J Algebr Comb (2009) 29: 1–34
DOI 10.1007/s10801-007-0116-x

On a generalization of cyclic semifields

**Norman L. Johnson · Giuseppe Marino ·
Olga Polverino · Rocco Trombetti**

Received: 5 January 2007 / Accepted: 15 December 2007 / Published online: 3 January 2008

Abstract A new construction is given of cyclic semifields of orders q^{2n}, n odd, with kernel (left nucleus) $\mathbb{F}_{q^n}$ and right and middle nuclei isomorphic to $\mathbb{F}_{q^2}$, and the isotopism classes are determined. Furthermore, this construction is generalized to produce potentially new semifields of the same general type that are not isotopic to cyclic semifields. In particular, a new semifield plane of order 4^5 and new semifield planes of order 16^5 are constructed by this method.

Keywords Cyclic semifield · Net replacement · Lifting

N.L. Johnson
Mathematics Dept., University of Iowa, Iowa City, IA 52242, USA
e-mail: njohnson@math.uiowa.edu

G. Marino · R. Trombetti
Dipartimento di Matematica e Applicazioni, Università degli Studi di Napoli “Federico II”,
80126 Napoli, Italy

G. Marino
e-mail: giuseppe.marino@unina.it

R. Trombetti
e-mail: rtrombet@unina.it

O. Polverino (✉)
Dipartimento di Matematica, Seconda Università degli Studi di Napoli, 81100 Caserta, Italy
e-mail: opolveri@unina.it

O. Polverino
e-mail: olga.polverino@unina2.it

1 Introduction

Finite semifields are of fundamental importance in the study of finite affine and projective planes and seem to appear in various classification results and construction procedures.

For example, in the classification of finite translation planes admitting non-solvable doubly transitive groups on line size sets, due to Ganley, Jha and Johnson [9], towards the end of the study, an unusual possibility arises: whether a semifield plane could admit a non-solvable collineation group acting doubly transitive on a parabolic oval. Ultimately, the semifield plane is shown to be a generalized twisted field plane. It is only through the knowledge that the full collineation group of any generalized twisted field plane is solvable (see Biliotti, Jha, Johnson [5]) that this case can be completely ruled out.

There are intimate connections between commutative semifields and symplectic semifield planes, as shown by Kantor [16]; the transpose+dual of a commutative semifield plane produces a symplectic semifield plane. In the Suetake planes of order q^n, where q and n are both odd, admitting a collineation group with two long orbits of length $(q^n-1)/2$ on the set of components, there is a class of associated generalized twisted field planes. In fact, such generalized twisted field planes are symplectic and by reversing the construction procedure, [2], Ball, Bamberg, Lavrauw, Penttila have shown that the Suetake planes are also symplectic, the first such non-semifield symplectic planes known of odd dimension and odd characteristic.

Another example of unlikely places for semifields to show up is in 'generalized Desarguesian' planes of Jha-Johnson [12, 13]. Starting with a translation plane of order q^3 admitting a collineation group isomorphic to $GL(2,q)$ acting canonically as in an associated Desarguesian plane of order q^3, it is possible to construct a type of semifield plane called a cyclic semifield plane. Conversely, any cyclic semifield plane of order q^3 constructs a generalized Desarguesian plane.

A cyclic semifield plane of order q^n is defined as follows: assume that T is an element of $\Gamma L(n,q)$, which is strictly semilinear and irreducible over $\mathbb{F}_q$. Then, there is a non-identity automorphism σ of $\mathbb{F}_q$ such that

$$\alpha T = T\alpha^{\sigma}, \forall \alpha \in \mathbb{F}_q.$$

The following defines a spread set and a corresponding semifield plane, called a *"cyclic semifield plane"*:

$$\begin{aligned}&\big\{x=0, y=x(\alpha_0+\alpha_1 T+\alpha_2 T^2+\cdots+\alpha_{n-1}T^{n-1});\\ &\quad \alpha_i\in\mathbb{F}_q,\ i=0,1,2,\dots,n-1\big\}.\end{aligned}$$

This construction generalizes that of Sandler [21] and is due to Jha-Johnson [11, 13].

If $n=3$, there are connections with generalized Desarguesian spreads. If S_3 is a cyclic semifield plane of order q^3, consider the group G isomorphic to $GL(2,q)$ acting canonically as a matrix group:

$$\left\langle \begin{pmatrix} a & b\\ c & d\end{pmatrix};\ ad-bc\neq 0, a,b,c,d\in\mathbb{F}_q\right\rangle.$$

If T defines S_3 as above, the following becomes a spread set:

$$\left\{x=0, y=x\alpha; \alpha\in\mathbb{F}_q\right\}\cup\{(y=xT)g;\ g\in G\}.$$

Such a translation plane admits $GL(2,q)$ as a collineation group and conversely any such plane constructs a cyclic semifield plane.

In a related article, the authors [14] determine all the cyclic semifields of order q^6 that are of dimension 6 over the associated centers and have right and middle nucleus isomorphic to $\mathbb{F}_{q^2}$ and left nucleus isomorphic to $\mathbb{F}_{q^3}$. In the same paper it has been proven that any semifield of order q^6 with left nucleus isomorphic to $\mathbb{F}_{q^3}$, middle and right nuclei both isomorphic to $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$ is isotopic to a cyclic semifield and hence it belongs to the so called family $\mathcal{F}_4$ of semifields 2-dimensional over their left nucleus and 6-dimensinal over their center, introduced in [20].

In this article, we determine all the cyclic semifields of order q^{2n}, n odd, with left nucleus isomorphic to $\mathbb{F}_{q^n}$, middle and right nuclei both isomorphic to $\mathbb{F}_{q^2}$ and center isomorphic to $\mathbb{F}_q$. Some of these were previously constructed by Jha–Johnson in [11] (see Section 10). Moreover, we generalize this family constructing a family of semifields with the same parameters. This wider family contains new classes of semifields not cyclic but isotopic to cyclic semifields (*semifields of degree 2*) and, for $q=2,4$ and $n=5$, examples of semifields not isotopic to any previously known semifield.

Furthermore, we are able to give a lower bound for the number of isotopism classes of cyclic semifields. In particular, for $q=p^h$, denoting by θ the number of elements of $\mathbb{F}_{q^n}$ not belonging to any proper subfield of $\mathbb{F}_{q^n}$, there are at least

$$\frac{q^n-\theta}{2nhq(q-1)}$$

mutually non-isotopic cyclic semifields.

2 Semifields, semifield spreads and spread sets

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

$$N_l=\{a\in\mathbb{S}\mid(ab)c=a(bc),\ \forall b,c\in\mathbb{S}\},$$

$$N_m=\{b\in\mathbb{S}\mid(ab)c=a(bc),\ \forall a,c\in\mathbb{S}\},$$

$$N_r=\{c\in\mathbb{S}\mid(ab)c=a(bc),\ \forall a,b\in\mathbb{S}\}$$

and

$$\mathcal{K}=\{a\in N_l\cap N_m\cap N_r\mid ab=ba,\ \forall b\in\mathbb{S}\}$$

are fields and are known, respectively, as the *left nucleus*, *middle nucleus*, *right nucleus* and *center* of the semifield. A finite semifield is a vector space over its nuclei and its center (for more details on semifields see [6] and [8]).

To any semifield spread $\mathcal{S}$ of $PG(3,q)$ it is possible to associate a translation plane $\pi(\mathcal{S})$ of order q^2, called a *semifield plane*, via the well known André–Bruck and Bose construction; i.e. a projective plane coordinatized by a semifield, of order q^2, say $\mathbb{S}$, which is at least two dimensional over its left nucleus.

