This work was supported by the Research Project of MIUR (Italian Office for University and Research) "Geometrie su Campi di Galois, piani di traslazione e geometrie di incidenza" and by the Research group GNSAGA of INDAM

1 Introduction

The term semifield is used to describe an algebraic structure with at least two elements and two binary operations, satisfying all axioms for a skewfield except (possibly) associativity of the multiplication. In this paper we are only interested in the finite case. For this reason, in what follows, the term semifield will always stand for finite semifield. One of the major reasons behind the great interest towards semifields during the sixties was the discovery that they can be used to coordinatize a class of affine (and hence projective) planes; in fact, the so called semifield planes. Very recently the theory of finite semifields has received an even greater attention stimulated by the connection that they have with other areas of discrete mathematics like coding theory and cryptography (see e.g. the chapter [15] in the collected work [3]).

A finite field is a trivial example of semifield and it is easy to see that, in general, the order of a proper semifield is a power of a prime number p. Such a prime is also called the *characteristic* of the semifield. The additive group of a semifield of characteristic p is an elementary abelian p–group and it is always possible to choose the support of the algebraic structure to be the finite field $\mathbb{F}_q$, $q = p^h$. This can be done in such a way that the semifield addition equals the field addition while the multiplication is defined by a rule in which appear both addition and multiplication of the field. In [13], the author tabulated all proper semifields of order 16. There are 23 non–isomorphic proper semifields of that order. In [14, Section 2], Knuth exhibits two examples of semifields over the field $\mathbb{F}_{2^4}$ which he refers as systems **V** and **W**. All semifields of order 16 are either isotopic to system **V** or isotopic to system **W**. Also, in [14], generalizing the work done by Dickson in [5], he constructs four infinite families of semifields of order p^m (p odd or even) where m is an even integer, in fact families $K.I$, $K.II$, $K.III$ and $K.IV$, showing that system **V** belongs to family $K.I$ and system **W** belongs to all four families.

In 1990 Huang and Johnson exhibited seven sporadic semifields of order 64, with left nucleus $\mathbb{F}_{2^3}$ and center $\mathbb{F}_2$: the Huang–Johnson semifields of type II, III, IV, V, VI, VII and $VIII$ [8]. These were constructed in the geometric setting of translation planes. In fact, in [8], the authors were mainly interested in the complete determination of all translation planes of order 64 with kernel isomorphic to $\mathbb{F}_{2^3}$ admitting a subgroup of order $2 \cdot 64$ in their linear translation complement. These translation planes turned out to be semifield planes and the semifields which coordinates them are the above mentioned semifields of Huang and Johnson. In [11, p. 281], the authors posed the question whether these seven examples could be extended to larger, possibly infinite, families. We answer this question by proving that some of Huang–Johnson semifields are contained into infinite families as in the case of systems **V** and **W**. Precisely, we prove that Huang–Johnson semifield of type VI is isotopic to a cyclic semifield of type $(q, 2, 3)$ introduced by Jha and Johnson in [9] and Huang–Johnson semifields of type VII and $VIII$ belong to the infinite families $\mathcal{F}_{IV}$ and $\mathcal{F}_V$ recently constructed in [6]. Nevertheless, we construct new infinite families of semifields containing examples for any even and odd prime power q, proving that semifields of type II and III belong to such families.

The technique used in the paper are heavily based on properties of linear sets of projective spaces. For more details on the theory of linear sets we refer to [20].

2 Preliminary Results

A *semifield* $\mathbb{S}$ is an algebraic structure satisfying all the axioms for a skewfield except (possibly) associativity. The subsets $\mathbb{N}_l = \{a \in \mathbb{S} \,|\, (ab)c = a(bc),\ \forall b, c \in \mathbb{S}\}$, $\mathbb{N}_m = \{b \in \mathbb{S} \,|\, (ab)c = a(bc),\ \forall a, c \in \mathbb{S}\}$, $\mathbb{N}_r = \{c \in \mathbb{S} \,|\, (ab)c = a(bc),\ \forall a, b \in \mathbb{S}\}$ and $\mathcal{K} = \{a \in \mathbb{N}_l \cap \mathbb{N}_m \cap \mathbb{N}_r \,|\, ab = ba,\ \forall b \in \mathbb{S}\}$ are skewfields which are known, respectively, as the *left nucleus*, *middle nucleus*, *right nucleus* and *center* of the semifield. A semifield is a vector space over its nuclei and its center.

If $\mathbb{S}$ satisfies all the axioms for a semifield, except that it does not have an identity element under multiplication, then $\mathbb{S}$ is called a *presemifield*. Two presemifields, say $\mathbb{S} = (\mathbb{S}, +, *)$ and $\mathbb{S}' = (\mathbb{S}', +, \circ)$ with the same characteristic p, are said to be *isotopic* if there exist three invertible $\mathbb{F}_p$-linear maps g_1, g_2, g_3 from $\mathbb{S}$ to $\mathbb{S}'$ such that

$$g_1(x) \circ g_2(y) = g_3(x * y)$$

for all $x, y \in \mathbb{S}$. From any presemifield, one can naturally construct a semifield which is isotopic to it (see [14]). Moreover, a presemifield $\mathbb{S}$, viewed as a vector space over some prime field $\mathbb{F}_p$, can be used to coordinatize an affine (and hence a projective) plane of order $|\mathbb{S}|$ (see [4]). Albert [1] showed that the projective planes coordinatized by the presemifields $\mathbb{S}$ and $\mathbb{S}'$ are isomorphic if and only if $\mathbb{S}$ and $\mathbb{S}'$ are isotopic. Any projective plane $\pi(\mathbb{S})$ coordinatized by a semifield (or presemifield) is called a *semifield plane*. If $\pi(\mathbb{S})$ is a semifield plane, then the dual plane is a semifield plane as well, and the semifield (or presemifield) coordinatizing it is called *transpose* of $\mathbb{S}$ and is denoted by $\mathbb{S}^t$.

Let b be an element of a semifield $\mathbb{S} = (\mathbb{S}, +, *)$; then the map $\varphi_b \colon x \in \mathbb{S} \to x * b \in \mathbb{S}$ is a linear map when $\mathbb{S}$ is regarded as a left vector space over $\mathbb{N}_l$. We call the set $S = \{\varphi_b \colon b \in \mathbb{S}\} \subseteq \mathbb{V} = End_{\mathbb{N}_l}(\mathbb{S})$ ([1]) the *semifield spread set of linear maps* of $\mathbb{S}$ (semifield spread set, for short). It satisfies the following properties: *i)* $|S| = |\mathbb{S}|$; *ii)* S is closed under addition and contains the zero map; *iii)* every non–zero map in S is non–singular (that is, invertible). Conversely, any set $\bar{S}$ of $\bar{F}$–linear maps of an $\bar{F}$–vector space $\bar{\mathbb{S}}$ satisfying *i)*, *ii)* and *iii)* defines a presemifield $\bar{\mathbb{S}} = (\bar{\mathbb{S}}, +, *)$ with

$$x * y = \varphi_y(x), \tag{1}$$

where φ_y is the unique element of $\bar{S}$ such that $\varphi_y(e) = y$ (with e a fixed non–zero element of $\bar{\mathbb{S}}$). Also, $\bar{\mathbb{S}}$ is a semifield whose identity is e, if and only if the identity map belongs to $\bar{S}$. In the latter case the left nucleus of $\bar{\mathbb{S}}$ contains $\bar{F}$.

