Finite Fields and Their Applications 17 (2011) 225–239

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

# $\mathbb{F}_q$-pseudoreguli of PG$(3, q^3)$ and scattered semifields of order $q^6$

Michel Lavrauw [a,1], Giuseppe Marino [b,2], Olga Polverino [b,*,2], Rocco Trombetti [c,2]

[a] *Department of Mathematics, University of Ghent, 9000-Ghent, Belgium*
[b] *Dipartimento di Matematica, Seconda Università degli Studi di Napoli, I-81100 Caserta, Italy*
[c] *Dipartimento di Matematica e Applicazioni, Università degli Studi di Napoli "Federico II", I-80126 Napoli, Italy*

ARTICLE INFO

*Article history:*
Received 29 July 2010
Accepted 1 December 2010
Available online 16 December 2010
Communicated by Simeon Ball

*MSC:*
51Exx
05B25
12K10

*Keywords:*
Semifield
Scattered linear set
Pseudoregulus

ABSTRACT

In this paper, we study rank two semifields of order $q^6$ that are of scattered type. The known examples of such semifields are some Knuth semifields, some Generalized Twisted Fields and the semifields recently constructed in Marino et al. (in press) [12] for $q \equiv 1 \pmod 3$. Here, we construct new infinite families of rank two scattered semifields for any $q$ odd prime power, with $q \equiv 1 \pmod 3$; for any $q = 2^{2h}$, such that $h \equiv 1 \pmod 3$ and for any $q = 3^h$ with $h \not\equiv 0 \pmod 3$. Both the construction and the proof that these semifields are new, rely on the structure of the linear set and the so-called pseudoregulus associated to these semifields.



## 1. Introduction

A nonassociative division algebra over a finite field is called a *finite semifield*. During the last decade the theory of finite semifields has received a lot of attention. This has no doubt been stimulated by the interesting connections between semifields and other areas, such as finite geometry and coding theory. In this paper we use a geometric approach to this theory. We refer to [5] for definitions and notations.

* Corresponding author.
*E-mail addresses:* michel.lavrauw@ugent.be (M. Lavrauw), giuseppe.marino@unina2.it (G. Marino), olga.polverino@unina2.it (O. Polverino), rtrombet@unina.it (R. Trombetti).

[1] This research has been supported by the Research Foundation Flanders (FWO).
[2] 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.

1071-5797/$ – see front matter 
doi:10.1016/j.ffa.2010.12.001

The semifields that we study here are six-dimensional $\mathbb{F}_q$-algebras, which have at least one nucleus of order $q^3$: *rank two semifields of order* $q^6$. The Knuth orbit of such a semifield contains an isotopism class $[\mathbb{S}]$, whose left nucleus has size $q^3$, and with the semifield $\mathbb{S}$, there is associated an $\mathbb{F}_q$-linear set $L(\mathbb{S})$ of rank six, disjoint from a hyperbolic quadric $\mathcal{Q}$ in $\mathrm{PG}(3,q^3)$. The isotopy class $[\mathbb{S}]$ corresponds to the orbit of $L(\mathbb{S})$ under the subgroup $\mathcal{G} \leqslant \mathrm{P\Gamma O}^+(4,q^3)$ that fixes the reguli of $\mathcal{Q}$.

These linear sets have been studied in detail in [10] and the corresponding isotopism classes of semifields can be partitioned into six families, $\mathcal{F}_i$ $(i = 0, 1, \ldots, 5)$, according with the different geometric configurations of the associated $\mathbb{F}_q$-linear sets. In this paper we study semifields in the class $\mathcal{F}_5$, in which case the linear sets are *scattered*, i.e., they have maximal size $(q^6-1)/(q-1)$. The semifields of class $\mathcal{F}_5$ are called *scattered semifields*. The known examples of semifields belonging to $\mathcal{F}_5$ are some Knuth semifields (see [10, Proposition 4.7]), some Generalized Twisted Fields (see [10, Proposition 4.8]) and finally the semifields recently constructed in [12], for $q \equiv 1 \pmod 3$.

In this paper we deduce the general form for a new class of scattered semifields and determine the nuclei of such a semifield in terms of its parameters. Next, we face with the existence issue for this class, and prove that it contains infinitely many examples. In fact, it contains examples for any odd prime power $q$, with $q \equiv 1 \pmod 3$; for any $q = 2^{2h}$, such that $h \equiv 1 \pmod 3$ and for any $q = 3^h$ with $h \not\equiv 0 \pmod 3$.

## 2. Preliminary results

In [10], the authors associate to any scattered $\mathbb{F}_q$-linear set $L$ of rank 6 of $\mathrm{PG}(3,q^3)$, a geometric object $\mathcal{P}(L)$, called an $\mathbb{F}_q$-*pseudoregulus*, consisting of $q^3+1$ lines of $\mathrm{PG}(3,q^3)$ intersecting $L$ in $q^2+q+1$ points. An $\mathbb{F}_q$-pseudoregulus has exactly two transversal lines and the above mentioned $q^3+1$ $(q^2+q+1)$-secants to $L$ are the unique lines of $\mathrm{PG}(3,q^3)$ intersecting $L$ in that number of points. A way to construct scattered $\mathbb{F}_q$-linear sets of rank 6 in $\mathrm{PG}(3,q^3)$ is the following. Let $r$ and $r'$ be two disjoint lines of $\mathrm{PG}(3,q^3) = \mathrm{PG}(V)$, say $r = \mathrm{PG}(U)$ and $r' = \mathrm{PG}(U')$, with $V = U \oplus U'$. Let $\phi_f : r \mapsto r'$ be a strictly semilinear collineation between $r$ and $r'$ having as companion automorphism $\sigma$ an $\mathbb{F}_{q^3}$-automorphism over $\mathbb{F}_q$ (i.e. $\sigma \in \{q, q^2\}$), induced by the semilinear invertible map $f : U \mapsto U'$. Let $W_\rho = \{\underline{u} + \rho f(\underline{u}) \colon \underline{u} \in U\}$ with $\rho \in \mathbb{F}_{q^3}^*$. Then $W_\rho$ is an $\mathbb{F}_q$-vector subspace of $V$ of dimension 6 and if $\rho \neq 0$, $W_\rho$ is not an $\mathbb{F}_{q^3}$-vector subspace of $V$. It is easy to see that

$$L(W_\rho) = \left\{ \langle \underline{u} + \rho f(\underline{u}) \rangle_{\mathbb{F}_{q^3}} \colon \underline{u} \in U \setminus \{\mathbf{0}\} \right\}$$

is a scattered $\mathbb{F}_q$-linear set or rank 6 of $\mathrm{PG}(3,q^3)$. Also, for any point $P \in r$ we have that

$$\left\langle P, P^{\phi_f} \right\rangle \cap L(W_\rho) = \left\{ \langle \lambda \underline{u} + \lambda^\sigma f(\underline{u}) \rangle_{\mathbb{F}_{q^3}} \colon \lambda \in \mathbb{F}_{q^3}^* \right\}.$$

So for each $P \in r$ the lines $\langle P, P^{\phi_f} \rangle$ are $(q^2+q+1)$-secants to $L(W_\rho)$. Hence, the $\mathbb{F}_q$-pseudoregulus associated with $L(W_\rho)$ is $\mathcal{P}(L(W_\rho)) = \{\langle P, P^{\phi_f} \rangle \colon P \in r\}$ and the lines $r$ and $r'$ are its transversal lines. Also, note that $L(W_\rho) \cap L(W_{\rho'}) \neq \emptyset$ if and only if $\rho^{q^2+q+1} = \rho'^{q^2+q+1}$; in fact in this case $L(W_\rho) = L(W_{\rho'})$, and for any $\rho \in \mathbb{F}_{q^3}^*$, $L(W_\rho)$ is disjoint from both $r$ and $r'$. So, we end up with $q-1$ disjoint linear sets which together with the lines $r$ and $r'$ partition the pointset of the $\mathbb{F}_q$-pseudoregulus. In [10, Proposition 2.7] it has been proven that scattered $\mathbb{F}_q$-linear sets of rank 6 of $\mathrm{PG}(3,q^3)$ are projectively equivalent with respect to the action of $\mathrm{P\Gamma L}(4,q^3)$. As a consequence of this theorem the above arguments prove the following result.