Let $\mathcal{S}$ be a semifield spread and choose homogeneous projective coordinates in $PG(3,q)$ in such a way that the lines

$$\ell_\infty = \{(0,0,c,d)\colon c,d \in \mathbb{F}_q\}$$

and

$$\ell_0 = \{(a,b,0,0)\colon a,b \in \mathbb{F}_q\}$$

belong to $\mathcal{S}$. For each line ℓ of $\mathcal{S}$ different from ℓ_∞ and ℓ_0, there is a unique non-singular 2×2 matrix X over $\mathbb{F}_q$ such that

$$\ell = \ell_X = \{(a,b,c,d) \mid (c,d) = (a,b)X \ : \ a,b \in \mathbb{F}_q\}.$$

In this setting, for any 2×2 non-zero matrix X over $\mathbb{F}_q$, the set

$$\mathcal{R}_X = \{l_{\lambda X} : \lambda \in \mathbb{F}_q\} \cup \{\ell_\infty\}$$

is a regulus containing the lines ℓ_∞ and ℓ_0 and any regulus through ℓ_∞ and ℓ_0 can be written in this way. The set

$$\mathcal{C}_{\mathcal{S}} = \{X \mid \ell_X \in \mathcal{S}\}$$

has the following properties:

(i) $\mathcal{C}_{\mathcal{S}}$ has q^2 elements,

(ii) the zero matrix belongs to $\mathcal{C}_{\mathcal{S}}$,

(iii) $X - Y$ is non-singular for all $X, Y \in \mathcal{C}_{\mathcal{S}}$, $X \neq Y$,

(iv) $\mathcal{C}_{\mathcal{S}}$ is closed under addition.

Such a set $\mathcal{C}_{\mathcal{S}}$ is called the *spread set* (of matrices) associated with $\mathcal{S}$ with respect to ℓ_0 and ℓ_∞ (see e.g. [6]). Conversely, starting from a set $\mathcal{C}$ of 2×2 matrices over $\mathbb{F}_q$ satisfying (i), (ii) and (iii), and closed under addition, the set of lines

$$\mathcal{S} = \{\ell_X\colon X \in \mathcal{C}\} \cup \{\ell_\infty\}$$

is a semifield spread of $PG(3,q)$ and $\mathcal{C}_{\mathcal{S}} = \mathcal{C}$.

Let $\pi(\mathcal{S})$ be the semifield plane defined by the semifield spread $\mathcal{S}$ of $PG(3,q)$, let $\mathcal{C}_{\mathcal{S}}$ be the spread set associated with $\mathcal{S}$ containing ℓ_0 and ℓ_∞, and let $\mathbb{V} = V(4,q)$ denote the vector space of all 2×2 matrices over $\mathbb{F}_q$. Since $\mathcal{C}_{\mathcal{S}}$ is closed under addition and contains the zero matrix, $\mathcal{C}_{\mathcal{S}}$ defines a vector subspace of $\mathbb{V}$ over some subfield of $\mathbb{F}_q$. Denote by K the maximal subfield of $\mathbb{F}_q$ with respect to which $\mathcal{C}_{\mathcal{S}}$ is a K-vector subspace of $\mathbb{V}$, i.e. K is the maximal subfield of $\mathbb{F}_q$ such that $\lambda X \in \mathcal{C}_{\mathcal{S}}$ for any $\lambda \in K$ and for any $X \in \mathcal{C}_{\mathcal{S}}$. If $\pi(\mathcal{S})$ is a non-Desarguesian semifield plane, then K is a proper subfield of $\mathbb{F}_q$ called the *center* of the semifield plane $\pi(\mathcal{S})$; equivalently, K is called the *center* of the semifield spread $\mathcal{S}$. It can be shown that K is isomorphic to the center $\mathcal{K}$ of the semifield $\mathbb{S}$ which coordinates $\pi(\mathcal{S})$.

Starting from a semifield spread $\mathcal{S}$ of a 3-dimensional projective space, another semifield spread, say $\hat{\mathcal{S}}$, can be constructed by applying any correlation of the space. The semifield spread $\hat{\mathcal{S}}$ does not depend, up to isomorphism, on the chosen correlation and it is called the *transpose* of $\mathcal{S}$ (see e.g. [6] and [3]).

Two semifield spreads $\mathcal{S}$ and $\mathcal{S}'$ are isomorphic if and only if the associated translation planes $\pi(\mathcal{S})$ and $\pi(\mathcal{S}')$ are isomorphic; this happens if and only if the associated semifields $\mathbb{S}$ and $\mathbb{S}'$ are *isotopic* (for more details on isotopy see [6]). The center of a semifield spread is invariant under isomorphisms.

In terms of the associated spread sets of matrices, we have that $\mathcal{S}$ and $\mathcal{S}'$ are isomorphic if and only if there exist two matrices $A, B \in GL(2, \mathbb{F}_q)$ and an automorphism $\sigma \in Aut(\mathbb{F}_q)$ such that

$$\mathcal{C}_{\mathcal{S}'} = \{AM^\sigma B\colon M \in \mathcal{C}_{\mathcal{S}}\} \quad ([6]).$$

A very successful tool towards the proof of many of the results contained in this article was looking at the spread set of a semifield spread $\mathcal{S}$ of $PG(3,q)$ as a set of $\mathbb{F}_q$-linear maps of $\mathbb{F}_{q^2}$; denote this set by S. Then, the set S is closed under addition between linear maps and it has the following properties: (i) the zero map belongs to S; (ii) $|S| = q^2$; (iii) any non-zero element of S is a non-singular map. In what follows we will refer to S as a *spread set of linear maps* of $\mathcal{S}$. In these terms we have that the spreads $\mathcal{S}$ and $\mathcal{S}'$ are isomorphic if and only if there exist two bijective $\mathbb{F}_q$-linear maps ϕ and ψ of $\mathbb{F}_{q^2}$ and $\tau \in Aut(\mathbb{F}_{q^2})$ such that

$$S' = \{\phi \circ \varphi^\tau \circ \psi\colon \varphi \in S\},$$

where

$$\varphi^\tau\colon x \in \mathbb{F}_{q^2} \to (a^\tau x + b^\tau x^q) \in \mathbb{F}_{q^2},$$

for

$$\varphi\colon x \in \mathbb{F}_{q^2} \to (ax + bx^q) \in \mathbb{F}_{q^2}$$

and S and S' are spread sets of linear maps of $\mathcal{S}$ and $\mathcal{S}'$ respectively. Also, if S is a spread set of linear maps of $\mathbb{F}_{q^2}$ of a semifield spread $\mathcal{S}$, then

$$\hat{S} = \{\hat{\varphi}\colon \varphi \in S\}$$

where

$$\hat{\varphi}\colon x \in \mathbb{F}_{q^2} \to ax + b^q x^q \in \mathbb{F}_{q^2}$$

for

$$\varphi\colon x \in \mathbb{F}_{q^2} \to ax + bx^q \in \mathbb{F}_{q^2},$$

is a spread set of linear maps of the transpose spread $\hat{\mathcal{S}}$ of $\mathcal{S}$.

Finally, if S is a spread set of linear maps of a semifield spread $\mathcal{S}$ containing the identity map, then the algebraic structure $(\mathbb{F}_{q^2}, +, \circ)$ where $+$ is the sum of the field $\mathbb{F}_{q^2}$ and $\circ$ is defined as

$$x \circ y = \varphi_y(x),$$

with φ_y the unique element of S such that $\varphi_y(1) = y$ is a semifield with identity 1 and left nucleus $\mathbb{F}_q$; this semifield is (up to isotopy) the semifield $\mathbb{S}$ which coordinatizes the plane $\pi(\mathcal{S})$.

3 Cyclic semifield spreads in $PG(3, q^n)$, n odd

In this section we will study cyclic $\mathbb{F}_q$-semifield spreads of $PG(3, q^n)$ ($n > 1$ odd) whose associated semifield $\mathbb{S}$ has middle and right nuclei both isomorphic to $\mathbb{F}_{q^2}$. We start by proving some lemmas which are fundamental to our purpose.