Let $\mathbb{S} = (\mathbb{S}, +, *)$ be a semifield with center $\mathcal{K}$, then the semifield spread set S of $\mathbb{S}$ is a $\mathcal{K}$–vector space. In what follows we will always assume that the semifields under consideration have as center the Galois field $\mathbb{F}_q$. If $\mathbb{S}$ is 2-dimensional over its left nucleus $\mathbb{F}_{q^n}$ and $2n$-dimensional over its center $\mathbb{F}_q$, then we can assume that $\mathbb{S} = (\mathbb{F}_{q^{2n}}, +, *)$ and in this case the semifield spread set S is an $\mathbb{F}_q$–vector subspace of $\mathbb{V} = End_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{2n}})$ of

[1] $End_{\mathbb{N}_l}(\mathbb{S})$ denotes the vector space of the endomorphisms of $\mathbb{S}$ over $\mathbb{N}_l$

dimension $2n$. Note that any $\mathbb{F}_{q^n}$–linear map of $\mathbb{F}_{q^{2n}}$ can be uniquely represented in the form

$$\varphi_{\eta,\zeta}\colon \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^{2n}} \quad \text{via} \quad x \to \eta x + \zeta x^{q^n},$$

for some $\eta, \zeta \in \mathbb{F}_{q^{2n}}$; i.e. through a q^n–*polynomial* over $\mathbb{F}_{q^{2n}}$. Hence the $\mathbb{F}_q$–vector space S defines, in the projective space $PG(\mathbb{V}, \mathbb{F}_{q^n}) = PG(3, q^n)$, an $\mathbb{F}_q$–linear set of rank $2n$, namely

$$L(\mathbb{S}) = L(S) = \{\langle \varphi_b \rangle_{\mathbb{F}_{q^n}} : b \in \mathbb{S} \setminus \{0\}\}.$$

Also, since the linear maps defining S are invertible, the linear set $L(S)$ is disjoint from the hyperbolic quadric $\mathcal{Q} = \mathcal{Q}^+(3, q^n)$ of $PG(\mathbb{V}, \mathbb{F}_{q^n})$ defined by the non–invertible maps of $\mathbb{V}$, namely

$$\mathcal{Q} = \{\langle \varphi_{\eta,\zeta} \rangle_{\mathbb{F}_{q^n}} :\ \eta, \zeta \in \mathbb{F}_{q^{2n}}, \eta^{q^n+1} = \zeta^{q^n+1}, (\eta, \zeta) \neq (0,0)\}.$$

Define $\mathcal{G}$ to be the index two subgroup of $Aut(\mathcal{Q})$ which leaves the reguli of $\mathcal{Q}$ invariant. If $\varphi\colon x \mapsto \eta x + \zeta x^{q^n}$, then for any $\tau \in Aut(\mathbb{F}_{q^{2n}})$ let φ^τ denote the $\mathbb{F}_{q^n}$-linear map of $\mathbb{F}_{q^{2n}}$ defined by the rule $\varphi^\tau\colon x \mapsto \eta^\tau x + \zeta^\tau x^{q^n}$.

Now for any non–singular $\mathbb{F}_{q^n}$-linear maps ψ and ϕ of $\mathbb{F}_{q^{2n}}$, define $\mathcal{I} = \mathcal{I}_{\psi\tau\phi}$ to be the collineation of $PG(\mathbb{V}, \mathbb{F}_{q^n})$ induced by the semilinear $\Theta = \Theta_{\psi\tau\phi}$ map on $\mathbb{V}$ whose rule is

$$\Theta :\ \varphi \mapsto \psi\varphi^\tau\phi.$$

Since φ is singular if and only if $\psi\varphi^\tau\phi$ is singular, $\mathcal{I}_{\psi\tau\phi}$ leaves the quadric $\mathcal{Q}$ invariant and

$$\mathcal{G} = \{\mathcal{I}_{\psi\tau\phi} \mid \tau \in Aut(\mathbb{F}_{q^{2n}}),\ \psi, \phi \ \text{ non–singular } \mathbb{F}_{q^n}\text{-linear maps of } \mathbb{F}_{q^{2n}}\}.$$

A version of the following result may be found in [2].

Theorem 2.1. [2, Thm. 2.1] *Let $\mathbb{S} = (\mathbb{F}_{q^{2n}}, +, *)$ and $\mathbb{S}' = (\mathbb{F}_{q^{2n}}, +, *')$ be two semifields with left nucleus $\mathbb{F}_{q^n}$ and let S and S' be the associated semifield spread sets, respectively. Then $\mathbb{S}$ and $\mathbb{S}'$ are isotopic if and only if $L(S') = L(S^\Theta) = L(S)^\mathcal{I}$, for some collineation $\mathcal{I}$ of $\mathcal{G}$.*

Remark 2.2. If Ψ is an invertible semilinear map of $\mathbb{V}$ inducing a collineation in $PG(\mathbb{V}, \mathbb{F}_{q^n})$ interchanging the reguli of the quadric $\mathcal{Q}$, then S^Ψ is a semifield spread set as well and it defines, up to isotopy, the transpose semifield $\mathbb{S}^t$ of $\mathbb{S}$ ([17, Thm. 4.2]).

Fixing an $\mathbb{F}_{q^n}$–basis of $\mathbb{F}_{q^{2n}}$, the vector space $\mathbb{V} = End_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^{2n}})$ can be identified with the vector space of all 2×2 matrices over $\mathbb{F}_{q^n}$; denote it by $\mathbb{M}$. In this setting, the semifeld spread set S is a set of q^{2n} elements of $\mathbb{M}$, closed under addition, containing the zero matrix and whose non–zero elements are invertible. In this case, we say that S is a semifield spread set of matrices associated with $\mathbb{S}$ and since every matrix of S is non–singular, the linear set $L(S)$ of $PG(\mathbb{M}, \mathbb{F}_{q^n})$ is disjoint from the hyperbolic quadric $\mathcal{Q}$ of $PG(\mathbb{M}, \mathbb{F}_{q^n})$ defined by singular 2×2 matrices of $\mathbb{M}$.

By Theorem 2.1, two semifields $\mathbb{S}_1$ and $\mathbb{S}_2$, 2–dimensional over their left nuclei and with center $\mathbb{F}_q$, are isotopic if and only if there exists a semilinear map $\phi\colon X \in \mathbb{M} \mapsto$

$AX^\sigma B \in \mathbb{M}$ (where A and B are two non–singular matrices over $\mathbb{F}_{q^n}$ and $\sigma \in Aut(\mathbb{F}_{q^n})$) such that $S_2 = S_1^\phi$, where S_1 and S_2 are the semifield spread sets of matrices associated with $\mathbb{S}_1$ and $\mathbb{S}_2$, respectively.

Starting from an $\mathbb{F}_q$–linear set $L(S)$ of $\mathbb{P} = PG(3, q^n)$ associated with a semifield 2–dimensional over the left nucleus $\mathbb{F}_{q^n}$ and $2n$ dimensional over the center $\mathbb{F}_q$ and using the polarity $\perp$ induced by the hyperbolic quadric $\mathcal{Q}$ of $\mathbb{P}$, it is possible to construct another $\mathbb{F}_q$–linear set of $\mathbb{P}$, say $L(S)^\perp$, of rank $2n$ which is disjoint from $\mathcal{Q}$ as well. Precisely, let β be the bilinear form arising from the quadric $\mathcal{Q}$ and let $Tr_{q^n/q}$ be the trace function of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The map $Tr_{q^n/q} \circ \beta$ is a non–degenerate $\mathbb{F}_q$–bilinear form of the vector space underlying $\mathbb{P}$, when it is regarded as an $\mathbb{F}_q$–vector space. Denote by $\perp'$ the polarity induced by $Tr_{q^n/q} \circ \beta$. The orthogonal complement $S^\perp$ of S with respect to the $\mathbb{F}_q$–bilinear form $Tr_{q^n/q} \circ \beta$ defines an $\mathbb{F}_q$–linear set $L(S)^\perp := L(S^{\perp'})$ of $\mathbb{P}$ of rank $2n$, which is disjoint from $\mathcal{Q}$ as well. Hence, $S^{\perp'}$ defines a presemifield of order q^{2n} whose associated semifield has left nucleus isomorphic to $\mathbb{F}_{q^n}$ and center isomorphic to $\mathbb{F}_q$. This presemifield is the *translation dual* of $\mathbb{S}$ and is denoted by $\mathbb{S}^\perp$ ([16], [17] and [11, Chapter 85]).