**Theorem 2.1.** *If $L$ is a scattered $\mathbb{F}_q$-linear set of rank 6 of $\mathrm{PG}(3,q^3)$ whose associated $\mathbb{F}_q$-pseudoregulus $\mathcal{P}(L)$ has transversal lines $r = \mathrm{PG}(U,q^3)$ and $r' = \mathrm{PG}(U',q^3)$, then there exist an element $\rho$ of $\mathbb{F}_{q^3}^*$ and a semilinear collineation $\phi_f$ between $r$ and $r'$ having as companion automorphism either $\sigma = q$ or $\sigma = q^2$ such that*

$$L = L(W_\rho) = \left\{ \langle \underline{u} + \rho f(\underline{u}) \rangle \colon \underline{u} \in U \setminus \{\mathbf{0}\} \right\} \quad \text{and} \quad \mathcal{P}(L) = \left\{ \left\langle P, P^{\phi_f} \right\rangle \colon P \in r \right\}.$$

If $\mathbb{S}$ is a semifield belonging to class $\mathcal{F}_5$, then the associated linear set $L(\mathbb{S})$ in $\mathrm{PG}(3,q^3)$ is a scattered $\mathbb{F}_q$-linear set of rank 6. Hence, there exists an $\mathbb{F}_q$-pseudoregulus $\mathcal{P}(L(\mathbb{S})) := \mathcal{P}(\mathbb{S})$ associated with $L(\mathbb{S})$. If $\mathbb{S}$ and $\mathbb{S}'$ are two isotopic semifields in class $\mathcal{F}_5$ then the corresponding scattered linear sets $L(\mathbb{S})$ and $L(\mathbb{S}')$ belong to the same orbit of the group $\mathcal{G} \leqslant \mathrm{P\Gamma O}^+(4,q^3)$ fixing the reguli of the quadric $\mathcal{Q}$. Hence, the associated pseudoreguli $\mathcal{P}(\mathbb{S})$ and $\mathcal{P}(\mathbb{S}')$ and the related transversal lines are $\mathcal{G}$-equivalent. This means that semifields in class $\mathcal{F}_5$, whose associated pseudoreguli have transversals not equivalent under the $\mathcal{G}$-action, are not isotopic. The only known examples of semifields belonging to $\mathcal{F}_5$ are

a) some Knuth semifields (see [10, Property 4.7]);
b) some Generalized Twisted Fields (see [10, Property 4.8]);
c) semifields constructed in [12] for $q \equiv 1 \pmod 3$.

The corresponding $\mathbb{F}_q$-pseudoregulus has the transversal lines both contained in $\mathcal{Q}$ in Case a), both external to $\mathcal{Q}$ and pairwise polar in Case b) and one external and the other one contained in $\mathcal{Q}$ in Case c). In the next section we study $\mathbb{F}_q$-pseudoreguli for which at least one of the transversal lines is external to the quadric $\mathcal{Q}$, in order to construct scattered $\mathbb{F}_q$-linear sets of $\mathrm{PG}(3,q^3)$ which are not $\mathcal{G}$-isomorphic to any linear set associated with a semifield of type a), b) or c). This leads to the construction of new semifields in the family $\mathcal{F}_5$.

## 3. Semifields from pseudoreguli with at least one external transversal line

Let $\mathbb{V} \cong \mathbb{F}_{q^3}^4$ denote the $\mathbb{F}_{q^3}$-vector space with elements $\{(x,y)\colon\ x,y \in \mathbb{F}_{q^6}\}$. We use the notation $\langle x,y\rangle$ for the points of $\mathbb{P} = \mathrm{PG}(\mathbb{V})$. Let $\mathcal{Q}$ be the hyperbolic quadric of $\mathbb{P}$ whose associated orthogonal polarity $\perp$ is induced by the symmetric bilinear form

$$\mathbf{b}\big((x,y),\big(x',y'\big)\big) = x^{q^3}x' + xx'^{q^3} - y^{q^3}y' - yy'^{q^3},$$

i.e.,

$$\mathcal{Q}\colon\quad X^{q^3+1} - Y^{q^3+1} = 0.$$

Let $N : \mathbb{F}_{q^6} \to \mathbb{F}_{q^3} : x \mapsto x^{q^3+1}$ denote the norm function of $\mathbb{F}_{q^6}$ over $\mathbb{F}_{q^3}$ and, as before, let $\mathcal{G}$ be the subgroup of $\mathrm{P\Gamma O}^+(4,q^3)$, fixing the reguli $\mathcal{R}_1$ and $\mathcal{R}_2$ of the quadric $\mathcal{Q}$, where $\mathcal{R}_1$ and $\mathcal{R}_2$ consist of the lines $\{L_\epsilon\colon\ \epsilon \in \mathbb{F}_{q^6},\ N(\epsilon) = 1\}$ and $\{M_\epsilon\colon\ \epsilon \in \mathbb{F}_{q^6},\ N(\epsilon) = 1\}$, respectively, with

$$L_\epsilon := \big\{\langle y, y\epsilon\rangle\colon\ y \in \mathbb{F}_{q^6}^*\big\},\quad \text{and}\quad M_\epsilon := \big\{\big\langle y, y^{q^3}\epsilon\big\rangle\colon\ y \in \mathbb{F}_{q^6}^*\big\}.$$

The linear collineations of $\mathbb{P}$ fixing the reguli of $\mathcal{Q}$ are

$$\langle x,y\rangle \mapsto \big\langle ACx + BD^{q^3}x^{q^3} + AD^{q^3}y + BCy^{q^3}, ADx + BC^{q^3}x^{q^3} + AC^{q^3}y + BDy^{q^3}\big\rangle \tag{1}$$

where $A, B, C$ and $D$ are elements of $\mathbb{F}_{q^6}$ with $A^{q^3+1} \neq B^{q^3+1}$ and $C^{q^3+1} \neq D^{q^3+1}$.

Let $Tr_{q^3/q}$ denote the trace function of $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$; the map $Tr_{q^3/q} \circ \mathbf{b}$ is a non-degenerate $\mathbb{F}_q$-bilinear form of $\mathbb{V}$, when $\mathbb{V}$ is regarded as an $\mathbb{F}_q$-vector space. Starting from a semifield $\mathbb{S}$ of order $q^6$, 2-dimensional over the left nucleus, using the form $Tr_{q^3/q} \circ \mathbf{b}$, we get a (pre)semifield[3] of order $q^6$, whose associated semifield is 2-dimensional over its left nucleus, as well. This (pre)semifield is the *translation dual* of $\mathbb{S}$ and it is denoted by $\mathbb{S}^\perp$. For further details on the translation dual of a semifield

[3] A *presemifield* satisfies all the axioms of a semifield except (possibly) the existence of the identity element. Each presemifield is isotopic to a semifield.

see [6,8] and [4, Chapter 85]. In [10, Proposition 3.1], it has been proven that the family $\mathcal{F}_5$ is closed under the translation dual operation.

Let $\mathbb{S}$ be a semifield belonging to class $\mathcal{F}_5$ and denote by $\mathcal{P}(\mathbb{S})$ its associated $\mathbb{F}_q$-pseudoregulus in $\mathbb{P}$, with transversal lines $r$ and $r'$ and suppose that $r$ is an external line to the hyperbolic quadric $\mathcal{Q}$. Since the group $\mathcal{G}$ acts transitively on the set of lines of $\mathbb{P}$ which are external to $\mathcal{Q}$ we can suppose, up to the $\mathcal{G}$-action, that

$$r := \{\langle y, 0\rangle\colon\ y \in \mathbb{F}_{q^6}^*\}.$$

Now, any line $r'$ of $\mathbb{P}$ disjoint from $r$ is of type $r' = \{\langle g(y), y\rangle\colon\ y \in \mathbb{F}_{q^6}^*\}$, where $g : \mathbb{F}_{q^6} \mapsto \mathbb{F}_{q^6}$ is an $\mathbb{F}_{q^3}$-linear map of $\mathbb{F}_{q^6}$, i.e.

$$r' = r_{\lambda,\mu} = \{\langle \lambda y + \mu y^{q^3}, y\rangle\colon\ y \in \mathbb{F}_{q^6}^*\},$$

where $\lambda, \mu$ are two elements of $\mathbb{F}_{q^6}$. If $\lambda = \mu = 0$, then $r' = r^\perp$ where $\perp$ is the polarity defined by $\mathcal{Q}$; whereas, the line $r'$ is contained in $\mathcal{Q}$ if and only if either $\lambda = 0$ and $N(\mu) = 1$ or $N(\lambda) = 1$ and $\mu = 0$. Denote by $\overline{\mathcal{G}}$ the linear part of the group $\mathcal{G}$. In what follows we will determine the stabilizer $\overline{\mathcal{G}}_r$ of the transversal line $r$ of $\mathcal{P}(\mathbb{S})$, with respect to the action of $\overline{\mathcal{G}}$. Then we study the action of $\overline{\mathcal{G}}_r$ on the lines $r'$ skew to $r$.