Lemma 1 *Let F_q be the field of scalar 2×2 matrices over $\mathbb{F}_q$, i.e.*

$$F_q = \left\{ \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix} : u \in \mathbb{F}_q \right\}.$$

If F is any field of 2×2 matrices over $\mathbb{F}_{q^n}$ isomorphic to $\mathbb{F}_{q^2}$ and containing F_q, then

$$F = \left\{ \begin{pmatrix} u + At & Bt \\ Ct & u + Dt \end{pmatrix} : u, t \in \mathbb{F}_q \right\},$$

where A, B, C, D are elements of $\mathbb{F}_{q^n}$ such that $A + D, BC - AD \in \mathbb{F}_q$ and the polynomial $X^2 + (A + D)X + AD - BC$ is $\mathbb{F}_q$-irreducible.

Proof Let $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be an element of $F \setminus F_q$. Any element of F has the form

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} \alpha + \beta A & \beta B \\ \beta C & \alpha + \beta D \end{pmatrix},$$

with $\alpha, \beta \in \mathbb{F}_q$. Since the field F is closed under the product, straightforward computations show that

$$A + D \in \mathbb{F}_q \qquad \text{and} \qquad BC - AD \in \mathbb{F}_q^*.$$

Moreover, since F is a field, any matrix of F is non-singular, i.e. the polynomial

$$X^2 + (A + D)X + AD - BC$$

is $\mathbb{F}_q$-irreducible. □

Lemma 2 *Let F be the field of the previous lemma and let $\alpha = \begin{pmatrix} u + At & Bt \\ Ct & u + Dt \end{pmatrix}$, with $u, t \in \mathbb{F}_q$, be any element of F. Then,*

$$\alpha^q = \begin{pmatrix} u + Dt & -Bt \\ -Ct & u + At \end{pmatrix}.$$

Proof Note that since

$$X^2+(A+D)X+AD-BC$$

is $\mathbb{F}_q$-irreducible, then also

$$X^2-(A+D)X+AD-BC$$

is $\mathbb{F}_q$-irreducible. Let λ be one root in $\mathbb{F}_{q^2}$ of

$$X^2-(A+D)X+AD-BC;$$

then $\lambda \in \mathbb{F}_{q^2}\setminus\mathbb{F}_q$ and hence $\{\lambda, 1\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^2}$. Also, the map

$$\psi : \begin{pmatrix} u+At & Bt \\ Ct & u+Dt \end{pmatrix} \in F \mapsto \lambda t + u \in \mathbb{F}_{q^2}$$

is an isomorphism between F and $\mathbb{F}_{q^2}=\mathbb{F}_q(\lambda)$. Hence, since $\lambda^q=(A+D)-\lambda$, if

$$\alpha = \begin{pmatrix} u+At & Bt \\ Ct & u+Dt \end{pmatrix},$$

with $u, t \in \mathbb{F}_q$, then

$$\alpha^q=\psi^{-1}(\lambda^q t+u)=\begin{pmatrix} u'+At' & Bt' \\ Ct' & u'+Dt' \end{pmatrix},$$

where $u'=u+t(A+D)$ and $t'=-t$; the result follows. □

Now, we are able to exhibit the general form of a cyclic $\mathbb{F}_q$-semifield spread of $PG(3,q^n)$, n odd, whose associated semifield has right and middle nuclei both isomorphic to $\mathbb{F}_{q^2}$.

Lemma 3 *Any cyclic semifield spread $\mathcal{S}$ of $PG(3,q^n)$, n odd, whose associated semifield has right and middle nuclei both isomorphic to $\mathbb{F}_{q^2}$ and center isomorphic to $\mathbb{F}_q$ can be described as follows*

$$x=0, \quad y=x(I(\alpha_0+\alpha_1 u+\cdots+\alpha_{\frac{n-1}{2}}u^{\frac{n-1}{2}})+T(\beta_0+\beta_1 u+\cdots+\beta_{\frac{n-3}{2}}u^{\frac{n-3}{2}})) \tag{3.1}$$

where α_i, β_j vary in F, with F a field of 2×2 matrices isomorphic to $\mathbb{F}_{q^2}$ described in Lemma 1, I is the identity matrix,

$$T=\begin{pmatrix} x_0 & \frac{(D-A)x_0-Bx_2}{C} \\ x_2 & -x_0 \end{pmatrix},$$

and $u=x_0^2+\frac{(D-A)x_0x_2-Bx_2^2}{C}$.

Proof If $\mathcal{S}$ is a cyclic semifield spread of $PG(3,q^n)$, whose associated semifield has right and middle nuclei both isomorphic to $\mathbb{F}_{q^2}$ and center isomorphic to $\mathbb{F}_q$, then its spread set with respect to the lines $\ell_\infty = \{(0,0,x_2,x_3)\colon x_2,x_3 \in \mathbb{F}_{q^n}\}$ and $\ell_0 = \{(x_0,x_1,0,0)\colon x_1,x_2 \in \mathbb{F}_{q^n}\}$ consists of the matrices

$$I\alpha_0 + T\beta_0 + T^2\alpha_1 + T^3\beta_1 + \cdots + T^{n-2}\beta_{\frac{n-3}{2}} + T^{n-1}\alpha_{\frac{n-1}{2}}, \tag{3.2}$$

where α_i, β_j vary in a field of matrices F isomorphic to $\mathbb{F}_{q^2}$ and T is a 2×2 matrix over $\mathbb{F}_{q^n}$ such that $\alpha T = T\alpha^q$ for any $\alpha \in F$ and such that T induces a non-linear collineation of $PG(n-1,q^2)$ without fixed proper subspaces (i.e., (T,F) is an *irreducible pair*, see [11]). Hence, the spread set $\mathcal{C}_{\mathcal{S}}$ of $\mathcal{S}$ is a right vector space over the field of matrices F generated by $\{I, T, T^2, \ldots, T^{n-1}\}$. Since $\mathcal{S}$ is a semifield spread with center $\mathbb{F}_q$, we may assume that F contains the field of scalar matrices over $\mathbb{F}_q$ and by Lemma 1 we have

$$F = \left\{ \begin{pmatrix} u + At & Bt \\ Ct & u + Dt \end{pmatrix} : u, t \in \mathbb{F}_q \right\},$$

where

$$A + D, AD - BC \in \mathbb{F}_q$$

and

$$X^2 + (A+D)X + AD - BC$$

is $\mathbb{F}_q$-irreducible. Since n is odd such a polynomial is also $\mathbb{F}_{q^n}$-irreducible and this implies that $BC \neq 0$ and that the field F is contained in the field of matrices (isomorphic to $\mathbb{F}_{q^{2n}}$)

$$\left\{ \begin{pmatrix} u + At & Bt \\ Ct & u + Dt \end{pmatrix} : u, t \in \mathbb{F}_{q^n} \right\}.$$

If $T = \begin{pmatrix} x_0 & x_1 \\ x_2 & x_3 \end{pmatrix}$, with $x_i \in \mathbb{F}_{q^n}$, by $\alpha T = T\alpha^q$ and by Lemma 2 we get

$$\begin{pmatrix} u + At & Bt \\ Ct & u + Dt \end{pmatrix} \begin{pmatrix} x_0 & x_1 \\ x_2 & x_3 \end{pmatrix} = \begin{pmatrix} x_0 & x_1 \\ x_2 & x_3 \end{pmatrix} \begin{pmatrix} u + Dt & -Bt \\ -Ct & u + tA \end{pmatrix}$$

for all u, t in $\mathbb{F}_q$ and this implies the following conditions:

$$x_3 = -x_0, \quad x_1 = \frac{(D-A)x_0 - Bx_2}{C}.$$

Hence,

$$T = \begin{pmatrix} x_0 & \frac{(D-A)x_0 - Bx_2}{C} \\ x_2 & -x_0 \end{pmatrix}.$$

Straightforward computations show that

$$T^{2k-1} = u^{k-1}T \qquad T^{2k} = u^k I$$

for $k=1,\dots,\frac{n-1}{2}$ and with

$$u=x_0^2+\frac{(D-A)x_0x_2-Bx_2^2}{C}.$$

Now the result follows. □

A spread set of the form (3.1) produces a cyclic semifield spread if the pair (T,F) is irreducible. So, by Lemma 3, we may obtain all the cyclic semifield spreads of $PG(3,q^n)$, n odd, whose associated semifield has middle and right nuclei both isomorphic to $\mathbb{F}_{q^2}$ and center isomorphic to $\mathbb{F}_q$, by determining all the irreducible pairs (T,F), where F is a field of 2×2 matrices over $\mathbb{F}_{q^n}$ isomorphic to $\mathbb{F}_{q^2}$ described in Lemma 1 and T is a 2×2 matrix of the type shown in Lemma 3.