If $T = PG(U, \mathbb{F}_{q^n})$ is a subspace of $\mathbb{P}$ of dimension s, then we define the *weight of T in $L(S)$* to be $\dim_{\mathbb{F}_q}(U \cap S)$, where we are treating U as an $\mathbb{F}_q$–vector subspace. We denote the weight of T in $L(S)$ by the symbol $w_{L(S)}(T)$. In particular a point $P = \langle \underline{v} \rangle_{\mathbb{F}_{q^n}}$ of $\mathbb{P}$ belongs to $L(S)$ if and only if $w_{L(S)}(P) \geq 1$.

Proposition 2.3. *The weight distribution of a linear set associated with a presemifield is invariant up to isotopy and up to the transpose operation.*

Proof. Let $\mathbb{S}_1$ and $\mathbb{S}_2$ be two presemifields with associated spread sets of linear maps S_1 and S_2, respectively. If $\mathbb{S}_1$ is either isotopic to $\mathbb{S}_2$ or isotopic to the transpose of $\mathbb{S}_2$, then by Theorem 2.1 and by Remark 2.2 $S_2 = S_1^\Psi$, where Ψ is an invertible semilinear map of $\mathbb{V}$ fixing the invertible elements of $\mathbb{V}$. Now, noting that an invertible semilinear map of $\mathbb{V}$ preserves the dimension of the $\mathbb{F}_q$–vector subspaces, the result easily follows. □

Now recall the following rule which is a particular case of [20, Proposition 2.6] relating the weights distribution of subspaces pairwise polar with respect to the polarity $\perp$, in the linear sets $L(S)$ and $L(S)^\perp$ of $\mathbb{P} = PG(3, q^n)$:

$$w_{L^\perp(S)}(T^\perp) - w_{L(S)}(T) = 2n - (s+1)n, \tag{2}$$

where T is an s–dimensional subspace of $\mathbb{P}$.

Finally, one property which will be useful in the sequel, proved in [12, Property 3.1], is the following.

Property 2.4. *A line r of $\mathbb{P} = PG(3, q^n)$ is contained in the linear set $L(S)$ if and only if $w_{L(S)}(r) \geq n + 1$.* □

3 Semifields in class $\mathcal{F}_3$

Let $\mathbb{S}$ be a semifield of order q^6 with left nucleus of order q^3 and center of order q and let S be the associated spread set. There are six possible geometric configurations for the associated linear set $L = L(S)$ in $\mathbb{P} = PG(3, q^3)$, as described in [18] and the corresponding classes of semifields are labeled $\mathcal{F}_i$, for $i = 0, 1, \cdots, 5$. The class $\mathcal{F}_4$ has been furtherly partitioned, again geometrically, into three subclasses, denoted $\mathcal{F}_4^{(a)}$, $\mathcal{F}_4^{(b)}$ and $\mathcal{F}_4^{(c)}$ [12]. Semifields belonging to different classes are not isotopic and the families $\mathcal{F}_i$, for $i = 0, 3, 4, 5$ are closed under the transpose and the translation dual operations. The linear set L associated with a semifield in class $\mathcal{F}_3$ has the following structure

($\mathcal{F}_3$) L contains a unique point of weight 2 and does not contain any line of $\mathbb{P}$ or, equivalently, L contains a unique point of weight grater than 1 and such a point has weight 2. In this case L is not contained in a plane and $|L| = q^5 + q^4 + q^3 + q^2 + 1$.

Suppose that $\mathbb{S}$ is a semifield belonging to class $\mathcal{F}_3$. Let S be the associated spread set and let $L(S)$ be the corresponding linear set of $\mathbb{P}$. Let P denote the unique point of $L(S)$ of weight 2. Since $L(S)$ is not contained in a plane, for each plane π of $\mathbb{P}$, we have that $3 \leq w_{L(S)}(\pi) \leq 5$.

Proposition 3.1. *There exists a unique plane π of $\mathbb{P}$ of weight 5 in $L(S)$ and the point P belongs to π. Also, if $\pi \neq P^\perp$, then the weight of the plane $P^\perp$ in $L(S)$ is 3 or 4, whereas the weight of the point $\pi^\perp$ in $L(S)$ is either 0 or 1.*

Proof. By [18, Theorem 4.4] the class $\mathcal{F}_3$ is closed under the translation dual operation, hence $L(S)^\perp$ has a unique point, say R, of weight 2. Now, by Equation (2), $R^\perp = \pi$ is the unique plane of $\mathbb{P}$ of weight 5 in $L(S)$. Also, since the weights of P and π in $L(S)$ are 2 and 5, respectively, and since $L(S)$ has rank 6, we have that P is a point of the plane π. The last part of the statement simply follows from the facts that any plane of $\mathbb{P}$, different from π, has weight 3 or 4 in $L(S)$ and that any point different from P has weight 0 or 1 in $L(S)$. □

Since P and π are the unique point and the unique plane of $\mathbb{P}$ of weight 2 and 5 in $L(S)$, respectively, and since the elements of $\mathcal{G}$ commute with $\perp$, we have that the weights of P, π, $P^\perp$ and $\pi^\perp$ in $L(S)$ are invariant under isotopisms. Hence, the following definition makes sense: a semifield $\mathbb{S}$ belonging to the class $\mathcal{F}_3$, with $\pi \neq P^\perp$, is *of type* (i, j), $i \in \{3, 4\}$ and $j \in \{0, 1\}$, if the weight of $P^\perp$ in $L(S)$ is i and the weight of $\pi^\perp$ in $L(S)$ is j.

Theorem 3.2. *Semifields belonging to $\mathcal{F}_3$, with $P \neq \pi^\perp$, of different types are not isotopic. Also, if a semifield $\mathbb{S}$ of $\mathcal{F}_3$ is of type (i, j), then the transpose semifield $\mathbb{S}^t$ of $\mathbb{S}$ is of type (i, j) as well.*

Proof. It follows from previous arguments and from Proposition 2.3. □

Theorem 3.3. *Let $\mathbb{S}$ be a semifields belonging to $\mathcal{F}_3$, then*

- *if $\mathbb{S}$ is of type $(4,1)$ or $(3,0)$, then its translation dual $\mathbb{S}^\perp$ is of type $(4,1)$ or $(3,0)$, respectively;*
- *if $\mathbb{S}$ is of type $(4,0)$ or $(3,1)$, then its translation dual $\mathbb{S}^\perp$ is of type $(3,1)$ or $(4,0)$, respectively.*

Proof. It is sufficient to recall that the class $\mathcal{F}_3$ is closed under the translation dual operation ([18, Theorem 4.4]) and to apply Eq. (2). □

3.1 The Huang–Johnson semifields of order 2^6

In [8], the authors exhibit eight non–isotopic semifields, say $\mathbb{S}_i$ $i \in \{I, II, III, IV, V, VI, VII, VIII\}$, of order 2^6. All of these, but $\mathbb{S}_I$, are proper semifields and they have left nucleus $\mathbb{F}_{2^3}$ and center $\mathbb{F}_2$.

Semifields with 2^6 elements have been classified in [21] and, apart from the Knuth types (17) and (19) and the semifields of Huang–Johnson, all the others are not 2-dimensional over their left nucleus.

In the literature the only infinite families of semifields of order q^6, 2–dimensional over their left nucleus and 6–dimensional over their center, containing examples of order 2^6 are

i) the Knuth semifields (17) and (19) [4, p. 241];

ii) the cyclic semifields of type $(q, 2, 3)$ ([9], [10] and [12]);

iii) the families $\mathcal{F}_{IV}$ and $\mathcal{F}_V$ of semifields recently constructed in [6].

These families are pairwise non–isotopic.