**Proposition 3.1.** *Two lines $r_{\lambda,\mu}$ and $r_{\lambda',\mu'}$ disjoint from $r$ belong to the same orbit under the action of $\overline{\mathcal{G}}_r$ if and only if $N(\lambda') = N(\lambda)$ and $N(\mu') = N(\mu)$.*

**Proof.** Taking (1) into account, it is easy to show that a projectivity of $\mathbb{P}$, fixing the reguli of $\mathcal{Q}$ and leaving invariant the line $r$ is either

$$\phi_{\ell,\varepsilon} : \langle x, y\rangle \mapsto \langle \ell x, \ell\varepsilon y\rangle$$

or

$$\phi'_{\ell,\varepsilon} : \langle x, y\rangle \mapsto \langle \ell\varepsilon x^{q^3}, \ell y^{q^3}\rangle,$$

where $\ell \in \mathbb{F}_{q^6}^*$ and $\varepsilon^{q^3+1} = 1$. Hence,

$$\phi_{\ell,\varepsilon}(r_{\lambda,\mu}) = \{\langle \ell(\lambda y + \mu y^{q^3}), \ell\varepsilon y\rangle\colon\ y \in \mathbb{F}_{q^6}^*\} = \left\{\left\langle \frac{\lambda}{\varepsilon} z + \frac{\varepsilon}{\ell^{q^3-1}} \mu z^{q^3}, z\right\rangle\colon\ z \in \mathbb{F}_{q^6}^*\right\}$$

and

$$\phi'_{\ell,\varepsilon}(r_{\lambda,\mu}) = \{\langle \ell\varepsilon(\lambda^{q^3} y^{q^3} + \mu^{q^3} y), \ell y^{q^3}\rangle\colon\ y \in \mathbb{F}_{q^6}^*\} = \left\{\left\langle \lambda^{q^3}\varepsilon z + \frac{\varepsilon}{\ell^{q^3-1}} \mu^{q^3} z^{q^3}, z\right\rangle\colon\ z \in \mathbb{F}_{q^6}^*\right\},$$

where $\ell \in \mathbb{F}_{q^6}^*$ and $\varepsilon^{q^3+1} = 1$. The result easily follows from these expressions. □

Now, we determine the generic form of an $\mathbb{F}_q$-pseudoregulus having as its transversals the lines $r$ and $r' = r_{\lambda,\mu}$. By Theorem 2.1 we need a strictly semilinear invertible map $\phi_f$ between $r'$ and $r$. Any such map has the following form:

$$\phi_f : \langle \lambda y + \mu y^{q^3}, y\rangle \in r' \mapsto \langle f(y), 0\rangle \in r, \tag{2}$$

where $f:\mathbb{F}_{q^6}\mapsto\mathbb{F}_{q^6}$ is a strictly $\mathbb{F}_{q^3}$-semilinear invertible map of $\mathbb{F}_{q^6}$ with companion automorphism an $\mathbb{F}_{q^6}$-automorphism $\sigma$ over $\mathbb{F}_q$; i.e., $f(\alpha y)=\alpha^\sigma f(y)$ for each $\alpha\in\mathbb{F}_{q^3}$ and $y\in\mathbb{F}_{q^6}$. A direct calculation shows that

$$f: y\mapsto ly^\sigma + my^{\sigma q^3}, \tag{3}$$

where $l$ and $m$ are two elements of $\mathbb{F}_{q^6}$ such that $N(l)\neq N(m)$ and $\sigma\in\{q,q^2,q^4,q^5\}$. Indeed, since $f$ is $\mathbb{F}_q$-linear, we can write

$$f(y)=\sum_{i=0}^{5} a_i y^{q^i},$$

with $a_i\in\mathbb{F}_{q^6}$. Now, since $f(\alpha y)=\alpha^\sigma f(y)$ for any $\alpha\in\mathbb{F}_{q^3}$ and for any $y\in\mathbb{F}_{q^6}$, we have

$$\forall\alpha\in\mathbb{F}_{q^3}\quad \forall i=0,\dots,5:\quad a_i\left(\alpha^{q^i}-\alpha^\sigma\right)=0.$$

It follows that $f$ must assume form (3).

This allows us to prove the following

**Theorem 3.2.** *Up to the action of the group $\mathcal{G}$, the generic form for a scattered $\mathbb{F}_q$-linear set $L$ of rank 6 of $\mathrm{PG}(3,q^3)$ disjoint from the hyperbolic quadric $\mathcal{Q}$ and whose associated $\mathbb{F}_q$-pseudoregulus has at least one of its transversal lines being external to $\mathcal{Q}$, is the following*

$$L=L(\lambda,\mu,\alpha,\beta,\sigma):=\left\{\left\langle \lambda y+\mu y^{q^3}+\alpha y^\sigma+\beta y^{\sigma q^3}, y\right\rangle:\ y\in\mathbb{F}_{q^6}^*\right\},$$

*where $\lambda,\mu,\alpha$ and $\beta$ are elements of $\mathbb{F}_{q^6}$ such that $N(\alpha)\neq N(\beta)$, $\sigma\in\{q,q^2,q^4,q^5\}$ and*

$$\forall y\in\mathbb{F}_{q^6}^*:\quad N(y)\neq N\left(\lambda y+\mu y^{q^3}+\alpha y^\sigma+\beta y^{\sigma q^3}\right). \tag{4}$$

*Also, the elements $\lambda$ and $\mu$ can be taken up to their norms, i.e., if $N(\lambda)=N(\lambda')$ and $N(\mu)=N(\mu')$, then*

$$L(\lambda,\mu,\alpha,\beta,\sigma)^{\mathcal{G}}=L\left(\lambda',\mu',\alpha,\beta,\sigma\right)^{\mathcal{G}}.$$

**Proof.** By the previous arguments we can suppose

$$r=\left\{\langle y,0\rangle:\ y\in\mathbb{F}_{q^6}^*\right\}$$

and

$$r'=r_{\lambda,\mu}=\left\{\left\langle \lambda y+\mu y^{q^3}, y\right\rangle:\ y\in\mathbb{F}_{q^6}\right\},$$

where $\lambda,\mu\in\mathbb{F}_{q^6}^*$ and $\lambda$ and $\mu$ can be taken up to their $\mathbb{F}_{q^3}$-norms. Also, by Theorem 2.1, $\mathcal{P}(L)=\{\langle P,P^{\phi_f}\rangle:\ P\in r'\}$, where $\phi_f$ is a semilinear map between $r'$ and $r$ as described in (2) and (3) and $L=L(W_\rho)$ ($\rho\in\mathbb{F}_{q^3}^*$), where

$$W_\rho=\left\{\left(\lambda y+\mu y^{q^3}+\rho\left(ly^\sigma+my^{\sigma q^3}\right), y\right):\ y\in\mathbb{F}_{q^6}\right\},$$

with $N(l) \neq N(m)$. Putting $\alpha = l\rho$ and $\beta = m\rho$ we have that

$$L = \{\langle \lambda y + \mu y^{q^3} + \alpha y^{\sigma} + \beta y^{\sigma q^3}, y\rangle \colon y \in \mathbb{F}_{q^6}^*\}, \tag{5}$$

for some $\lambda, \mu, \alpha, \beta \in \mathbb{F}_{q^6}$, such that $N(\alpha) \neq N(\beta)$. Finally, since $L \cap \mathcal{Q} = \emptyset$,

$$\forall y \in \mathbb{F}_{q^6}^*\colon \quad N(y) \neq N\big(\lambda y + \mu y^{q^3} + \alpha y^{\sigma} + \beta y^{\sigma q^3}\big). \qquad \square$$

Let $\mathbb{S}$ be a presemifield in class $\mathcal{F}_5$ and let $L(\mathbb{S})$ be the associated scattered $\mathbb{F}_q$-linear set of rank 6 in $\mathrm{PG}(3, q^3)$. By Theorem 3.2, up to the $\mathcal{G}$-action we have

$$L(\mathbb{S}) = L(\lambda, \mu, \alpha, \beta, \sigma) = \{\langle \lambda y + \mu y^{q^3} + \alpha y^{\sigma} + \beta y^{\sigma q^3}, y\rangle \colon y \in \mathbb{F}_{q^6}^*\}.$$

By [8], the $\mathcal{G}$-orbit corresponding to the isotopism class $[\mathbb{S}^t]$ of the transpose semifield $\mathbb{S}^t$ of $\mathbb{S}$ is obtained by an element of $\mathrm{P\Gamma O}^+(4, q^3)$ interchanging the reguli $\mathcal{R}_1$ and $\mathcal{R}_2$, for instance $\langle x, y\rangle \mapsto \langle x, y^{q^3}\rangle$; indeed $[\mathbb{S}^t]$ corresponds to the $\mathcal{G}$-orbit $L(\mathbb{S}^t)^{\mathcal{G}}$ with

$$L\big(\mathbb{S}^t\big) = \{\langle \mu z + \lambda z^{q^3} + \beta z^{\sigma} + \alpha z^{\sigma q^3}, z\rangle \colon z \in \mathbb{F}_{q^6}^*\} = L(\mu, \lambda, \beta, \alpha, \sigma). \tag{6}$$

Also, direct computation shows that the orthogonal complement of the projective space $L(\mathbb{S})$ over $\mathbb{F}_q$, with respect to the $\mathbb{F}_q$-bilinear form $Tr_{q^3/q} \circ \mathbf{b}$, described at the beginning of this section, is

$$\{\langle z, g(z)\rangle \colon z \in \mathbb{F}_{q^6}^*\}, \quad \text{where } g(z) = \lambda^{q^3} z + \mu z^{q^3} + \alpha^{\sigma^{-1}q^3} z^{\sigma^{-1}} + \beta^{\sigma^{-1}} z^{\sigma^{-1}q^3}.$$