In order to do this, it is useful to describe the spread set associated with a cyclic semifield spread in terms of $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$ in such a way that the field of the matrices F corresponds to the field of the scalar maps of $\mathbb{F}_{q^{2n}}$ defined by elements of $\mathbb{F}_{q^2}$, i.e. the maps $x\in\mathbb{F}_{q^{2n}}\mapsto \alpha x\in\mathbb{F}_{q^{2n}}$, with $\alpha\in\mathbb{F}_{q^2}$.

To this aim, let $\mathcal{S}$ be a cyclic semifield spread and let $\mathcal{C}_{\mathcal{S}}$ be the associated spread set as described in Lemma 3. Recall that, since n is odd, the polynomial

$$X^2-(A+D)X+AD-BC$$

is both $\mathbb{F}_q$-irreducible and $\mathbb{F}_{q^n}$-irreducible and in particular $C\neq 0$. Let λ be a root in $\mathbb{F}_{q^{2n}}$ of $X^2-(A+D)X+AD-BC$; then $\lambda\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ and $\mathbb{F}_{q^{2n}}=\mathbb{F}_{q^n}(\lambda)$. Set $\bar{\lambda}=\frac{\lambda}{C}-\frac{D}{C}$ and consider the $\mathbb{F}_{q^n}$-basis $\{\bar{\lambda},1\}$ of $\mathbb{F}_{q^{2n}}$. The 2×2 matrix over $\mathbb{F}_{q^n}$ representing (in the fixed basis and with respect to the left multiplication) the linear map

$$\bar{\alpha}: x\in\mathbb{F}_{q^{2n}}\mapsto \alpha x\in\mathbb{F}_{q^{2n}},$$

with $\alpha\in\mathbb{F}_{q^{2n}}$, is

$$\begin{pmatrix} u+At & Bt\\ Ct & u+Dt\end{pmatrix},$$

where t,u are the components of α in the $\mathbb{F}_{q^n}$-basis $\{\lambda,1\}$. In particular, if $\alpha\in\mathbb{F}_{q^2}$ then $t,u\in\mathbb{F}_q$.

On the other hand the matrix

$$T=\begin{pmatrix} x_0 & \frac{(D-A)x_0-Bx_2}{C}\\ x_2 & -x_0\end{pmatrix}$$

represents, in the fixed basis $\{\overline{\lambda},1\}$, the $\mathbb{F}_{q^n}$-linear map of $\mathbb{F}_{q^{2n}}$

$$\bar{T}: x\in\mathbb{F}_{q^{2n}}\mapsto bx^{q^n}\in\mathbb{F}_{q^{2n}},$$

where $b=x_2\bar{\lambda}-x_0$. It follows that for any $k=1,\dots,\frac{n-1}{2}$ the matrices T^{2k-1} and T^{2k} represent, in the fixed basis $\{\overline{\lambda},1\}$, the $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$

$$\bar{T}^{2k-1}: x\in\mathbb{F}_{q^{2n}}\mapsto bu^{k-1}x^{q^n}\in\mathbb{F}_{q^{2n}}$$

and

$$\bar{T}^{2k} : x \in \mathbb{F}_{q^{2n}} \mapsto u^k x \in \mathbb{F}_{q^{2n}},$$

where $u = b^{q^n+1}$. Then, the $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$ corresponding to the matrices of $\mathcal{C}_{\mathcal{S}}$ in the basis $\{\overline{\lambda}, 1\}$, are

$$id\alpha_0 + \bar{T}\beta_0 + \bar{T}^2\alpha_1 + \bar{T}^3\beta_1 + \cdots + \bar{T}^{n-2}\beta_{\frac{n-3}{2}} + \bar{T}^{n-1}\alpha_{\frac{n-1}{2}},$$

where $\alpha_0, \ldots, \alpha_{\frac{n-1}{2}}, \beta_0, \ldots, \beta_{\frac{n-3}{2}} \in \mathbb{F}_{q^2}$, i.e.

$$\begin{aligned} x \in \mathbb{F}_{q^{2n}} \mapsto & (\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}})x \\ & + b(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})x^{q^n} \in \mathbb{F}_{q^{2n}}, \end{aligned}$$

where $\alpha_i, \beta_j \in \mathbb{F}_{q^2}$. Let S be such a set of $\mathbb{F}_{q^n}$-linear maps. Note that, since $|S| = q^{2n}$, then $\{1, u, \ldots, u^{\frac{n-1}{2}}\}$ is independent over $\mathbb{F}_{q^2}$ and this implies that $\mathbb{F}_{q^{2n}} = \mathbb{F}_{q^2}(u)$, i.e. $\{1, u, \ldots, u^{n-1}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$. Therefore, by the previous arguments and by Lemma 3, we obtain part (1) of the following:

Theorem 1 (1) *Any spread set of $\mathbb{F}_{q^n}$-linear maps of a cyclic semifield spread $\mathcal{S}$ of $PG(3, q^n)$, n odd, whose associated semifield has the right and middle nuclei both isomorphic to $\mathbb{F}_{q^2}$ and the center isomorphic to $\mathbb{F}_q$ may be represented in the following form*:

$$y = (\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}})x + b(\beta_0 + \beta_1 u \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})x^{q^n},$$

where α_i, β_i vary in $\mathbb{F}_{q^2}$, u is a fixed element of $\mathbb{F}_{q^n}$ such that $\{1, u, \ldots, u^{n-1}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ and b is a fixed element of $\mathbb{F}_{q^{2n}}$ such that $b^{q^n+1} = u$.

(2) *Conversely, if u and b are two fixed elements of $\mathbb{F}_{q^n}$ and $\mathbb{F}_{q^{2n}}$ (n odd), respectively, such that $\{1, u, \ldots, u^{n-1}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ and $b^{q^n+1} = u$ then the following*

$$y = (\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}})x + b(\beta_0 + \beta_1 u \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})x^{q^n},$$

(*where α_i, β_i vary in $\mathbb{F}_{q^2}$*) *is a spread set of $\mathbb{F}_{q^n}$-linear maps of a cyclic semifield spread of $PG(3, q^n)$, whose associated semifield has the right and middle nuclei both isomorphic to $\mathbb{F}_{q^2}$ and the center isomorphic to $\mathbb{F}_q$.*

Proof We give the proof of part (2). The set of the $\mathbb{F}_{q^n}$-linear maps

$$S_{u,b} = \{\varphi_{\alpha_0,\ldots,\alpha_{\frac{n-1}{2}},\beta_0,\ldots,\beta_{\frac{n-3}{2}}} : \alpha_i, \beta_j \in \mathbb{F}_{q^2}\},$$

where $\varphi_{\alpha_0,\ldots,\alpha_{\frac{n-1}{2}},\beta_0,\ldots,\beta_{\frac{n-3}{2}}}$ is defined by

$$\begin{aligned} x \in \mathbb{F}_{q^{2n}} \longmapsto &(\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}})x \\ &+ b(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})x^{q^n} \in \mathbb{F}_{q^{2n}}, \end{aligned}$$

contains the zero map, is closed under the sum and $|S_{u,b}| = q^{2n}$. So it defines a spread set of a semifield spread if the non-zero maps of $S_{u,b}$ are non-singular. Suppose that there exist $x \in \mathbb{F}^*_{q^{2n}}$ and $\alpha_i, \beta_j \in \mathbb{F}_{q^2}$ such that

$$(\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}})x + b(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})x^{q^n} = 0.$$

Then

$$b(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})x^{q^n-1} = -\alpha_0 - \alpha_1 u - \cdots - \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}}$$

and hence

$$b^{q^n+1}(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})^{q^n+1} = (\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}})^{q^n+1},$$

i.e.

$$\begin{aligned} &u(\beta_0^q + \beta_1^q u + \cdots + \beta^q_{\frac{n-3}{2}} u^{\frac{n-3}{2}})(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}}) \\ &= (\alpha_0^q + \alpha_1^q u + \cdots + \alpha^q_{\frac{n-1}{2}} u^{\frac{n-1}{2}})(\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}}). \end{aligned}$$

Now, since $\{1, u, \dots, u^{n-1}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ (in particular since n is odd and $u \in \mathbb{F}_{q^n}$, it is also an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$), we get $\alpha_i = \beta_j = 0$ for any $i = 0, \dots, \frac{n-1}{2}$ and for any $j = 0, \dots, \frac{n-3}{2}$. So the non-zero maps of $S_{u,b}$ are all non-singular.