In what follows we will determine which Huang–Johnson semifields belong to the infinite families *ii*) and *iii*). In order to do this let $\mathbb{P} = PG(3, 2^3) = PG(\mathbb{M}, \mathbb{F}_{2^3})$; in the table here below we list the semifield spread sets of matrices S_i, $i \in \{II, III, IV, V, VI, VII, VIII\}$, associated with any $\mathbb{S}_i$ (see [8]).

Type	Spread sets of matrices
S_{II}	$\left\{ \begin{pmatrix} x+y+y^2+y^4 & y^2+x^2+x^4 \\ y & x \end{pmatrix} : y,x \in \mathbb{F}_{2^3} \right\}$
S_{III}	$\left\{ \begin{pmatrix} x+y+y^2+y^4 & y^4+x^2+x^4 \\ y & x \end{pmatrix} : y,x \in \mathbb{F}_{2^3} \right\}$
S_{IV}	$\left\{ \begin{pmatrix} x+y+\alpha y+y^2+\alpha^3 y^4 & \alpha^6 y^4+\alpha x+x^2+\alpha^3 x^4 \\ y & x \end{pmatrix} : y,x \in \mathbb{F}_{2^3} \right\}$
S_{V}	$\left\{ \begin{pmatrix} x+y+\alpha y+y^2+\alpha^3 y^4 & \alpha^6 y^2+\alpha x+x^2+\alpha^3 x^4 \\ y & x \end{pmatrix} : y,x \in \mathbb{F}_{2^3} \right\}$
S_{VI}	$\left\{ \begin{pmatrix} x+y+\alpha^3 y+y^2+\alpha y^4 & y+\alpha^3 x+x^2+\alpha x^4 \\ y & x \end{pmatrix} : y,x \in \mathbb{F}_{2^3} \right\}$
S_{VII}	$\left\{ \begin{pmatrix} x+y+\alpha^3 y+y^2+\alpha y^4 & y+\alpha^6 y^2+\alpha y^4+\alpha^3 x+x^2+\alpha x^4 \\ y & x \end{pmatrix} : y,x \in \mathbb{F}_{2^3} \right\}$
S_{VIII}	$\left\{ \begin{pmatrix} x+y+\alpha^3 y+y^2+\alpha y^4 & y+y^2+\alpha^4 y^4+\alpha^3 x+x^2+\alpha x^4 \\ y & x \end{pmatrix} : y,x \in \mathbb{F}_{2^3} \right\}$

Table 1

Here α is an element of $\mathbb{F}_{2^3} \setminus \mathbb{F}_2$ such that $\alpha^3+\alpha+1=0$. Each semifield $\mathbb{S}_i$ is self–transpose (i.e., it is isotopic to its transpose) with the exception of $\mathbb{S}_{IV}$ and $\mathbb{S}_V$ that, in fact, are pairwise transpose (see [8, Table 1]). Moreover

Proposition 3.4. *The semifield $\mathbb{S}_{III}$ is, up to isotopy, the translation dual of $\mathbb{S}_{II}$.*

Proof. Each S_i, $i \in \{II, \ldots, VIII\}$, is an $\mathbb{F}_2$–vector subspace of the vector space $\mathbb{M}$ of all 2×2 matrices over $\mathbb{F}_{2^3}$, and the translation dual $\mathbb{S}_i^{\perp}$ of $\mathbb{S}_i$ is defined by the orthogonal complement $S_i^{\perp}$ of S_i with respect to the bilinear form

$$Tr_{2^3/2}(\beta(X,Y)) = Tr_{2^3/2}(X_0Y_3 + X_3Y_0 - X_1Y_2 - X_2Y_1),$$

where $X = \begin{pmatrix} X_0 & X_1 \\ X_2 & X_3 \end{pmatrix}$ and $Y = \begin{pmatrix} Y_0 & Y_1 \\ Y_2 & Y_3 \end{pmatrix}$.

Then, the set $S_{II}^{\perp}$ is an $\mathbb{F}_2$–vector subspace of $\mathbb{M}$ of dimension 6 and it can be represented as follows

$$S_{II}^{\perp} = \left\{ \begin{pmatrix} f(y',x') & g(y',x') \\ y' & x' \end{pmatrix} : y', x' \in \mathbb{F}_{2^3} \right\},$$

where $f(y',x')$ and $g(y',x')$ are two $\mathbb{F}_2$–linear functions of $\mathbb{F}_{2^3}$, satisfying the following condition

$$Tr_{2^3/2}((x+y+y^2+y^4)x' + f(y',x')x + (y^2+x^2+x^4)y' + yg(y',x')) = 0 \; \forall x, y \in \mathbb{F}_{2^3}. \quad (3)$$

A direct computation shows that the maps $f(y',x') = y'^2 + y'^4 + x'$ and $g(y',x') = y'^4 + x'^4 + x'^2 + x'$ satisfy (3). Hence,

$$S_{II}^{\perp} = \left\{ \begin{pmatrix} x + y^2 + y^4 & x + x^2 + x^4 + y^4 \\ y & x \end{pmatrix} : y, x \in \mathbb{F}_{2^3} \right\}.$$

Consider the collineation ϕ_g of $\mathcal{G} < PGO^+(4, 2^3)$ induced by the linear map g

$$g : \begin{pmatrix} X_0 & X_1 \\ X_2 & X_3 \end{pmatrix} \mapsto \begin{pmatrix} X_0 + X_2 & X_1 + X_3 \\ X_2 & X_3 \end{pmatrix},$$

then $(S_{II}^{\perp})^g = S_{III}$. This implies that, up to isotopy, the Huang–Johnson semifield $\mathbb{S}_{III}$ is the translation dual of $\mathbb{S}_{II}$. □

In what follows we investigate the geometric structure of the linear sets $L(S_i)$ with $i \in \{II, III, IV, V, VI, VII, VIII\}$.

Proposition 3.5. *The Huang–Johnson semifields $\mathbb{S}_{II}$, $\mathbb{S}_{III}$, $\mathbb{S}_{IV}$ and $\mathbb{S}_V$ belong to the class $\mathcal{F}_3$. Precisely, $\mathbb{S}_{II}$ and $\mathbb{S}_{III}$ are of type $(4,1)$, whereas $\mathbb{S}_{IV}$ and $\mathbb{S}_V$ are of type $(3,0)$.*

Proof. Let $L_i = L(S_i)$, $i \in \{II, III, IV, V\}$. Since $\mathbb{S}_{IV}^t = \mathbb{S}_V$ and $\mathbb{S}_{II}^{\perp}$ is isotopic to $\mathbb{S}_{III}$, by Theorems 3.2 and 3.3, we can argue considering just one between $\mathbb{S}_{II}$ and $\mathbb{S}_{III}$ and just one between $\mathbb{S}_{IV}$ and $\mathbb{S}_V$.

Let (X_0, X_1, X_2, X_3) be the homogeneous projective coordinates of the point

$$\langle \begin{pmatrix} X_0 & X_1 \\ X_2 & X_3 \end{pmatrix} \rangle$$

of $\mathbb{P} = PG(3, 2^3) = PG(\mathbb{M}, \mathbb{F}_{2^3})$ and let P be the point with coordinates $(1, 1, 0, 1)$. A direct computation shows that P belongs to L_{II}, has weight 2 and all other points of L_{II} have weight 1. Indeed, let

$$R_{x,y} \equiv (x + y + y^2 + y^4, y^2 + x^2 + x^4, y, x),$$

with $x, y \in \mathbb{F}_{2^3}$, be a point of L_{II} having weight $w_{L_{II}}(R_{x,y}) > 1$. Then, there exist $\lambda \in \mathbb{F}_{2^3} \setminus \mathbb{F}_2$ and $x', y' \in \mathbb{F}_{2^3}$ such that

$$\begin{cases} \lambda y = y' \\ \lambda x = x' \\ \lambda(x + y + y^2 + y^4) = x' + y' + y'^2 + y'^4 \\ \lambda(y^2 + x^2 + x^4) = y'^2 + x'^2 + x'^4. \end{cases}$$

This implies that

$$\begin{cases} \lambda(y^2 + y^4) = \lambda^2 y^2 + \lambda^4 y^4 \\ \lambda(y^2 + x^2 + x^4) = \lambda^2 y^2 + \lambda^2 x^2 + \lambda^4 x^4. \end{cases} \tag{4}$$

If $y = 0$, from the second equation of System (4), we get $x = \lambda^2+\lambda^4$; hence $Tr_{2^3/2}(x) = 0$ and then $R_{x,y} = P$. If $y \neq 0$, from the first equation of System (4), we get $y = \lambda^2 + \lambda^4$. Hence $Tr_{2^3/2}(y) = 0$ and by substituting y in the second equation of System (4), we get

$$x^4 + (\lambda + \lambda^4)x^2 + (\lambda + \lambda^4)^2 = 0,$$

which admits no solution in $\mathbb{F}_{2^3}$.