Using the collineation $\langle x, y\rangle \mapsto \langle y, x\rangle$ of $\mathcal{G}$, we get that the $\mathcal{G}$-orbit corresponding to the isotopism class of the translation dual $\mathbb{S}^{\perp}$ of $\mathbb{S}$ is $L(\mathbb{S}^{\perp})^{\mathcal{G}}$, with

$$L\big(\mathbb{S}^{\perp}\big) = \{\langle \lambda^{q^3} z + \mu z^{q^3} + \alpha^{\sigma^{-1}q^3} z^{\sigma^{-1}} + \beta^{\sigma^{-1}} z^{\sigma^{-1}q^3}, z\rangle \colon z \in \mathbb{F}_{q^6}^*\} = L\big(\lambda^{q^3}, \mu, \alpha^{\sigma^{-1}q^3}, \beta^{\sigma^{-1}}, \sigma^{-1}\big).$$

Hence, by [2, Theorem 2.1], by Theorem 3.2 and by the previous arguments it follows

**Theorem 3.3.** *Up to isotopism, the multiplication for a presemifield $\mathbb{S} = (\mathbb{F}_{q^6}, +, \star)$ belonging to the class $\mathcal{F}_5$ and whose associated $\mathbb{F}_q$-pseudoregulus has one of its transversal lines external to the quadric $\mathcal{Q}$ can be written in the following fashion*

$$x \star y = \big(\lambda y + \mu y^{q^3} + \alpha y^{\sigma} + \beta y^{\sigma q^3}\big)x + yx^{q^3}, \tag{7}$$

*where $\lambda, \mu, \alpha, \beta \in \mathbb{F}_{q^6}$, $\sigma \in \{q, q^2, q^4, q^5\}$ and $N(\alpha) \neq N(\beta)$; such that*

$$\forall y \in \mathbb{F}_{q^6}^*\colon \quad N(y) \neq N\big(\lambda y + \mu y^{q^3} + \alpha y^{\sigma} + \beta y^{\sigma q^3}\big). \tag{8}$$

*Also, the elements $\lambda$ and $\mu$ can be taken up to their norms over $\mathbb{F}_{q^3}$. We denote such a semifield by $\mathbb{S} = \mathbb{S}(\lambda, \mu, \alpha, \beta, \sigma)$. The isotopism class of the transposed presemifield is given by*

$$\big[\mathbb{S}^t\big] = \big[\mathbb{S}(\lambda, \mu, \alpha, \beta, \sigma)^t\big] = \big[\mathbb{S}(\mu, \lambda, \beta, \alpha, \sigma)\big].$$

*The isotopism class of the translation dual $\mathbb{S}^{\perp}$ of $\mathbb{S}$ is given by*

$$\big[\mathbb{S}^{\perp}\big] = \big[\mathbb{S}(\lambda, \mu, \alpha, \beta, \sigma)^{\perp}\big] = \big[\mathbb{S}\big(\lambda^{q^3}, \mu, \alpha^{\sigma^{-1}q^3}, \beta^{\sigma^{-1}}, \sigma^{-1}\big)\big].$$

**Remark 3.4.** Note that $\mathbb{S}(\lambda, \mu, \alpha, \beta, \sigma) = \mathbb{S}(\lambda, \mu, \beta, \alpha, \sigma q^3)$.

## 4. Nuclei

The definition of nuclei of a semifield can be found, for instance, in [5]. If $\mathbb{S}$ is a presemifield, then $\mathbb{S}$ turns out to be isotopic to a semifield, say $\mathbb{S}'$. Since the size of the center as well as the size of the nuclei of a semifield are invariant under isotopy, we will say that a presemifield $\mathbb{S}$ has left (respectively, middle and right) nucleus of order $q'$, and we write $q' = |\mathbb{N}_l(\mathbb{S})|$ (respectively, $|\mathbb{N}_m(\mathbb{S})|$ and $|\mathbb{N}_r(\mathbb{S})|$) if the left (respectively, middle and right) nucleus of a semifield $\mathbb{S}'$ isotopic to it has order $q'$ (see [12, Theorem 2.1 and Remark 2.2]).

Let $\mathbb{S}$ be a presemifield belonging to the class $\mathcal{F}_5$ and whose associated $\mathbb{F}_q$-pseudoregulus has one of its transversal lines external to the quadric $\mathcal{Q}$. Then by Theorem 3.3, up to isotopism, the multiplication of $\mathbb{S} = \mathbb{S}(\lambda, \mu, \alpha, \beta, \sigma)$ is

$$x \star y = \big(\lambda y + \mu y^{q^3} + \alpha y^{\sigma} + \beta y^{\sigma q^3}\big)x + yx^{q^3},$$

where $\lambda, \mu, \alpha, \beta \in \mathbb{F}_{q^6}$, $\sigma \in \{q, q^2, q^4, q^5\}$ and $N(\alpha) \neq N(\beta)$; such that

$$\forall y \in \mathbb{F}_{q^6}^*: \quad N(y) \neq N\big(\lambda y + \mu y^{q^3} + \alpha y^{\sigma} + \beta y^{\sigma q^3}\big).$$

Let $S = S(\lambda, \mu, \alpha, \beta, \sigma) = \{\varphi_y : x \mapsto (\lambda y + \mu y^{q^3} + \alpha y^{\sigma} + \beta y^{\sigma q^3})x + yx^{q^3}\}$ be the spread set of linear maps associated with the presemifield $\mathbb{S}$. Then $S$ is contained in the 4-dimensional vector space $\mathbb{V} = \mathrm{End}_{\mathbb{F}_{q^3}}(\mathbb{F}_{q^6})$ of the endomorphisms of $\mathbb{F}_{q^6}$ over $\mathbb{F}_{q^3}$.

By [11, Property 2.1], the right nucleus of a semifield isotopic to $\mathbb{S}$ is isomorphic to the largest subfield of the space $\mathbb{V}$ whose elements $\varphi_{A,B} : x \mapsto Ax + Bx^{q^3}$, with $A, B \in \mathbb{F}_{q^6}$, satisfy the property

$$\varphi_{A,B} \circ \varphi_y \in S, \quad \text{for each } \varphi_y \in S.$$

Put $\ell(y) = \lambda y + \mu y^{q^3} + \alpha y^{\sigma} + \beta y^{\sigma q^3}$; then $y \mapsto \ell(y)$ is an additive map from $\mathbb{F}_{q^6} \to \mathbb{F}_{q^6}$ and

$$\varphi_{A,B} \circ \varphi_y : x \mapsto \big(A\ell(y) + By^{q^3}\big)x + \big(Ay + B\ell(y)^{q^3}\big)x^{q^3}.$$

Then

$$\begin{aligned} \varphi_{A,B} \circ \varphi_y \in S \quad &\Leftrightarrow \quad \forall y \in \mathbb{F}_{q^6}: \quad A\ell(y) + By^{q^3} = \ell\big(Ay + B\ell(y)^{q^3}\big) \\ &\Leftrightarrow \quad \forall y \in \mathbb{F}_{q^6}: \quad A\big(\lambda y + \mu y^{q^3} + \alpha y^{\sigma} + \beta y^{\sigma q^3}\big) + By^{q^3} = \ell(Ay) + \ell\big(B\ell(y)^{q^3}\big). \end{aligned} \tag{9}$$

We now look at Eq. (9) as a polynomial equation in the variable $y$. On the left-hand side, $y$ appears with degrees 1, $q^3$, $\sigma$ and $\sigma q^3$ while it is easy to check that on the right-hand side the variable $y$ appears with degrees 1, $q^3$, $\sigma$, $\sigma q^3$, $\sigma^2$ and $\sigma^2 q^3$. Since $\sigma^2 \in \{q^2, q^4\}$ and $\sigma^2 q^3 \in \{q, q^5\}$, Eq. (9) implies the two conditions

$$\alpha^{\sigma q^3 + 1} B^{\sigma} + \beta^{1+\sigma} B^{\sigma q^3} = 0 \tag{10}$$

and

$$B^{\sigma} \beta^{\sigma q^3} \alpha + B^{\sigma q^3} \beta \alpha^{\sigma} = 0. \tag{11}$$

Since $N(\alpha) \neq N(\beta)$, from Eqs. (10) and (11) we get $B = 0$, and taking this into account, Eq. (9) can be written as

$$\forall y \in \mathbb{F}_{q^6}: \quad A\big(\lambda y + \mu y^{q^3} + \alpha y^{\sigma} + \beta y^{\sigma q^3}\big) = \lambda Ay + \mu A^{q^3} y^{q^3} + \alpha A^{\sigma} y^{\sigma} + \beta A^{\sigma q^3} y^{\sigma q^3}. \tag{12}$$

From (12) we get

$$\mu\left(A - A^{q^3}\right) = 0, \tag{13}$$

$$\alpha\left(A - A^{\sigma}\right) = 0, \tag{14}$$

$$\beta\left(A - A^{\sigma q^3}\right) = 0. \tag{15}$$

If $\mu \neq 0$, since $(\alpha, \beta) \neq (0, 0)$, from conditions (13), (14) and (15) we get $A \in \mathbb{F}_q$. If $\mu = 0$, $\alpha \neq 0$ and $\beta = 0$, we have $A = A^{\sigma}$ and, hence, $A \in \mathbb{F}_{q^2}$ if $\sigma \in \{q^2, q^4\}$, whereas $A \in \mathbb{F}_q$ if $\sigma \in \{q, q^5\}$. If, on the other hand, $\mu = 0$, $\alpha = 0$ and $\beta \neq 0$ then $A = A^{\sigma q^3}$ and, hence, $A \in \mathbb{F}_{q^2}$ if $\sigma \in \{q, q^5\}$, whereas $A \in \mathbb{F}_q$ if $\sigma \in \{q^2, q^4\}$. Finally, if $\mu = 0$, $\alpha \neq 0$ and $\beta \neq 0$ then $A \in \mathbb{F}_q$. Hence, we can prove the following result.