Let

$$T : x \in \mathbb{F}_{q^{2n}} \mapsto bx^{q^n} \in \mathbb{F}_{q^{2n}}$$

and note that $T \in S_{u,b}$. Since

$$T(\alpha x) = \alpha^q b x^{q^n} = \alpha^q T(x)$$

for any $\alpha \in \mathbb{F}_{q^2}$, T induces a strictly semilinear collineation of $PG(n-1, q^2) = PG(\mathbb{F}_{q^{2n}}, \mathbb{F}_{q^2})$. Let U_m be an m-dimensional subspace of $PG(n-1, q^2)$ ($m > -1$) fixed by T of minimum dimension. Then we can write

$$U_m = \langle x, T(x), \dots, T^m(x) \rangle$$

and hence

$$T^{m+1}(x) = \alpha_0 x + \cdots + \alpha_m T^m(x)$$

for some $\alpha_i \in \mathbb{F}_{q^2}$. If $m < n-1$, then the $\mathbb{F}_{q^n}$-linear map

$$\alpha_0 + \alpha_1 T + \cdots + \alpha_m T^m - T^{m+1}$$

of $S_{u,b}$ is singular, a contradiction. So, T induces an irreducible semilinear collineation over $\mathbb{F}_{q^2}$ and since $S_{u,b}$ is the subspace over $\mathbb{F}_{q^2}$ generated by

$$\{id, T, T^2, \dots, T^{n-1}\},$$

we have that $S_{u,b}$ defines a cyclic semifield spread of $PG(3,q^n)$.

Now we compute the nuclei of the semifield $\mathbb{S}_{u,b}$ defined by $S_{u,b}$. It is easy to see that an element y of a semifield $\mathbb{S}$ belongs to N_r (resp. N_m) if and only if $\varphi_y \circ \varphi \in S$ (resp. $\varphi \circ \varphi_y \in S$) for any element φ of S (see e.g. [22, Sec. 4]). From this, we get that $\mathbb{F}_{q^2}$ is contained in the right and middle nuclei of the semifield $\mathbb{S}_{u,b}$. Also if $\varphi : x \mapsto Ax + Bx^{q^n}$ is an element of the right nucleus of $\mathbb{S}_{u,b}$, then $\varphi \circ \varphi_{\alpha_0,\dots,\alpha_{\frac{n-1}{2}},0,\dots,0} \in S_{u,b}$ for any $\alpha_i \in \mathbb{F}_{q^2}$, and this implies $B = 0$. Now, from $\varphi \circ \varphi_{\alpha_0,\dots,\alpha_{\frac{n-1}{2}},0,\dots,0} = A\varphi_{\alpha_0,\dots,\alpha_{\frac{n-1}{2}},0,\dots,0} \in S_{u,b}$ for any $\alpha_i \in \mathbb{F}_{q^2}$, we get $A[1,u,\dots,u^{\frac{n-1}{2}}]_{\mathbb{F}_{q^2}} = [1,u,\dots,u^{\frac{n-1}{2}}]_{\mathbb{F}_{q^2}}$. Hence $A \in \mathbb{F}_{q^2}$, i.e. $N_r = \mathbb{F}_{q^2}$. By using similar arguments we obtain $N_m = \mathbb{F}_{q^2}$; this concludes the proof. □

Corollary 1 *The transpose $\hat{\mathcal{S}}$ of a cyclic semifield spread $\mathcal{S}$ of $PG(3,q^n)$, n odd, whose associated semifield has right and middle nuclei both isomorphic to $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$ is a cyclic semifield spread.*

Proof By the previous theorem part (1) a spread set of linear maps of $\mathcal{S}$ can be represented in the form $S_{u,b}$ where u is a fixed element of $\mathbb{F}_{q^n}$ such that $\{1,u,\dots,u^{n-1}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ and b is a fixed element of $\mathbb{F}_{q^{2n}}$ such that $b^{q^n+1} = u$. So a spread of linear maps of $\hat{\mathcal{S}}$ is $S_{u,b^{q^n}}$ and since $(b^{q^n})^{q^n+1} = b^{q^n+1} = u$, from (2) of Theorem 1 we get the result. □

By Theorem 1, all of the cyclic semifield spreads in $PG(3,q^n)$, n odd, whose associated semifields have middle and right nuclei both isomorphic to $\mathbb{F}_{q^2}$ and center isomorphic to $\mathbb{F}_q$, are obtained by selecting the elements $b \in \mathbb{F}_{q^{2n}}$ such that $\{1,u,\dots,u^{n-1}\}$ is an $\mathbb{F}_q$-basis with $b^{q^{n+1}} = u$, i.e. selecting the elements $b \in \mathbb{F}_{q^{2n}}$ in such a way that b^{q^n+1} does not belong to any proper subfield of $\mathbb{F}_{q^n}$. So far, the only known examples of cyclic semifield spreads have been exhibited by Jha and Johnson (see e.g. [10]) and they are obtained by choosing the element b as a primitive element of $\mathbb{F}_{q^{2n}}$. In the rest of this section, we will denote by $\mathcal{S}_{u,b}$ a cyclic semifield spread defined by the set $S_{u,b}$ of $\mathbb{F}_{q^n}$-linear maps of Theorem 1.

Now we describe some geometric properties of the cyclic semifield spreads $\mathcal{S}_{u,b}$. First we give a technical lemma

Lemma 4 *Let u be an element of $\mathbb{F}_{q^n}$ such that $\{1,u,\dots,u^{n-1}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ (n odd). Let*

$$\gamma(u) = \gamma_0 + \gamma_1 u + \cdots + \gamma_s u^s \text{ with } s \le \frac{n-1}{2}, \gamma_i \in \mathbb{F}_{q^2}$$

and $\gamma_s \neq 0$ *and suppose that the polynomial*

$$\gamma(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_s x^s$$

has no non-constant factors in $\mathbb{F}_q[x]$. *If*

$$\beta(u) = \beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-1}{2}} u^{\frac{n-1}{2}} \neq 0$$

with $\beta_i \in \mathbb{F}_{q^2}$ *and* $\frac{\gamma(u)}{\beta(u)} \in \mathbb{F}_{q^n}$, *then*

$$\beta(u) = t(u)\gamma(u),$$

where $t(u) = t_0 + t_1 u + \cdots + t_c u^c \in \mathbb{F}_{q^n}$, $t_c \neq 0$ *and* $c \leq \frac{n-1}{2} - s$.