These facts assure that $\mathbb{S}_{II}$ belongs to the class $\mathcal{F}_3$. Also, let π be the plane of $\mathbb{P}$ with equation $X_0 = X_3$; then we have that

$$L_{II} \cap \pi = \{(x, y^2 + x^2 + x^4, y, x) \ : \ x, y \in \mathbb{F}_{2^3}, Tr_{2^3/2}(y) = 0\},$$

which implies that π is the unique plane of $\mathbb{P}$ of weight 5 in L_{II}. Finally, the plane $P^\perp : X_0 + X_2 + X_3 = 0$ and the point $\pi^\perp \equiv (1, 0, 0, 1)$ have weight 4 and 1 in L_{II}, respectively. Hence the semifield $\mathbb{S}_{II}$ is of type $(4, 1)$.
Now, consider the semifield $\mathbb{S}_{IV}$. By using similar arguments, it can be proven that $P \equiv (1, \alpha^4, 0, 1)$ is the unique point of L_{IV} of weight 2 and all the other points have weight 1. This assures that the semifield $\mathbb{S}_{IV}$ belongs to the class $\mathcal{F}_3$, as well. Also, we have that $\pi' : X_0 + \alpha^5 X_2 + X_3 = 0$ is the unique plane of $\mathbb{P}$ of weight 5 in L_{IV}, the point $\pi'^\perp \equiv (1, \alpha^5, 0, 1)$ does not belong to L_{IV} and the plane $P^\perp : X_0 + \alpha^4 X_2 + X_3 = 0$ has weight 3 in L_{IV}. Hence the semifield $\mathbb{S}_{IV}$ is of type $(3, 0)$. □

In what follows we will show that the remaining Huang–Johnson semifields $\mathbb{S}_{VI}$, $\mathbb{S}_{VII}$ and $\mathbb{S}_{VIII}$ belong to the class $\mathcal{F}_4^{(c)}$. A linear set L of $PG(3, q^3)$ associated with a semifield belonging to the class $\mathcal{F}_4$ contains a unique line of $PG(3, q^3)$, say l ([18, Thm. 4.3]). Moreover, such a semifield falls within the subclass $\mathcal{F}_4^{(c)}$ if the polar line $l^\perp$ of l, with respect to the polarity induced by the quadric $\mathcal{Q}$, intersects the linear set L in $q + 1$ points ([12, Sec. 3]).

Proposition 3.6. *The Huang–Johnson semifields $\mathbb{S}_{VI}$, $\mathbb{S}_{VII}$ and $\mathbb{S}_{VIII}$ belong to the class $\mathcal{F}_4^{(c)}$.*

Proof. Let start with the Huang–Johnson semifield $\mathbb{S}_{VII}$. Arguing as in the proof of Proposition 3.5 and taking $\alpha^3 = \alpha + 1$ into account, we have that a point $R_{x,y}$ of L_{VII} has weight greater than 1 if there exist $\lambda \in \mathbb{F}_{2^3} \setminus \mathbb{F}_2$ and $x', y' \in \mathbb{F}_{2^3}$ such that

$$\begin{cases} \lambda y = y' \\ \lambda x = x' \\ \lambda(x + \alpha y + y^2 + \alpha y^4) = x' + \alpha y' + y'^2 + \alpha y'^4 \\ \lambda(y + \alpha^6 y^2 + \alpha y^4 + \alpha^3 x + x^2 + \alpha x^4) = y' + \alpha^6 y'^2 + \alpha y'^4 + \alpha^3 x' + x'^2 + \alpha x'^4. \end{cases}$$

This implies that

$$\begin{cases} (\lambda^2 + \lambda)y^2 + \alpha(\lambda^4 + \lambda)y^4 = 0 \\ \alpha^6(\lambda^2 + \lambda)y^2 + \alpha(\lambda^4 + \lambda)y^4 + (\lambda^2 + \lambda)x^2 + \alpha(\lambda^4 + \lambda)x^4 = 0. \end{cases} \tag{5}$$

If $y = 0$, since $\lambda \notin \mathbb{F}_2$ and $(\lambda + \lambda^4)^2 = \lambda^2 + \lambda$, from the second equation of Sistem (5) we get $x^2 = \frac{\lambda+\lambda^4}{\alpha}$ and hence $x = \alpha^3(\lambda^2+\lambda^4)$. This means that $x = \alpha^3 t$, with $Tr_{2^3/2}(t) = 0$, and hence $\alpha^3 x + x^2 + \alpha x^4 = 0$. Then, the point $R_{\alpha^3 t,0} = P \equiv (1, 0, 0, 1)$ has weight 2 in L_{VII}. If $y \neq 0$, from the first equation of System (5) we get $y = \alpha^3(\lambda^2 + \lambda^4)$. Substituting that value in the first equation of System (5) we get the following

$$\alpha x^4 + (\lambda + \lambda^4)x^2 + \alpha(\lambda + \lambda^4)^2 = 0. \tag{6}$$

Since $Tr_{2^3/2}(\alpha^2) = 0$, Equation (6) has two solutions:

$$x = \alpha^5(\lambda^2 + \lambda^4) \quad \text{and} \quad x = \alpha^2(\lambda^2 + \lambda^4).$$

So, by putting $x = \alpha^5 t$ and $x = \alpha^3(\alpha^2 + 1)t$, respectively, where in both positions t is an element of $\mathbb{F}_{2^3}$ such that $Tr_{2^3/2}(t) = 0$, it is easy to see that the points

$$P_1 \equiv (\alpha^4, \alpha, \alpha^5, 1) \quad \text{and} \quad P_2 \equiv (1, \alpha, \alpha^5, \alpha^4)$$

belong to L_{VII} and have weight 2 in it. Hence, again by Property 2.4, the line $< P_1, P_2 >$ with equations $\alpha^4 X_1 + X_2 = \alpha X_0 + (\alpha^4 + 1)X_1 + \alpha X_3 = 0$ is contained in the relevant linear set and it contains the point P. Also, straightforward computations show that the polar line $< P_1, P_2 >^\perp$, with equations $X_0 + X_3 = \alpha^4 X_0 + \alpha^5 X_1 + \alpha X_2 + X_3 = 0$ intersects the relevant linear set in three points; hence, $\mathbb{S}_{VII}$ belongs to the class $\mathcal{F}_4^{(c)}$. By using similar arguments it can be proven that also Huang–Johnson semifield $\mathbb{S}_{VIII}$ belongs to the class $\mathcal{F}_4^{(c)}$ as well.