**Theorem 4.1.** *Let $\mathbb{S} = (\mathbb{F}_{q^6}, +, \star)$ be a presemifield as in Theorem* 3.3*, then $|\mathbb{N}_r(\mathbb{S})|, |\mathbb{N}_m(\mathbb{S})| \in \{q, q^2\}$ and one of the following holds true*:

i) $\left|\mathbb{N}_m(\mathbb{S})\right| = q$ *and* $\left|\mathbb{N}_r(\mathbb{S})\right| = q^2 \quad \Leftrightarrow \quad \begin{cases} \mu = \beta = 0,\ \alpha \neq 0 \text{ and } \sigma \in \{q^2, q^4\} \text{ or} \\ \mu = \alpha = 0,\ \beta \neq 0 \text{ and } \sigma \in \{q, q^5\}, \end{cases}$

ii) $\left|\mathbb{N}_m(\mathbb{S})\right| = q^2$ *and* $\left|\mathbb{N}_r(\mathbb{S})\right| = q \quad \Leftrightarrow \quad \begin{cases} \lambda = \alpha = 0,\ \beta \neq 0 \text{ and } \sigma \in \{q^2, q^4\} \text{ or} \\ \lambda = \beta = 0,\ \alpha \neq 0 \text{ and } \sigma \in \{q, q^5\}, \end{cases}$

iii) $|\mathbb{N}_m(\mathbb{S})| = |\mathbb{N}_r(\mathbb{S})| = q$ *in the remaining cases.*

**Proof.** By the previous arguments it follows that $|\mathbb{N}_r(\mathbb{S})| \in \{q, q^2\}$. In particular $|\mathbb{N}_r(\mathbb{S})| = q^2$ if and only if $\mu = \beta = 0, \alpha \neq 0$ and $\sigma \in \{q^2, q^4\}$ or $\mu = \alpha = 0$, $\beta \neq 0$ and $\sigma \in \{q, q^5\}$. Since $[\mathbb{S}^t] = [\mathbb{S}(\lambda, \mu, \alpha, \beta, \sigma)^t] = [\mathbb{S}(\mu, \lambda, \beta, \alpha, \sigma)]$ and since the transpose operation permutes the sizes of the right and the middle nuclei and leaves invariant the sizes of the left nucleus and of the center ([7] and [9]), we have that $|\mathbb{N}_m(\mathbb{S})| \in \{q, q^2\}$ and if $|\mathbb{N}_r(\mathbb{S})| = q^2$, then $|\mathbb{N}_m(\mathbb{S})| = q$. Also, Statement ii) holds true. Finally, when the parameters $(\lambda, \mu, \alpha, \beta, \sigma)$ assume values different from those listed in i) and ii), we have $|\mathbb{N}_r(\mathbb{S})| = |\mathbb{N}_m(\mathbb{S})| = q$. □

## 5. New constructions of semifields $\mathbb{S}(\lambda, 0, \lambda, 0, q^2)$

As mentioned in the introduction, the only known examples of semifields in class $\mathcal{F}_5$, for which the corresponding $\mathbb{F}_q$-pseudoregulus has at least one transversal line external to $\mathcal{Q}$ are the examples b) and c) listed in Section 2, since the Knuth semifields of type a) have both transversals contained in $\mathcal{Q}$. These correspond to the following parameter sets $(\lambda, \mu, \alpha, \beta, \sigma)$:

b) If $\lambda = \mu = \beta = 0$ or $\lambda = \mu = \alpha = 0$ the multiplication of $\mathbb{S} = \mathbb{S}(\lambda, \mu, \alpha, \beta, \sigma)$ is given by

$$x \star y = \alpha y^{\sigma} x + y x^{q^3}$$

or

$$x \star y = \beta y^{\sigma q^3} x + y x^{q^3},$$

respectively, and hence the semifield $\mathbb{S}$ is a Generalized Twisted Field (see [3, p. 241]). In such a case the associated $\mathbb{F}_q$-pseudoregulus has both transversal lines external to $\mathcal{Q}$ and pairwise polar [10, Property 4.8].

c) If $\mu=\beta=0$, $\lambda=1$, $\alpha\neq 0$ and $\sigma\in\{q^2,q^4\}$ or $\lambda=\alpha=0$, $\mu=1$, $\beta\neq 0$ and $\sigma\in\{q^2,q^4\}$, the multiplication of $\mathbb{S}=\mathbb{S}(\lambda,\mu,\alpha,\beta,\sigma)$ is given by

$$x\star y=\big(y+\alpha y^{\sigma}\big)x+yx^{q^3}$$

or

$$x\star y=\big(y^{q^3}+\beta y^{\sigma q^3}\big)x+yx^{q^3},$$

respectively. These correspond to the examples constructed in [12] for $\alpha^{1+q^2+q^4}=1$, or $\beta^{1+q^2+q^4}=1$, and $q\equiv 1\ (mod\ 3)$. In such a case the associated $\mathbb{F}_q$-pseudoregulus has the other transversal line contained in $\mathcal{Q}$ [12, Section 4].

In what follows we show that there exist other choices for the parameter sets $(\lambda,\mu,\alpha,\beta,\sigma)$ producing semifields not isotopic to those of examples b) and c). Choose $\mu=\beta=0$, $\lambda=\alpha\neq 0$, with $N(\lambda)\neq 1$ and $\sigma=q^2$. In this way

$$\mathbb{S}=\mathbb{S}\big(\lambda,0,\lambda,0,q^2\big):\quad x\star y=\lambda\big(y+y^{q^2}\big)x+yx^{q^3}$$

and the non-singularity condition becomes

$$\forall y\in\mathbb{F}_{q^6}^*:\quad \frac{1}{N(\lambda)}\neq N\left(\frac{y+y^{q^2}}{y}\right). \tag{16}$$

**Remark 5.1.** Since $\lambda\neq 0$ and $N(\lambda)\neq 1$, the line $r'=r_{\lambda,0}$ is external to $\mathcal{Q}$ and $r'\neq r^{\perp}$. This means that the ensuing semifields, whenever they exist, are not isotopic to the known semifields belonging to $\mathcal{F}_5$ (listed as a), b), c) in Section 2).

We start by proving the following

**Lemma 5.2.** *Let $q$ be an odd prime power, $q\equiv 1\ (mod\ 3)$ and let $\xi$ be a primitive 6th root of unity in $\mathbb{F}_q$. Then*

$$2(1-\xi)\notin\left\{\left(\frac{y+y^{q^2}}{y}\right)^{q^3+1}:\ y\in\mathbb{F}_{q^6}^*\right\}. \tag{17}$$

**Proof.** First note that since $q$ is odd and $q\equiv 1\ (mod\ 3)$, we have that $q\equiv 1\ (mod\ 6)$ and so $\mathbb{F}_q$ contains 6th roots of unity. Let $\xi$ be a primitive 6th root of unity over $\mathbb{F}_q$ and let $\rho\in\mathbb{F}_q$ such that $\rho^{\frac{q-1}{6}}=\xi$. Now, let $u\in\mathbb{F}_{q^6}$ be a solution of the equation $x^6=\rho$.