Proof Let

$$\beta(x) = \beta_0 + \beta_1 x + \cdots + \beta_{\frac{n-1}{2}} x^{\frac{n-1}{2}} = m(x)\delta(x)$$

where $m(x)$ is the factor of $\beta(x)$ of maximum degree belonging to $\mathbb{F}_q[x]$ and let

$$\delta(x) = \delta_0 + \delta_1 x + \cdots + \delta_l x^l$$

where $l \leq \frac{n-1}{2}$. Since $\frac{\gamma(u)}{\beta(u)} \in \mathbb{F}_{q^n}$, $\beta(u) = m(u)\delta(u)$ and $m(u)^{q^n} = m(u)$, we get

$$\gamma(u)\delta(u)^{q^n} = \delta(u)\gamma(u)^{q^n},$$

i.e.

$$\begin{aligned}(\gamma_0 + \gamma_1 u + \cdots + \gamma_s u^s)&(\delta_0^q + \delta_1^q u + \cdots + \delta_l^q u^l)\\ &= (\gamma_0^q + \gamma_1^q u + \cdots + \gamma_s^q u^s)(\delta_0 + \delta_1 u + \cdots + \delta_l u^l).\end{aligned}$$

Since $s + l \leq n - 1$ and $\{1, u, \ldots, u^{n-1}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ from the above equality we get the following polynomial equality

$$\gamma(x)\hat{\delta}(x) = \hat{\gamma}(x)\delta(x) \tag{3.3}$$

where $\hat{\gamma}(x)$ and $\hat{\delta}(x)$ are the conjugates over $\mathbb{F}_{q^2}$ of $\gamma(x)$ and $\delta(x)$, respectively. Note that if a polynomial $g(x) \in \mathbb{F}_{q^2}[x]$ does not have non-constant factors in $\mathbb{F}_q[x]$ then $g(x)$ and $\hat{g}(x)$ do not have non-constant common factors. Then $\gamma(x)$ (resp. $\delta(x)$) and $\hat{\gamma}(x)$ (resp. $\hat{\delta}(x)$) does not have non-constant factors in common. So by Equality 3.3 we get $\delta(x) = \alpha\gamma(x)$ with $\alpha \in \mathbb{F}_q$. So

$$\beta(x) = \alpha m(x)\gamma(x) = t(x)\gamma(x),$$

where $t(x) \in \mathbb{F}_q[x]$ has degree at most $\frac{n-1}{2} - s$ and hence $\beta(u)$ has the required form. □

Now we can prove the following

Theorem 2 *Let $\mathcal{S}_{u,b}$ be a cyclic semifield spread defined by the spread set of $\mathbb{F}_{q^n}$-linear maps $S_{u,b}$. The following properties hold true.*

a) The Desarguesian spread $\mathcal{D}$ containing the lines ℓ_∞ and ℓ_0 whose spread set of $\mathbb{F}_{q^n}$-linear maps is

$$D = \{x \in \mathbb{F}_{q^{2n}} \mapsto \xi x \in \mathbb{F}_{q^{2n}} : \xi \in \mathbb{F}_{q^{2n}}\}$$

shares $q^{n+1}+1$ lines with the spread $\mathcal{S}_{u,b}$.
The Desarguesian spread $\mathcal{D}'$ containing the lines ℓ_∞ and ℓ_0 whose spread set of $\mathbb{F}_{q^n}$-linear maps is

$$D' = \{x \in \mathbb{F}_{q^{2n}} \mapsto \eta x^{q^n} \in \mathbb{F}_{q^{2n}} : \eta \in \mathbb{F}_{q^{2n}}\}$$

shares $q^{n-1}+1$ lines with the spread $\mathcal{S}_{u,b}$.

b) Any regulus $\mathcal{R}$ (resp. $\mathcal{R}'$) passing through ℓ_∞ and ℓ_0 and contained in $\mathcal{D}$ (resp. $\mathcal{D}'$) shares $q^{s+1}+1$ lines with $\mathcal{S}_{u,b}$, where $-1 \le s \le \frac{n-1}{2}$ (resp. $-1 \le s \le \frac{n-3}{2}$). Moreover, there exist exactly $q+1$ reguli in $\mathcal{D}$ sharing $q^{\frac{n+1}{2}}+1$ lines with $\mathcal{S}_{u,b}$. Each of these $q+1$ reguli is defined by the set of $\mathbb{F}_{q^n}$-linear maps

$$R_\alpha = \{x \in \mathbb{F}_{q^{2n}} \mapsto \lambda\alpha x \in \mathbb{F}_{q^{2n}} : \lambda \in \mathbb{F}_{q^n}\},$$

where $\alpha \in \mathbb{F}^*_{q^2}$.

c) The Desarguesian spread $\mathcal{D}$ is the unique Desarguesian spread containing the line ℓ_∞ and ℓ_0 sharing $q^{n+1}+1$ lines with $\mathcal{S}_{u,b}$.

Proof *a*) Since

$$\begin{aligned} S_{u,b} = \{x \in \mathbb{F}_{q^{2n}} \mapsto {} & (\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}})x \\ & + b(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})x^{q^n} \in \mathbb{F}_{q^{2n}} : \alpha_i \in \mathbb{F}_{q^2}\} \end{aligned}$$

(see proof of Theorem 1 part (2)), it is clear that

$$D \cap S_{u,b} = \{x \in \mathbb{F}_{q^{2n}} \mapsto (\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}})x \in \mathbb{F}_{q^{2n}} : \alpha_i \in \mathbb{F}_{q^2}\},$$

and

$$D' \cap S_{u,b} = \{x \in \mathbb{F}_{q^{2n}} \mapsto b(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})x^{q^n} \in \mathbb{F}_{q^{2n}} : \alpha_i \in \mathbb{F}_{q^2}\}.$$

Hence

$$|D \cap S_{u,b}| = q^{n+1} \text{ and } |D' \cap S_{u,b}| = q^{n-1},$$

i.e.

$$|\mathcal{D} \cap \mathcal{S}_{u,b}| = q^{n+1}+1 \text{ and } |\mathcal{D}' \cap \mathcal{S}_{u,b}| = q^{n-1}+1.$$

b) Note that any regulus passing through ℓ_∞ and ℓ_0 is defined by a set R of $\mathbb{F}_{q^n}$-linear maps of $\mathbb{V}$ (the vector space of all $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$) which is an

1-dimensional $\mathbb{F}_{q^n}$-subspace of $\mathbb{V}$. Let $\mathcal{R}$ be a regulus through ℓ_∞ and ℓ_0, contained in $\mathcal{D}$ and passing through another line of $\mathcal{S}_{u,b}$. Then, the set of the $\mathbb{F}_{q^n}$-linear maps defining the lines of $\mathcal{R} \setminus \{\ell_\infty\}$ is

$$R_{\alpha(u)} = \{x \in \mathbb{F}_{q^{2n}} \mapsto \lambda\alpha(u)x \in \mathbb{F}_{q^{2n}} : \lambda \in \mathbb{F}_{q^n}\}$$

where

$$\alpha(u) = \alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}}$$

with α_i given elements of $\mathbb{F}_{q^2}$ not all zero. Let

$$\alpha(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{\frac{n-1}{2}} x^{\frac{n-1}{2}} \in \mathbb{F}_{q^2}[x]$$

and write

$$\alpha(x) = l(x)\gamma(x)$$

where $l(x)$ is the factor of $\alpha(x)$ belonging to $\mathbb{F}_q[x]$ with maximum degree. Let

$$\gamma(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_s x^s, \text{ with } \gamma_i \in \mathbb{F}_{q^2} \text{ and } \gamma_s \neq 0.$$