Regarding the Huang–Johnson semifield $\mathbb{S}_{VI}$, taking into account that the solutions of the equation $\alpha^3 z + z^2 + \alpha z^4 = 0$ are $z = \alpha^3 t$, with $Tr_{2^3/2}(t) = 0$, it is easy to show that the points $P \equiv (1, 0, 0, 1)$ and $Q \equiv (1, 1, 1, 0)$ have weight 2 in L_{VI}. Hence, the line $l =< P, Q >_{\mathbb{F}_{2^3}}$ joining this two points has weight 4 in L_{VI} and hence, by Property 2.4, is contained in it. Straightforward computations show that any other point of L_{VI} has weight 1 and hence l is the unique line of $\mathbb{P}$ contained in L_{VI}. This means that the Huang–Johnson semifield $\mathbb{S}_{VI}$ belongs to the class $\mathcal{F}_4$. Now, consider the polar line $l^\perp$ of l with equations $X_0 + X_3 = X_1 + X_2 + X_3 = 0$. Direct computation shows that $|l^\perp \cap L_{VI}| = 3$. Hence, also $\mathbb{S}_{VI}$ falls within the class $\mathcal{F}_4^{(c)}$. □

Theorem 3.7. *The Huang–Johnson semifields $\mathbb{S}_{VI}$, $\mathbb{S}_{VII}$ and $\mathbb{S}_{VIII}$ belong to infinite families. Precisely, $\mathbb{S}_{VI}$ is isotopic to a cyclic semifield, whereas $\mathbb{S}_{VII}$ and $\mathbb{S}_{VIII}$ fill in the families $\mathcal{F}_{IV}$ and $\mathcal{F}_V$ constructed in [6].*

Proof. In [21] the authors completely classify, up to isotopy, all semifields with 64 elements giving a description of their parameters, i.e. the dimensions of the semifields over their nuclei and center. In this list, the Huang–Johnson semifields $\mathbb{S}_i$, with $i \in \{II, III, \cdots, VIII\}$ are the only semifields of order 2^6, with exactly one nucleus of order 2^3 and with center of order 2. In particular, $\mathbb{S}_{VI}$ has dimension 2 over its left nucleus and both middle and right nuclei isomorphic to $\mathbb{F}_4$. Semifields with these parameters have been classified in [12, Theorem 2.9] and they are either cyclic or isotopic to cyclic

ones. The semifields $\mathbb{S}_{VII}$ and $\mathbb{S}_{VIII}$ have right and middle nuclei $\mathbb{F}_2$ and by [21] and Proposition 3.6, these are the only two semifields of order 2^6 belonging to the class $\mathcal{F}_4^{(c)}$ and having middle and right nuclei both $\mathbb{F}_2$. Since the semifields of order 2^6, belonging to the non–isotopic families $\mathcal{F}_{IV}$ and $\mathcal{F}_V$ constructed in [6], fill in $\mathcal{F}_4^{(c)}$ and have the above parameters, we can state that, up to isotopy, $\mathbb{S}_{VII}$ and $\mathbb{S}_{VIII}$ belong to $\mathcal{F}_{IV}$ and $\mathcal{F}_V$. □

In [11], the authors posed the problem to understand whether the sporadic examples found by Huang and Johnson belong to infinite families. The previous theorem gives a positive answer to the question for the Huang–Johnson semifields $\mathbb{S}_{VI}$, $\mathbb{S}_{VII}$ and $\mathbb{S}_{VIII}$.

So far, the Huang–Johnson semifields $\mathbb{S}_{II}$, $\mathbb{S}_{III}$, $\mathbb{S}_{IV}$ and $\mathbb{S}_V$ do not belong to any infinite family. In what follows we will prove that two of these semifields, in fact $\mathbb{S}_{II}$ and $\mathbb{S}_{III}$, belong to new infinite families of semifields of order q^6 constructed in the next section.

3.2 New semifields in class $\mathcal{F}_3$

Recall that if $\mathbb{S} = (\mathbb{F}_{q^6}, +, *)$ is a semifield of order q^6, 2–dimensional over its left nucleus $\mathbb{F}_{q^3}$ and with center $\mathbb{F}_q$, the associated spread set S of $\mathbb{F}_{q^3}$–linear maps of $\mathbb{F}_{q^6}$ is a 6–dimensional $\mathbb{F}_q$–vector space contained in $\mathbb{V} = End_{\mathbb{F}_{q^3}}(\mathbb{F}_{q^6})$ and each non–zero map in S is invertible. Also, if an $\mathbb{F}_{q^3}$–linear map of $\mathbb{F}_{q^6}$ is represented in the form

$$\varphi_{\eta,\zeta}\colon \mathbb{F}_{q^6} \to \mathbb{F}_{q^6} \quad \text{via} \quad x \to \eta x + \zeta x^{q^3},$$

for some $\eta, \zeta \in \mathbb{F}_{q^6}$, then $\varphi_{\eta,\zeta}$ is invertible if and only if

$$N(\eta) \neq N(\zeta), \tag{7}$$

where N is the norm from $\mathbb{F}_{q^6}$ to $\mathbb{F}_{q^3}$.

In the construction of the new examples a crucial role is played by the existence of an element in $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ with predetermined trace and norm. Precisely, by [19, Thm. 3.2], there exists $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ for any prime power q, such that $u^3 = \sigma u + 1$ with $\sigma \in \mathbb{F}_q^*$ (i.e., $Tr_{q^3/q} = 0$ and $N_{q^3/q}(u) = 1$).

Proposition 3.8. *Let $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ such that $u^3 = \sigma u + 1$ with $\sigma \in \mathbb{F}_q^*$, $\xi \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^3}$, $D \in \mathbb{F}_{q^3}^*$ and $b \in \mathbb{F}_{q^6}^*$. The set*

$$S = \{x \in \mathbb{F}_{q^6} \mapsto ((\alpha_0 + \alpha_1 u) + (\alpha_2 + \alpha_3 u)\xi)x + b(\alpha_3 u^2 + \alpha_4 + \alpha_5 D\xi)x^{q^3} \in \mathbb{F}_{q^6} : \alpha_i \in \mathbb{F}_q\},$$

defines an $\mathbb{F}_q$–linear set $L(S)$ of $\mathbb{P} = PG(\mathbb{V}, \mathbb{F}_{q^3})$ of rank 6 having a unique point P of weight 2 (and hence a unique plane π of $\mathbb{P}$ of weight 5) and each other point of weight 1. Moreover, if one of the following additional assumptions holds true:

i) q is even;

ii) q is odd and $Tr_{q^6/q^3}(\xi) = 0$;

then $P^\perp$ and $\pi^\perp$ have weights 4 and 1 in $L(S)$, respectively, where $\perp$ is the polarity induced by the quadric $\mathcal{Q}$ of $\mathbb{P}$.

Proof. Note that $\{1,\xi\}$ is an $\mathbb{F}_{q^3}$–basis of $\mathbb{F}_{q^6}$ and $\{1,u,u^2\}$ is an $\mathbb{F}_q$–basis of $\mathbb{F}_{q^3}$. So, since $D \in \mathbb{F}_{q^3}^*$, we have that the $\mathbb{F}_q$–linear set

$$L(S) = \{\langle x \mapsto ((\alpha_0+\alpha_1 u)+(\alpha_2+\alpha_3 u)\xi)x + b(\alpha_3 u^2+\alpha_4+\alpha_5 D\xi)x^{q^3}\rangle_{\mathbb{F}_{q^3}} : \alpha_i \in \mathbb{F}_q\}$$

of $\mathbb{P}$ has rank 6.