Since $\rho^{\frac{q^2-1}{6}}=\xi^2$ and $\rho^{\frac{q^3-1}{6}}=\xi^3$, we have $u\notin(\mathbb{F}_{q^2}\cup\mathbb{F}_{q^3})$. Also $u^{q^i}=\xi^i u$, $i\in\{1,\dots,5\}$; indeed $u^q=uu^{q-1}=u\,(u^6)^{\frac{q-1}{6}}=u\rho^{\frac{q-1}{6}}=\xi u$. Since $\{1,u,u^2,u^3,u^4,u^5\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^6}$, each element $y\in\mathbb{F}_{q^6}$ can be written uniquely as $y=\sum_{i=0}^5 a_i u^i$, $a_i\in\mathbb{F}_q$. Taking into account that $u^{q^3}=\xi^3 u=-u$, we have that

$$\begin{aligned}N(y)=y^{q^3+1}=a_0^2+\rho\big(-a_3^2+2a_2a_4-2a_1a_5\big)+\big(a_4^2\rho+2a_0a_2-a_1^2-2a_3a_5\rho\big)u^2\\+\big(a_2^2+2a_0a_4-a_5^2\rho-2a_1a_3\big)u^4.\end{aligned}$$

Moreover,

$$N\big(y+y^{q^2}\big) = 4a_0^2 + \rho\big(-4a_3^2 + 2a_2a_4\big(\xi^2+1\big)(1-\xi) - 2a_1a_5\big(\xi^2+1\big)(1-\xi)\big) + \big[a_4^2\big(\xi^2+1\big)^2\rho + 4a_2a_0(1-\xi) - a_1^2\big(\xi^2+1\big)^2 - 4a_3a_5(1-\xi)\rho\big]u^2 + \big[a_2^2(1-\xi)^2 + 4a_0a_4\big(\xi^2+1\big) - \rho a_5^2(1-\xi)^2 - 4a_1a_3\big(\xi^2+1\big)\big]u^4.$$

Since $\rho^{\frac{q-1}{2}} = \xi^3 = -1$ and since $\{1, u^2, u^4\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^3}$, straightforward computations show that $2(1-\xi)N(y) = N(y+y^{q^2})$ if and only if $y=0$; this implies (17). □

Now, we can prove

**Theorem 5.3.** *Let $q$ be an odd prime power, $q \equiv 1 \pmod 3$ and let $\xi$ be a primitive 6th root of unity over $\mathbb{F}_q$; then the multiplications*

$$x \star y = \lambda\big(y+y^{q^2}\big)x + yx^{q^3} \quad \text{and} \quad x \star' y = \lambda\big(y^{q^3}+y^{q^5}\big)x + yx^{q^3},$$

*where $\lambda \in \mathbb{F}_{q^6}$ such that $N(\lambda) = \frac{1}{2(1-\xi)}$, define the presemifields $\mathbb{S} = (\mathbb{F}_{q^6}, +, \star)$ and $\mathbb{S}' = (\mathbb{F}_{q^6}, +, \star')$ with $|\mathbb{N}_r(\mathbb{S})| = |\mathbb{N}_m(\mathbb{S}')| = q^2$ and $|\mathbb{N}_m(\mathbb{S})| = |\mathbb{N}_r(\mathbb{S}')| = q$, belonging to the class $\mathcal{F}_5$. Also, $[\mathbb{S}^t] = [\mathbb{S}']$, the presemifields $\mathbb{S}$ and $\mathbb{S}'$ are not isotopic and are not isotopic to any previously known semifield.*

**Proof.** By Lemma 5.2, if $\lambda$ is an element of $\mathbb{F}_{q^6}$ such that $N(\lambda) = \frac{1}{2(1-\xi)}$, the non-singularity condition (16) is satisfied and hence we get a presemifield $\mathbb{S} = (\mathbb{F}_{q^6}, +, \star) = \mathbb{S}(\lambda, 0, \lambda, 0, q^2)$, where $x \star y = \lambda(y+y^{q^2})x + yx^{q^3}$, belonging to the family $\mathcal{F}_5$ and with $|\mathbb{N}_m(\mathbb{S})| = q$ and $|\mathbb{N}_r(\mathbb{S})| = q^2$ (see Theorem 4.1). Also, the associated $\mathbb{F}_q$-pseudoregulus has both the transversal lines $r$ and $r' = r_{\lambda,0}$ external to the quadric $\mathcal{Q}$ (indeed $\lambda \neq 0$ and $N(\lambda) \neq 1$ for each $q \equiv 1 \pmod 3$) and $r' \neq r^\perp$. Hence, by Remark 5.1, the presemifield $\mathbb{S}$ is not isotopic to any previously known semifield. By Theorem 3.3, $[\mathbb{S}'] = [\mathbb{S}^t] = [\mathbb{S}(0, \lambda, 0, \lambda, q^2)]$ and by using Theorem 4.1 and by Remark 5.1, the remaining parts of the statement follow. □

Now we focus on the case $q$ even, starting from the following technical lemma.

**Lemma 5.4.** *If $q = 2^{2h}$ and $h \equiv 1 \pmod 3$, then $\frac{q-1}{3} \equiv 1 \pmod 3$.*

**Proof.** If $q = 2^{2h}$ and $h = 1+3k$, then $\frac{q-1}{3} = 4^{3k} + 4^{3k-1} + \cdots + 4^2 + 4 + 1 \equiv 1 \pmod 3$. □

**Lemma 5.5.** *Let $q = 2^{2h}$, such that $h \equiv 1 \pmod 3$, $\eta$ be a primitive 3th root of unity over $\mathbb{F}_q$ and let $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ such that $u^3 = \eta$. Then*

$$\eta(1+u) \notin \left\{ \left( \frac{y+y^{q^2}}{y} \right)^{q^3+1} : y \in \mathbb{F}_{q^6}^* \right\}. \tag{18}$$

**Proof.** Since $q \equiv 1 \pmod 3$, the finite field $\mathbb{F}_q$ contains a primitive 3rd root of unity, say $\eta$. Since $h \equiv 1 \pmod 3$ we have $\frac{q-1}{3} \equiv 1 \pmod 3$, by the previous lemma. Hence, there exists an element $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ such that $u^3 = \eta$ and $u^q = uu^{q-1} = u(u^3)^{\frac{q-1}{3}} = u\eta^{\frac{q-1}{3}} = u\eta$. Since $\{1, u, u^2\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^6}$, any element $y \in \mathbb{F}_{q^6}$ can be uniquely written as $y = \alpha + \beta u + \gamma u^2$, with $\alpha, \beta, \gamma \in \mathbb{F}_{q^2}$. Condition (18) is equivalent to show that

$$\eta(1+u)N(y) = N\big(y+y^{q^2}\big) \quad \text{if and only if } y = 0. \tag{19}$$

Moreover, condition (19) corresponds to

$$\begin{aligned}&\eta(1+u)\big[\alpha^{1+q}+(\beta\gamma^q+\beta^q\gamma)\eta+(\alpha\beta^q+\alpha^q\beta+\gamma^{1+q}\eta)u+(\alpha\gamma^q+\alpha^q\gamma+\beta^{q+1})u^2\big]\\&\quad=(\beta\gamma^q+\beta^q\gamma)\eta+\eta^2\gamma^{1+q}u+\beta^{1+q}\eta^2u^2\end{aligned}$$

if and only if $(\alpha,\beta,\gamma)=(0,0,0)$, namely

$$\begin{aligned}&\big[\alpha^{1+q}+(\beta\gamma^q+\beta^q\gamma)\eta+(\alpha\gamma^q+\alpha^q\gamma+\beta^{q+1})\eta\big]\\&\quad+\big[\alpha\beta^q+\alpha^q\beta+\gamma^{1+q}\eta+\alpha^{1+q}+(\beta\gamma^q+\beta^q\gamma)\eta\big]u\\&\quad+\big[\alpha\gamma^q+\alpha^q\gamma+\beta^{q+1}+\alpha\beta^q+\alpha^q\beta+\gamma^{1+q}\eta\big]u^2\\&=(\beta\gamma^q+\beta^q\gamma)+\eta\gamma^{1+q}u+\beta^{1+q}\eta u^2.\end{aligned}\tag{20}$$

If $\gamma=0$, since $\{1,u,u^2\}$ is an $\mathbb{F}_q$-basis, from (20) we get

$$\begin{cases}\alpha^{q+1}+\beta^{q+1}\eta=0,\\ \alpha^q\beta+\beta^q\alpha+\alpha^{q+1}=0,\\ \beta^{q+1}+\alpha^q\beta+\beta^q\alpha=\beta^{q+1}\eta\end{cases}$$

and hence $\alpha=\beta=0$, i.e. $y=0$.