It is clear that $R_{\alpha(u)} = R_{\gamma(u)}$. Now, a line of $\mathcal{S}_{u,b} \setminus \{\ell_0\}$ belongs to such a regulus if and only if there exist $\lambda \in \mathbb{F}^*_{q^n}$ and $\beta_0, \beta_1, \ldots, \beta_{\frac{n-1}{2}} \in \mathbb{F}_{q^2}$ (not all zero) such that

$$\lambda\gamma(u) = \beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-1}{2}} u^{\frac{n-1}{2}}$$

i.e., from Lemma 4, if and only if

$$\lambda = t(u) = t_0 + t_1 u + \cdots + t_c u^c,$$

with $t_i \in \mathbb{F}_q$ and $c \leq \frac{n-1}{2} - s$. Hence, if $t = \frac{n-1}{2} - s$, then $|\mathcal{R} \cap \mathcal{S}_{u,b}| = q^{t+1} + 1$. Similar arguments show the results related to the regulus passing through the lines ℓ_∞ and ℓ_0 and contained in $\mathcal{D}'$. Moreover, the reguli of $\mathcal{D}$ through the lines ℓ_∞ and ℓ_0 sharing with $\mathcal{S}_{u,b}$ $q^{\frac{n+1}{2}} + 1$ lines are obtained with $s = 0$, i.e. with $\gamma(x) = \gamma \in \mathbb{F}^*_{q^2}$; precisely they are the reguli defined by the $\mathbb{F}_{q^n}$-linear maps

$$R_\gamma = \{x \in \mathbb{F}_{q^{2n}} \mapsto \lambda\gamma \in \mathbb{F}_{q^{2n}} : \lambda \in \mathbb{F}_{q^n}\}, \text{ where } \gamma \in \mathbb{F}^*_{q^2}.$$

c) Let $\bar{\mathcal{D}}$ be a Desarguesian spread of $PG(3, q^n)$ different from $\mathcal{D}$ containing the lines ℓ_∞ and ℓ_0, sharing $q^{n+1} + 1$ lines with $\mathcal{S}_{u,b}$ and let $\bar{D}$ be the spread set of $\mathbb{F}_{q^n}$-linear maps defining $\bar{\mathcal{D}}$. The spread sets of $\mathbb{F}_{q^n}$-linear maps D and $\bar{D}$ are distinct $\mathbb{F}_{q^n}$-vector subspaces of $\mathbb{V} = V(4, \mathbb{F}_{q^n})$ of dimension 2 and hence $\dim_{\mathbb{F}_{q^n}}(D \cap \bar{D})$ is either 0 or 1. Recalling that $S_{u,b}$ is an $\mathbb{F}_q$-vector subspace of $\mathbb{V} = V(4n, \mathbb{F}_q)$ of dimension $2n$, since

$$|S_{u,b} \cap D| = |S_{u,b} \cap \bar{D}| = q^{n+1},$$

then

$$\dim_{\mathbb{F}_q}(S_{u,b} \cap D) = \dim_{\mathbb{F}_q}(S_{u,b} \cap \bar{D}) = n + 1.$$

If $D \cap \bar{D} = \{\mathbf{0}\}$, then

$$2n = \dim_{\mathbb{F}_q} S_{u,b} \geq \dim_{\mathbb{F}_q} \langle S_{u,b} \cap D, S_{u,b} \cap \bar{D} \rangle = n+1+n+1 = 2n+2,$$

a contradiction. So $\dim_{\mathbb{F}_{q^n}}(D \cap \bar{D}) = 1$. Hence $\mathcal{D}$ and $\bar{\mathcal{D}}$ share a regulus through ℓ_∞ and ℓ_0 defined by the $\mathbb{F}_{q^n}$-linear maps of $D \cap \bar{D}$. Since by $b)$ a regulus through ℓ_∞ and ℓ_0 of $\mathcal{D}$ shares with $\mathcal{S}_{u,b}$ at most $q^{\frac{n+1}{2}} + 1$ lines, then

$$\dim_{\mathbb{F}_q}(S_{u,b} \cap D \cap \bar{D}) \leq \frac{n+1}{2}$$

and this implies

$$\dim_{\mathbb{F}_q}(S_{u,b} \cap \langle D, \bar{D} \rangle) \geq n+1+n+1-\frac{n+1}{2} = \frac{3n+3}{2}.$$

Since $D' \cap D = \{\mathbf{0}\}$, we have $D' \nsubseteq \langle D, \bar{D} \rangle_{\mathbb{F}_{q^n}}$ and hence $\dim_{\mathbb{F}_{q^n}}(D' \cap (\langle D, \bar{D} \rangle)) = 1$, i.e. $D' \cap \langle D, \bar{D} \rangle_{\mathbb{F}_{q^n}}$ defines a regulus of $\mathcal{D}'$ through ℓ_∞ and ℓ_0. Since by $b)$ a regulus of $\mathcal{D}'$ through ℓ_∞ and ℓ_0 shares at most $q^{\frac{n-1}{2}} + 1$ lines with $\mathcal{S}_{u,b}$ we have

$$\dim_{\mathbb{F}_q}(S_{u,b} \cap (D' \cap \langle D, \bar{D} \rangle)) \leq \frac{n-1}{2}.$$

Finally, since $|S_{u,b} \cap D'| = q^{n-1}$, we get

$$\begin{aligned} 2n = \dim_{\mathbb{F}_q} S_{u,b} &\geq \dim_{\mathbb{F}_q} \langle S_{u,b} \cap \langle D, \bar{D} \rangle, S_{u,b} \cap D' \rangle \\ &\geq \frac{3n+3}{2} + n - 1 - \frac{n-1}{2} = 2n+1, \end{aligned}$$

a contradiction. This proves the Theorem. □

4 A generalization

In the previous setting we have the norm $N(b) = N_{q^{2n}/q^n}(b) = b^{q^n+1} = u$. However, the general form of the spread of linear maps can produce other non-cyclic semifields, which may be considered as constructed from cyclic semifields.

Let $S_{u,b}$ be the set consisting of the $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$

$$S_{u,b} = \{\varphi_{\alpha_0,\ldots,\alpha_{\frac{n-1}{2}},\beta_0,\ldots,\beta_{\frac{n-3}{2}}} : \alpha_i, \beta_j \in \mathbb{F}_{q^2}\} \tag{$*$}$$

where

$$\begin{aligned} \varphi_{\alpha_0,\ldots,\alpha_{\frac{n-1}{2}},\beta_0,\ldots,\beta_{\frac{n-3}{2}}} : x \in \mathbb{F}_{q^{2n}} \mapsto &(\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}})x \\ &+ b(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})x^{q^n} \in \mathbb{F}_{q^{2n}} \end{aligned}$$

with $u \in \mathbb{F}_{q^n}^*$, $b \in \mathbb{F}_{q^{2n}}^*$ and $\{1, u, \ldots u^{n-1}\}$ an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ (n odd). So $|S_{u,b}| = q^{2n}$, the zero map belongs to $S_{u,b}$ and $S_{u,b}$ is closed under sum. We have the following

Proposition 1 *The set $S_{u,b}$ is a spread set of $\mathbb{F}_{q^n}$-linear maps if and only if*

$$N(b) \notin P(u) = \left\{ \frac{N(\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}})}{N(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})} : \alpha_i, \beta_j \in \mathbb{F}_{q^2} \right\}. \tag{4.1}$$

In this case the associated semifield $\mathbb{S}_{u,b}$ has $N_l = \mathbb{F}_{q^n}$, $N_r = N_m = \mathbb{F}_{q^2}$ and center $\mathbb{F}_q$.

Proof The set $S_{u,b}$ is a spread set if and only if all the non-zero elements of $S_{u,b}$ are non-singular maps, and this is equivalent to require that

$$N(b)N(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}}) \neq N(\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}}),$$

for all $\alpha_0, \ldots, \alpha_{\frac{n-1}{2}}$ and $\beta_0, \ldots, \beta_{\frac{n-3}{2}} \in \mathbb{F}_{q^2}$ not all zero, i.e. $N(b) \notin P(u)$. In this case, the left nucleus of the associated semifield $\mathbb{S}_{u,b}$ is $\mathbb{F}_{q^n}$ and it is easy to verify that the right and the middle nuclei are both $\mathbb{F}_{q^2}$ and the center is $\mathbb{F}_q$. □

If Condition (4.1) holds true then the semifield $\mathbb{S}_{u,b}$ and the semifield spread $\mathcal{S}_{u,b}$ defined by $S_{u,b}$ are called *semifield* and *semifield spread of type* $(*)$, respectively.