Let $P = \langle I\rangle_{\mathbb{F}_{q^3}}$ be the point of $\mathbb{P}$ defined by the identity map $I : x \mapsto x$, then

$$P \cap S = \langle I, uI\rangle_{\mathbb{F}_q} = \{x \mapsto (\alpha_0+\alpha_1 u)x : \alpha_i \in \mathbb{F}_q\},$$

i.e. P has weight 2 in $L(S)$. Also, direct computations show that any other point of $L(S)$ has weight 1. Indeed, let $T = \langle x \mapsto ((\alpha_0+\alpha_1 u)+(\alpha_2+\alpha_3 u)\xi)x+b(\alpha_3 u^2+\alpha_4+\alpha_5 D\xi)x^{q^3}\rangle_{\mathbb{F}_{q^3}}$, with $\alpha_i \in \mathbb{F}_q$, be a point of $L(S)$ different from P. If $w_{L(S)}(T) > 1$, then there exist $\lambda \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and $\alpha_i' \in \mathbb{F}_q$ such that

$$\begin{cases} \lambda((\alpha_0+\alpha_1 u)+(\alpha_2+\alpha_3 u)\xi) &= (\alpha_0'+\alpha_1' u)+(\alpha_2'+\alpha_3' u)\xi \\ \lambda(\alpha_3 u^2+\alpha_4+\alpha_5 D\xi) &= \alpha_3' u^2+\alpha_4'+\alpha_5' D\xi. \end{cases}$$

Since $\{1,\xi\}$ is an $\mathbb{F}_{q^3}$–basis of $\mathbb{F}_{q^6}$, the previous system is satisfied if and only if the following equations hold true:

$$\lambda(\alpha_0+\alpha_1 u) = (\alpha_0'+\alpha_1' u) \quad (8)$$
$$\lambda(\alpha_2+\alpha_3 u) = (\alpha_2'+\alpha_3' u) \quad (9)$$
$$\lambda(\alpha_3 u^2+\alpha_4) = (\alpha_3' u^2+\alpha_4') \quad (10)$$
$$\lambda\alpha_5 = \alpha_5'. \quad (11)$$

From Eq. (11), since $\lambda \notin \mathbb{F}_q$, we have $\alpha_5 = \alpha_5' = 0$. If $\alpha_2+\alpha_3 u = 0$, from Eq. (9) and (10), we get $\alpha_2 = \alpha_3 = \alpha_4 = 0$, i.e. $T = P$, a contradiction. It follows that $\alpha_2+\alpha_3 u \neq 0$ and, by similar arguments, $\alpha_3 u^2+\alpha_4 \neq 0$. Hence, by Eq. (9) and (10), we have

$$\frac{\alpha_2'+\alpha_3' u}{\alpha_2+\alpha_3 u} = \frac{\alpha_3' u^2+\alpha_4'}{\alpha_3 u^2+\alpha_4},$$

which is equivalent to the following equations

$$\alpha_2'\alpha_4 = \alpha_2\alpha_4' \quad (12)$$
$$\alpha_3'\alpha_4 = \alpha_3\alpha_4' \quad (13)$$
$$\alpha_2'\alpha_3 = \alpha_2\alpha_3'. \quad (14)$$

If $\alpha_i = 0$, with $i \in \{2,3,4\}$, we have either $T = P$ or $\lambda \in \mathbb{F}_q$. In both cases we get a contradiction. Hence $\frac{\alpha_2'}{\alpha_2} = \frac{\alpha_3'}{\alpha_3} = \frac{\alpha_4'}{\alpha_4} = s \in \mathbb{F}_q$, and by Eq. (9), $\lambda = s \in \mathbb{F}_q$, again a contradiction.

Moreover, the plane

$$\pi = \{x \mapsto \lambda x + \mu b x^{q^3} : \ \lambda \in \mathbb{F}_{q^6}, \mu \in \mathbb{F}_{q^3}\}$$

is the plane of $\mathbb{P}$ of weight 5 in $L(S)$, indeed

$$\pi \cap S = \{x \mapsto ((\alpha_0 + \alpha_1 u) + (\alpha_2 + \alpha_3 u)\xi)x + b(\alpha_3 u^2 + \alpha_4)x^{q^3} : \ \alpha_i \in \mathbb{F}_q\}.$$

Recalling that the bilinear form β arising from $\mathcal{Q}$ is

$$\beta(\varphi_{a,b}, \varphi_{c,d}) = a^{q^3}c + ac^{q^3} - b^{q^3}d - bd^{q^3},$$

we have

$$P^\perp = \{x \mapsto \mu\eta x + \lambda x^{q^3} : \ \lambda \in \mathbb{F}_{q^6}, \mu \in \mathbb{F}_{q^3}\}$$

and

$$\pi^\perp = \{x \mapsto \gamma\eta b x^{q^3} : \ \gamma \in \mathbb{F}_{q^3}\},$$

where η is a given element of $\mathbb{F}_{q^6}$ such that $\eta^{q^3} = -\eta$ (note that if q is even $\eta \in \mathbb{F}_{q^3}$).

Let q be even. Then

$$P^\perp \cap S = \{x \mapsto (\alpha_0 + \alpha_1 u)x + b(\alpha_4 + \alpha_5 D\xi)x^{q^3} : \ \alpha_i \in \mathbb{F}_q\}$$

and

$$\pi^\perp \cap S = \{x \mapsto b\alpha_4 x^{q^3} : \ \alpha_4 \in \mathbb{F}_q\},$$

i.e., the weights of $P^\perp$ and $\pi^\perp$ in $L(S)$ are 4 and 1, respectively.

Now suppose Conditions *ii)* hold true. Then, since $\eta \notin \mathbb{F}_{q^3}$, we can uniquely written $\xi = \gamma\eta$, with $\gamma \in \mathbb{F}_{q^3}^*$. Straightforward computations show that

$$P^\perp \cap S = \{x \mapsto (\alpha_2 + \alpha_3 u)\gamma\eta x + b(\alpha_4 + \alpha_5 D\gamma\eta)x^{q^3} : \ \alpha_i \in \mathbb{F}_q\},$$

and

$$\pi^\perp \cap S = \{x \mapsto b\alpha_5 D\gamma\eta x^{q^3} : \ \alpha_5 \in \mathbb{F}_q\},$$

i.e. the weights of $P^\perp$ and $\pi^\perp$ in $L(S)$ are 4 and 1, respectively. □

Now, we prove that for any q, there exist some values for ξ, D and b such that the linear set $L(S)$ of Proposition 3.8 is disjoint from the quadric $\mathcal{Q}$, namely S is a spread set.

Theorem 3.9. *Let $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ such that $u^3 = \sigma u + 1$ with $\sigma \in \mathbb{F}_q^*$ and let*

$$S = \{x \in \mathbb{F}_{q^6} \mapsto ((\alpha_0 + \alpha_1 u) + (\alpha_2 + \alpha_3 u)\xi)x + b(\alpha_3 u^2 + \alpha_4 + \alpha_5 D\xi)x^{q^3} \in \mathbb{F}_{q^6} : \ \alpha_i \in \mathbb{F}_q\},$$

where

I) $\xi = \ell + u + u^2$ $(\ell \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q)$, $D = 1$ *and* $N(b) = 1 + u + u^2$, *if* $q = 2$;

II) $\xi = \ell^2 + \ell^2 u^2$ *(ℓ non–square in $\mathbb{F}_{q^2}$), $D = u^{21}$ and $N(b) = 2$, if $q = 3$;*

III) $\xi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *with $Tr_{q^2/q}(\xi) = 1$, $D = 1$ and $N(b) = Au$ with $A \in \mathbb{F}_q^*$ and $Tr_{q/2}(A) = 0$, if q is even and $q > 2$;*

IV) $\xi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *with $\xi^q = -\xi$, $D = 1$ and $N(b) = Au$, $A \in \mathbb{F}_q^*$, with $\xi^2 + A$ a non–square in $\mathbb{F}_q$, if q is odd and $q > 3$.*

Then, S is a semifield spread set defining a semifield $\mathbb{S} = (\mathbb{F}_{q^6}, +, *)$ of order q^6, with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$, where

$$x * y = ((\alpha_0 + \alpha_1 u) + (\alpha_2 + \alpha_3 u)\xi)x + b(\alpha_3 u^2 + \alpha_4 + \alpha_5 D\xi)x^{q^3}, \tag{15}$$

with $y = \alpha_0 + \alpha_1 u + \alpha_2 \xi + \alpha_3(u\xi + bu^2) + \alpha_4 b + \alpha_5 Db\xi$. Moreover the semifield $\mathbb{S}$ belongs to the family $\mathcal{F}_3$ and is of type $(4, 1)$.