Suppose, on the other hand, that $\gamma\neq0$. Dividing Eq. (20) by $\gamma^{q+1}$ and replacing $\alpha/\gamma$ by $\alpha$ and $\beta/\gamma$ by $\beta$, Eq (20) is equivalent to the following system

$$\begin{cases}\beta+\beta^q=\alpha^{1+q}+(\beta+\beta^q)\eta+(\alpha+\alpha^q+\beta^{1+q})\eta,\\ 0=\alpha\beta^q+\alpha^q\beta+\alpha^{1+q}+\eta(\beta+\beta^q),\\ \beta^{1+q}\eta=\alpha+\alpha^q+\beta^{1+q}+\alpha\beta^q+\alpha^q\beta+\eta.\end{cases}\tag{21}$$

Now, let $\xi\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ such that $\xi^2+\xi+\rho=0$, with $\rho\in\mathbb{F}_q$ and $Tr_{q/2}(\rho)=1$. So, writing $\alpha=x+y\xi$ and $\beta=z+t\xi$, with $x,y,z,t\in\mathbb{F}_q$ and taking into account that $\alpha+\alpha^q=y$, $\alpha^{q+1}=x^2+xy+y^2\rho$ and $\alpha^q\beta+\beta^q\alpha=xt+yz$, system (21) becomes

$$\begin{cases}t=x^2+xy+y^2\rho+t\eta+\eta(y+z^2+zt+t^2\rho),\\ 0=xt+yz+x^2+xy+y^2\rho+\eta t,\\ (z^2+zt+t^2\rho)\eta=y+z^2+zt+t^2\rho+xt+yz+\eta.\end{cases}\tag{22}$$

Now, the assertion is proven if we show that system (22) has no solution $(x,y,z,t)\in\mathbb{F}_q^4$. To this aim we start by noting that if $(x,y,z,0)$ were a solution of (22), then by adding the three equations of (22), and multiplying by $\eta$ we obtain

$$y=\eta z^2+\eta^2.$$

By substituting this value of $y$ in the third equation of system (22), we get

$$z^3+\eta^2z^2+\eta z+\eta^2=0,$$

which means that $z$ is a solution of the cubic equation

$$X^3+\eta^2X^2+\eta X+\eta^2=0,$$

with coefficients in $\mathbb{F}_q$. Hence, $z\in\{\eta^2+u,\eta^2+\eta u,\eta^2+\eta^2u\}$ and so $z\notin\mathbb{F}_q$; a contradiction.

Now suppose $(x, y, z, t) \in \mathbb{F}_q^4$ with $t \neq 0$ is a solution of system (22). By adding the three equations of (22), and multiplying by $\eta$, we get

$$y = \eta R + t\eta + \eta^2, \tag{23}$$

where $R = z^2 + zt + \rho t^2$. Then by adding the first two equations of (22) and substituting (23) we have

$$tx = \eta Rz + R + \eta tz + \eta^2 z + \eta t + 1. \tag{24}$$

Since $t \neq 0$, by solving (24) in $x$ and substituting in the first equation of system (22) we get

$$R^3 + \eta^2 R^2 t + \eta R^2 + Rt^2 + \eta Rt + t^3 + \eta^2 R + \eta t^2 + t + \eta = 0. \tag{25}$$

Hence, if system (22) admits a solution $(x, y, z, t) \in \mathbb{F}_q^4$, with $t \neq 0$ then the algebraic curve $\Gamma$ of order 6 of the projective plane $\mathrm{PG}(2, \mathbb{F})$, where $\mathbb{F}$ is the algebraic closure of $\mathbb{F}_q$, defined by Eq. (25) has an $\mathbb{F}_q$-rational point $P = (z, t)$, with $t \neq 0$. Let $\phi$ be the semilinear collineation of $\mathrm{PG}(2, \mathbb{F})$ induced by the $\mathbb{F}_q$-automorphism $x \mapsto x^q$; from (25) we have that $\Gamma^\phi = \Gamma$. Moreover, direct computation shows that $\Gamma$ is the union of the two cubic curves of $\mathrm{PG}(2, \mathbb{F})$, say $\mathcal{C}_3$ and $\mathcal{C}_3'$, with equations

$$\begin{aligned} G(z,t) = {} & z^3 + (\xi+1)z^2 t + \eta^2 z^2 + \xi^2 zt^2 + zt + \eta z + \xi\rho t^3 + \big(\xi\eta + \rho\eta^2\big)t^2 \\ & + \big(\eta^2 + \xi\eta\big)t + \eta^2 = 0 \end{aligned} \tag{26}$$

and

$$\begin{aligned} G_1(z,t) = {} & z^3 + \xi z^2 t + \eta^2 z^2 + \big(\xi^2+1\big)zt^2 + zt + \eta z + (\xi+1)\rho t^3 + \big((\xi+1)\eta + \rho\eta^2\big)t^2 \\ & + \big(\eta^2 + (\xi+1)\eta\big)t + \eta^2 = 0, \end{aligned} \tag{27}$$

respectively. In particular, since $\xi^q = \xi + 1$, we get $\mathcal{C}_3' = \mathcal{C}_3^\phi$ and $\mathcal{C}_3^{\phi^2} = \mathcal{C}_3$. If $P = (\bar{z}, \bar{t})$, with $\bar{t} \neq 0$ were an $\mathbb{F}_q$-rational point of $\Gamma$ then $P \in \mathcal{C}_3 \cap \mathcal{C}_3'$ and hence we would have $G(\bar{z}, \bar{t}) + G_1(\bar{z}, \bar{t}) = 0$, i.e.

$$\overline{R} = \eta(\bar{t} + 1), \tag{28}$$

where $\overline{R} = \bar{z}^2 + \bar{z}\bar{t} + \rho\bar{t}^2$. Taking into account (28), from (25) we obtain $\bar{t} = 1$ and hence $\bar{z}^2 + \bar{z} + \rho = 0$ and, since $Tr_{q/2}(\rho) = 1$, this again implies that $\bar{z} \notin \mathbb{F}_q$, a contradiction. Hence, the assertion follows. □

Then, we have the following

**Theorem 5.6.** *Let $q = 2^{2h}$, such that $h \equiv 1 \pmod 3$, $\eta$ be a primitive 3rd root of unity over $\mathbb{F}_q$ and let $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ such that $u^3 = \eta$; then the multiplications*

$$x \star y = \lambda\big(y + y^{q^2}\big)x + yx^{q^3} \quad \text{and} \quad x \star' y = \lambda\big(y^{q^3} + y^{q^5}\big)x + yx^{q^3},$$

*where $\lambda \in \mathbb{F}_{q^6}$ such that $N(\lambda) = \frac{1}{\eta(1+u)}$, define the presemifields $\mathbb{S} = (\mathbb{F}_{q^6}, +, \star)$ and $\mathbb{S}' = (\mathbb{F}_{q^6}, +, \star')$ with $|\mathbb{N}_r(\mathbb{S})| = |\mathbb{N}_m(\mathbb{S}')| = q^2$ and $|\mathbb{N}_m(\mathbb{S})| = |\mathbb{N}_r(\mathbb{S}')| = q$, belonging to the class $\mathcal{F}_5$. Also, $[\mathbb{S}^t] = [\mathbb{S}']$, the presemifields $\mathbb{S}$ and $\mathbb{S}'$ are not isotopic and are not isotopic to any previously known semifield.*

**Proof.** By using Lemma 5.5 and arguing as in the proof of Theorem 5.3, we get the assertion. □

**Lemma 5.7.** *Let $q = 3^h$ with $h \not\equiv 0 \pmod 3$ and let $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ such that $u^3 = u + 1$. Then,*

$$-(u+u^2) \notin \left\{ \left( \frac{y+y^{q^2}}{y} \right)^{q^3+1} : y \in \mathbb{F}_{q^6}^* \right\}. \tag{29}$$

**Proof.** First note that, since $q = 3^h$ the polynomial $x^3 - x - 1$ has roots in $\mathbb{F}_{3^3} \setminus \mathbb{F}_3$, and since $h \not\equiv 0 \pmod 3$ it is irreducible over $\mathbb{F}_q$. This means that it has 3 distinct roots in $\mathbb{F}_{q^3}$, conjugate over $\mathbb{F}_q$. Hence, there exists an element $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ such that $u^3 = u+1$. Also, using the fact that $u + u^q + u^{q^2} = 0$ and $u^{q^2+q+1} = 1$, straightforward computations show that $\{u^q, u^{q^2}\} = \{1+u, -1+u\}$. In order to take this fact into account in what follows, we put $u^q = \epsilon + u$, where $\epsilon = \pm 1$, and hence $u^{q^2} = -\epsilon + u$. Note that condition (29) is equivalent to show that

$$-(u+u^2)N(y) = N\left(y + y^{q^2}\right), \tag{30}$$

if and only if $y = 0$. Now, since $\{1, u, u^2\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^3}$ (and hence an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^6}$), any element $y \in \mathbb{F}_{q^6}$ can be uniquely written as $y = \alpha + \beta u + \gamma u^2$, where $\alpha, \beta, \gamma \in \mathbb{F}_{q^2}$.

As in the proof of Lemma 5.5, we first assume $\gamma = 0$. Hence

$$N(y) = \alpha^{q+1} + (\alpha\beta^q + \alpha^q\beta)u + \beta^{q+1}u^2$$

and

$$N\left(y + y^{q^2}\right) = (\alpha + \beta\epsilon)^{q+1} + \left((\alpha + \beta\epsilon)\beta^q + \left(\alpha^q + \beta^q\epsilon\right)\beta\right)u + \beta^{q+1}u^2,$$

from Eq. (30), we get

$$\begin{cases} -(\alpha\beta^q + \alpha^q\beta) - \beta^{q+1} = (\alpha + \beta\epsilon)^{q+1}, \\ \beta^{1+q} - \alpha^{1+q} - (\alpha\beta^q + \alpha^q\beta) = (\alpha + \beta\epsilon)\beta^q + \left(\alpha^q + \beta^q\epsilon\right)\beta, \\ -\alpha^{1+q} - (\alpha\beta^q + \alpha^q\beta) - \beta^{q+1} = \beta^{1+q}. \end{cases} \tag{31}$$

From the third equation of (31) we get

$$\beta^{q+1} - \alpha^{1+q} - (\alpha\beta^q + \alpha^q\beta) = 0$$

and hence from the second equation we have

$$\alpha\beta^q + \alpha^q\beta - \beta^{q+1}\epsilon = 0. \tag{32}$$

Taking into account (32) in the first equation of (31), we get

$$\alpha^{q+1} = -\epsilon\beta^{q+1}. \tag{33}$$

So, system (31) is equivalent to

$$\begin{cases} \alpha^{q+1} + \epsilon\beta^{q+1} = 0, \\ \alpha\beta^q + \alpha^q\beta - \epsilon\beta^{q+1} = 0, \\ \alpha\beta^q + \alpha^q\beta - \beta^{q+1} + \alpha^{q+1} = 0, \end{cases}$$

which admits as unique solution $\beta = \alpha = 0$, i.e. $y = 0$.

Suppose now $\gamma \neq 0$. As in Lemma 5.5, up to replacing $\alpha/\gamma$ by $\alpha$ and $\beta/\gamma$ by $\beta$, without loss of generality, we can suppose $y = \alpha + \beta u + u^2$, with $\alpha, \beta \in \mathbb{F}_{q^2}$.

In such a case, we have

$$N(y) = \left(\alpha^{q+1} + \beta + \beta^q\right) + \left(\alpha\beta^q + \alpha^q\beta + \beta + \beta^q + 1\right)u + \left(\beta^{q+1} + \alpha + \alpha^q + 1\right)u^2$$

and

$$\begin{aligned} N\left(y + y^{q^2}\right) = {} & \left[(-\alpha - \beta\epsilon + 1)^{q+1} + (\beta - \epsilon) + (\beta - \epsilon)^q\right] \\ & - \left[(-\alpha - \beta\epsilon + 1)(\beta - \epsilon)^q + (-\alpha - \beta\epsilon + 1)^q(\beta - \epsilon) - (\beta - \epsilon) - \left(\beta^q - \epsilon\right) - 1\right]u \\ & + \left[(-\alpha - \beta\epsilon + 1) + \left(-\alpha^q - \beta^q\epsilon + 1\right) + (\beta - \epsilon)\left(\beta^q - \epsilon\right) + 1\right]u^2. \end{aligned}$$

Again taking into account $u^3 = u + 1$ and $u^4 = u^2 + u$, Eq. (29) is equivalent to the following system

$$\begin{cases} \alpha^{q+1} - \beta^{q+1} + \left(\alpha\beta^q + \alpha^q\beta\right)(1 + \epsilon) + \left(\beta + \beta^q\right)(-1 - \epsilon) + \epsilon = 0, \\ -\alpha^{q+1} + (1 + \epsilon)\beta^{q+1} + \left(\alpha\beta^q + \alpha^q\beta\right) + (1 + \epsilon)\left(\alpha + \alpha^q\right) - \left(\beta + \beta^q\right) - 1 = 0, \\ \alpha^{q+1} - \beta^{q+1} + \left(\alpha\beta^q + \alpha^q\beta\right) - \left(\alpha + \alpha^q\right) - \left(\beta + \beta^q\right) - 1 = 0. \end{cases} \tag{34}$$

Let $\epsilon = -1$. Then system (34) becomes

$$\alpha^{q+1} - \beta^{q+1} - 1 = 0, \tag{35}$$

$$-\alpha^{q+1} + \alpha\beta^q + \alpha^q\beta - \beta - \beta^q - 1 = 0, \tag{36}$$

$$\alpha^{q+1} - \beta^{q+1} + \alpha\beta^q + \alpha^q\beta - \alpha - \alpha^q - \beta - \beta^q - 1 = 0, \tag{37}$$

which is equivalent to the following incompatible system

$$\begin{cases} \beta^{q+1} = \alpha^{q+1} - 1, \\ \alpha\beta^q + \alpha^q\beta - \beta - \beta^q - 1 = \alpha^{q+1}, \\ \alpha^{q+1} - \alpha^q - \alpha + 1 = \alpha^q(\alpha - 1) - (\alpha - 1) = 0. \end{cases}$$

In the case $\epsilon = 1$, arguing in a similar way we have the assertion. □

So, we have the following

**Theorem 5.8.** *Let $q = 3^h$ with $h \not\equiv 0 \pmod 3$ and let $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ such that $u^3 = u + 1$. Then*

$$x \star y = \lambda\left(y + y^{q^2}\right)x + yx^{q^3} \quad \text{and} \quad x \star' y = \lambda\left(y^{q^3} + y^{q^5}\right)x + yx^{q^3},$$

*where $\lambda \in \mathbb{F}_{q^6}$ such that $N(\lambda) = \frac{1}{-(u+u^2)}$, define the presemifields $\mathbb{S} = (\mathbb{F}_{q^6}, +, \star)$ and $\mathbb{S}' = (\mathbb{F}_{q^6}, +, \star')$ with $|\mathbb{N}_r(\mathbb{S})| = |\mathbb{N}_m(\mathbb{S}')| = q^2$ and $|\mathbb{N}_m(\mathbb{S})| = |\mathbb{N}_r(\mathbb{S}')| = q$, belonging to the class $\mathcal{F}_5$. Also, $[\mathbb{S}^t] = [\mathbb{S}']$, the presemifields $\mathbb{S}$ and $\mathbb{S}'$ are not isotopic and are not isotopic to any previously known semifield.*

**Proof.** By using Lemma 5.7 and arguing as in the proof of Theorem 5.3, we get the assertion. □

## 6. Computational results

We conclude this paper with some observations from the computational results which we obtained using the computer algebra system MAGMA [1].

For $q = 2$, an exhaustive search shows that there are no new semifields $\mathbb{S}(\lambda, \mu, \alpha, \beta, \sigma)$. We remark that semifields of order 64 were recently classified by Rùa et al. in [13], and our computational result can also be obtained from the properties of semifields $\mathbb{S}(\lambda, \mu, \alpha, \beta, \sigma)$, and the information listed in [13, Table 1].

For $q > 2$, besides the examples that belong to the infinite families from the previous section, we obtained many new examples of semifields $\mathbb{S}(\lambda, \mu, \alpha, \beta, \sigma)$ of order $3^6$ and $4^6$, with $(\mu, \beta) \neq (0, 0)$ and $\alpha \neq \lambda$. As an illustration we list some of these examples below. Note that we have not done any exhaustive computer searches, except in the case that $q = 3$, and the transversal $r_{\lambda,\mu}$ is tangent to the hyperbolic quadric $\mathcal{Q}$, where we found no examples.

| $q$ | $\sigma$ | $\lambda$ | $\mu$ | $\alpha$ | $\beta$ | $r_{\lambda,\mu}$ is | Comments |
|---|---|---|---|---|---|---|---|
| 2 | $q$ | | | | | | no result (Exhaustive search) |
| 3 | $q$ | $z$ | $z^5$ | $z^{25}$ | $z^{93}$ | External | |
| 3 | | | | | | Tangent | no result (Exhaustive search) |
| 3 | $q$ | $z^{15}$ | $z^{20}$ | $z$ | $z^{403}$ | Secant | |
| 4 | $q$ | $z^5$ | $z^{40}$ | $z^{43}$ | $z^{31}$ | External | |
| 4 | $q$ | $z^5$ | $z^{30}$ | 1 | $z^{230}$ | Tangent | |
| 4 | $q$ | $z^{70}$ | $z^{20}$ | $z^{85}$ | $z^{2022}$ | Secant | |

## References


[1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (3–4) (1997) 235–265.

[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] P. Dembowski, Finite Geometries, Springer-Verlag, Berlin, 1968.

[4] N.L. Johnson, V. Jha, M. Biliotti, Handbook of Finite Translation Planes, Pure Appl. Math., Taylor Books, 2007.

[5] M. Lavrauw, O. Polverino, Finite semifields, in: J. De Beule, L. Storme (Eds.), Current Research Topics in Galois Geometries, Nova Academic Publishers, in press.

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

[7] G. Lunardon, Symplectic spreads and finite semifields, Des. Codes Cryptogr. 44 (1–3) (2007) 39–48.

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

[9] D.M. Maduram, Transposed translation planes, Proc. Amer. Math. Soc. 53 (1975) 265–270.

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

[11] G. Marino, O. Polverino, R. Trombetti, On semifields of type $(q^{2n}, q^n, q^2, q^2, q)$, $n$ odd, Innov. Incidence Geom. 6 (2008) 209–227.

[12] G. Marino, O. Polverino, R. Trombetti, Towards the classification of rank 2 semifields 6-dimensional over their center, Des. Codes Cryptogr., doi:10.1007/s10623-010-9436-2, in press.

[13] I.F. Rúa, E.F. Combarro, J. Ranilla, Classification of 64-element finite semifields, J. Algebra 322 (2009) 4011–4029.