Proof. By Proposition 3.8, to prove that S is a semifield spread set, it is enough to prove the non–singularity condition for the non–zero maps of S. So, from (7) we see that the non–singularity condition is equivalent to

$$N((\alpha_0 + \alpha_1 u) + (\alpha_2 + \alpha_3 u)\xi) = N(b)N(\alpha_3 u^2 + \alpha_4 + \alpha_5 D\xi) \quad \text{if and only if } \alpha_i = 0. \tag{16}$$

If $q = 2$ or $q = 3$, with the choices stated in $I)$ or $II)$, respectively, a direct computation shows that (16) is satisfied.

Consider now the Case $III)$. Since $Tr_{q^2/q}(\xi) = 1$, the $\mathbb{F}_q$–irreducible polynomial of which ξ is a root is of type $x^2 + x + \rho$, where $Tr_{q/2}(\rho) = 1$. Then, Condition (16) is equivalent to show that

$$\begin{aligned}(\alpha_0^2 + \alpha_0\alpha_2 + \rho\alpha_2^2) + (\alpha_0\alpha_3 + \alpha_1\alpha_2)u + (\alpha_1^2 + \alpha_1\alpha_3 + \rho\alpha_3^2)u^2 = \\ = A((\sigma\alpha_3^2 + \alpha_3\alpha_5) + (\alpha_4^2 + \sigma^2\alpha_3^2 + \alpha_4\alpha_5 + \sigma\alpha_3\alpha_5 + \rho\alpha_5^2)u + \alpha_3^2 u^2)\end{aligned} \tag{17}$$

if and only if $\alpha_i = 0$.

Since $\{1, u, u^2\}$ is an $\mathbb{F}_q$–basis of $\mathbb{F}_{q^3}$, the previous equality corresponds to the following system

$$\begin{cases} \alpha_0^2 + \alpha_0\alpha_2 + \rho\alpha_2^2 = A(\sigma\alpha_3^2 + \alpha_3\alpha_5) \\ \alpha_0\alpha_3 + \alpha_1\alpha_2 = A(\alpha_4^2 + \sigma^2\alpha_3^2 + \alpha_4\alpha_5 + \sigma\alpha_3\alpha_5 + \rho\alpha_5^2) \\ \alpha_1^2 + \alpha_1\alpha_3 + \rho\alpha_3^2 = A\alpha_3^2. \end{cases} \tag{18}$$

Since $Tr_{q/2}(A + \rho) = 1$, from the third equation of System (18), it follows $\alpha_1 = \alpha_3 = 0$ and then from the first and the second equation we get $\alpha_0 = \alpha_2 = 0$ and $\alpha_4 = \alpha_5 = 0$.

Using similar arguments, it is possible to prove that (16) is satisfied also with the choices of $IV)$.

This assures that in all cases $I) - -IV)$, S is a semifield spread set. Hence, S defines a semifield $\mathbb{S} = (\mathbb{F}_{q^6}, +, *)$, with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$, where $*$ is defined as in (1) and φ_y is the unique element of S such that $\varphi_y(1) = y$. Moreover, with the choices listed in $I)$ and $III)$, the set S satisfies Condition $i)$ of Proposition 3.8, whereas with the choices listed in $II)$ and $IV)$, the set S satisfies Condition $ii)$ of Proposition 3.8. Hence, from the above proposition, the semifield $\mathbb{S}$ belongs to $\mathcal{F}_3$ and turns out to be of type $(4, 1)$. □

Note that, for $q > 2$ and $q > 3$, we can always choose the parameters as in cases III) and IV), respectively. So, by Theorem 3.9, for any value of q there exist semifields whose Multiplication is given by the Rule (15). Hence, we end up with an infinite family of semifields, which turns out to be new. Indeed

Theorem 3.10. *Each semifield $\mathbb{S} = (\mathbb{F}_{q^6}, +, *)$, with $q > 2$, whose multiplication is defined as in (15) turns out to be non–isotopic to each known semifield.*

Proof. Since the semifields belonging to the family $\mathcal{F}_3$ known so far are the Huang–Johnson semifields of type II, III, IV and V (see table in [7]), by Theorem 3.9 we get the assertion. □

Finally, through the translation dual operation any semifield belonging to the above mentioned infinite family defines a semifield which belongs to the class $\mathcal{F}_3$ and of type $(4, 1)$, as well (see Thm. 3.3). This provides another infinite family. By the classification result in [21] and by Proposition 3.5, the Huang–Johnson semifields $\mathbb{S}_{II}$ and $\mathbb{S}_{III}$ are, up to isotopy, the only semifields of order 2^6 belonging to $\mathcal{F}_3$ and of type $(4, 1)$. Also, by Proposition 3.4, they are one the translation dual of the other. So, the semifields of order 2^6, with Multiplication (15) and the parameters chosen as in I) of Theorem 3.9, and their translation duals, must be isotopic to $\mathbb{S}_{II}$ and $\mathbb{S}_{III}$. Hence, we have positively answered to the question posed in [11] also for the Huang–Johnson semifields $\mathbb{S}_{II}$ and $\mathbb{S}_{III}$.

Theorem 3.11. *The Huang–Johnson semifields $\mathbb{S}_{II}$ and $\mathbb{S}_{III}$ belong to infinite families of semifields of order q^6, precisely the family of semifields with Multiplication (15) and the family of their translation duals.* □

References

[1] A.A. Albert: On the collineation groups of certain non–Desarguesian planes, *Portugaliae Mathematica*, **18** (1959), 207–224.

[2] I. Cardinali, O. Polverino, 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.

[3] J. De Beule, L. Storme (Editors): Current research topics in Galois Geometry, NOVA Academic Publishers, to appear.

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

[5] L. E. Dickson: Linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc.*, **7** (1906), no. 3, 370–390.

[6] G.L. Ebert, G. Marino, O. Polverino, R. Trombetti: Infinite families of new semifields, *Combinatorica*, **6** (2009), 637–663.

[7] G.L. Ebert, G. Marino, O. Polverino, R. Trombetti: Semifields in Class $\mathcal{F}_4^{(a)}$, *Electron. J. Combin.*, **16** (2009), 1–20.

[8] H. Huang, N.L. Johnson: Semifield planes of order 8^2, *Discrete Math.*, **80** (1990), 69–79.

[9] V. Jha, 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), no. 1, 1–35.

[10] V. Jha, N.L. Johnson: Translation planes of large dimension admitting nonsolvable groups, *J. Geom.* **45** (1992), no. 1–2, 87–104.

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

[12] N.L. Johnson, G. Marino, O. Polverino, R. Trombetti: Semifields of order q^6 with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$, *Finite Fields Appl.*, **14** (2008), 456–469.

[13] E. Kleinfeld: Technique for enumerating Veblen-Wedderburn systems, *J. Assoc. Comp. Mach.*, **7** (1960), 330–337.

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

[15] M. Lavrauw, O. Polverino: Finite semifields. Chapter in *Current research topics in Galois Geometry* (J. De Beule and L. Storme, Eds.), NOVA Academic Publishers, to appear.

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

[17] G. Lunardon, G. Marino, O. Polverino, R. Trombetti: Translation dual of a semifield, *J. Combin. Theory Ser. A*, **115** (2008), 1321–1332.

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

[19] M. Moisio: Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, *Acta Arith.*, **132** (2008), no. 4, 329–350.

[20] O. Polverino: Linear sets in Finite Projective Spaces, *Discrete Math.*, **310**, no. 22 (2010), 3096–3107.

[21] I.F. Rúa, E.F. Combarro, J. Ranilla: Classification of 64-element finite semifields, *Journal of Algebra*, **322** (2009), no. 11, 4011–4029.