It is useful to observe that a set $S_{u,b}$ of $\mathbb{F}_{q^n}$-linear maps defined as type $(*)$ is not uniquely defined by the pair (u, b). Indeed

Proposition 2 *Let $S_{u,b}$ and $S_{u',b'}$ be two sets of $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$ defined as in $(*)$, then $S_{u,b} = S_{u',b'}$ if and only if $u' = \alpha + \beta u$, $\alpha, \beta \in \mathbb{F}_q$, $\beta \neq 0$ and $b' = \xi b$ with $\xi \in \mathbb{F}^*_{q^2}$.*

Proof We first note that $S_{u,b} = S_{u',b'}$ if and only if the following conditions hold true

$$[1, u, \ldots, u^{\frac{n-1}{2}}]_{\mathbb{F}_{q^2}} = [1, u', \ldots, u'^{\frac{n-1}{2}}]_{\mathbb{F}_{q^2}}; \tag{4.2}$$

$$b[1, u, \ldots, u^{\frac{n-3}{2}}]_{\mathbb{F}_{q^2}} = b'[1, u', \ldots, u'^{\frac{n-3}{2}}]_{\mathbb{F}_{q^2}}. \tag{4.3}$$

The sufficient condition is obvious. Concerning the necessary condition, from (4.2) it follows that $u' \in [1, u, \ldots, u^{\frac{n-1}{2}}]_{\mathbb{F}_{q^2}}$, then there exist $\alpha_0, \alpha_1, \ldots, \alpha_t \in \mathbb{F}_{q^2}$, with $\alpha_t \neq 0$ *and* $1 \leq t \leq \frac{n-1}{2}$, such that $u' = \alpha_0 + \alpha_1 u + \cdots + \alpha_t u^t$. Again from (4.2) since $u'^2 \in [1, u, \ldots, u^{\frac{n-1}{2}}]_{\mathbb{F}_{q^2}}$ and $\{1, u, \ldots, u^{n-1}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$, then $2t \leq (n-1)/2$. After $\frac{n-1}{2}$ steps, taking into account (4.2) we get $t = 1$. Let now

$$u' = \alpha + \beta u, \text{ with } \alpha \in \mathbb{F}_q \text{ and } \beta \in \mathbb{F}^*_q.$$

By (4.3) there exist $\beta_0, \beta_1, \dots, \beta_k \in \mathbb{F}_{q^2}$, with $\beta_k \neq 0$ and $0 \leq k \leq \frac{n-3}{2}$ such that

$$b' = b(\beta_0 + \beta_1 u + \cdots + \beta_k u^k).$$

So

$$b'u' = b(\beta_0 + \beta_1 u + \cdots + \beta_k u^k)(\alpha + \beta u)$$

and again from (4.3) we get $k + 1 \leq (n-3)/2$. After $\frac{n-3}{2}$ steps, (4.3) yields $k = 0$. This concludes the proof. □

Definition 1 *Since $\{1, u, \dots, u^{n-1}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ and $N(b) = b^{q^n+1} \in \mathbb{F}_{q^n}$ then $N(b)$ can be uniquely written in the following manner:*

$$N(b) = L_0 + L_1 u + \cdots + L_{n-1} u^{n-1} \ with\ L_i \in \mathbb{F}_q.$$

If $S_{u,b} = S_{u',b'}$ then, by Proposition 2, $b' = \xi b$ with $\xi \in \mathbb{F}_{q^2}$ and $u' = \alpha + \beta u$, $\alpha, \beta \in \mathbb{F}_q$, $\beta \neq 0$ and hence

$$N(b') = \xi^{q+1} N(b) = \xi^{q+1}(L_0 + L_1 u + \cdots + L_{n-1} u^{n-1})$$
$$= \xi^{q+1}\left(L_0 + L_1\left(\frac{u'-\alpha}{\beta}\right) + \cdots + L_{n-1}\left(\frac{u'-\alpha}{\beta}\right)^{n-1}\right).$$

This means that if t is the maximum integer $(1 \leq t \leq n-1)$ such that

$$N(b) = L_0 + L_1 u + \cdots + L_t u^t,\ with\ L_t \neq 0,$$

then

$$N(b') = L'_0 + L'_1 u' + \cdots + L'_t u'^t,\ with\ L'_t \neq 0.$$

From these arguments the following definition makes sense.
A semifield $\mathbb{S}_{u,b}$ of type $(*)$ has degree t $(1 \leq t \leq n-1)$ if

$$N(b) = L_0 + L_1 u + \cdots + L_t u^t \ with\ L_t \neq 0.$$

Proposition 3 *A semifield $\mathbb{S}_{u,b}$ of type $(*)$ is cyclic if and only if it has degree* 1.

Proof It follows from Theorem 1, Proposition 2 and Definition 1. □

Theorem 3 *The transpose of a semifield spread of type $(*)$ is a semifield spread of type $(*)$ with the same degree.*

Proof The spread set of linear maps of the transpose of $\mathcal{S}_{u,b}$ is $S_{u,b^{q^n}}$. Since $N(b^{q^n}) = N(b)$, the result follows. □

From Theorem 1 we have that the pairs (u, b) with $N(b) = u$ satisfy Condition (4.1). From this, a question naturally arises:

Are there other pairs (u, b) satisfying Condition (4.1)?
Or equivalently:
Do there exist semifields $\mathbb{S}_{u,b}$ of type $(*)$ of degree greater than 1? (Q)
A first answer to this question is the following

Theorem 4 *If*

$$N(b) = A + Bu + Cu^2 \ (A, B, C \in \mathbb{F}_q \text{ and } C \neq 0),$$

then $\mathbb{S}_{u,b}$ is a semifield if and only if the polynomial

$$f(x) = A + Bx + Cx^2 \in \mathbb{F}_q[x]$$

has two distinct roots in $\mathbb{F}_q$.

In order to prove this theorem, we start with the following

Lemma 5 *Let*

$$f(x) = A + Bx + Cx^2 \in \mathbb{F}_q[x]$$

non-constant and let $n \geq 3$. Then, there exist $\alpha_0, \alpha_1, \dots, \alpha_{\frac{n-1}{2}}$ and $\beta_0, \beta_1, \dots, \beta_{\frac{n-3}{2}}$ elements of $\mathbb{F}_{q^2}$ not all zero, such that

$$\begin{aligned}(A + Bx + Cx^2)&(\beta_0 + \beta_1 x \cdots + \beta_{\frac{n-3}{2}} x^{\frac{n-3}{2}})(\beta_0^q + \beta_1^q x \cdots + \beta_{\frac{n-3}{2}}^q x^{\frac{n-3}{2}}) \\ &= (\alpha_0 + \alpha_1 x + \cdots + \alpha_{\frac{n-1}{2}} x^{\frac{n-1}{2}})(\alpha_0^q + \alpha_1^q x + \cdots + \alpha_{\frac{n-1}{2}}^q x^{\frac{n-1}{2}}) \qquad (4.4)\end{aligned}$$

if and only if $f(x)$ has either two coincident roots in $\mathbb{F}_q$ or two conjugate roots in $\mathbb{F}_{q^2}$.

Proof We start by proving the sufficient condition. In our hypotheses, we can write $f(x) = C(x - x_0)(x - x_0^q)$, and hence $B = -C(x_0 + x_0^q)$ and $A = Cx_0^{q+1}$. Now, let $\alpha_1 \in \mathbb{F}_{q^2}$ such that $\alpha_1^{q+1} = C$ and let $\alpha_0 = -x_0\alpha_1$. Then

$$A + Bx + Cx^2 = \alpha_0^{q+1} + (\alpha_0\alpha_1^q + \alpha_0^q\alpha_1)x + \alpha_1^{q+1}x^2 = (\alpha_0 + \alpha_1 x)(\alpha_0^q + \alpha_1^q x)$$

and hence (4.4) occurs.

Now, we prove the necessary condition. Suppose that (4.4) occurs for some $\alpha_i, \beta_i \in \mathbb{F}_{q^2}$ not all zero. By way of contradiction suppose that either $f(x)$ has degree 1 or $f(x)$ has two distinct roots in $\mathbb{F}_q$. Let

$$g(x) = (\beta_0 + \beta_1 x \cdots + \beta_{\frac{n-3}{2}} x^{\frac{n-3}{2}}),\ \hat{g}(x) = (\beta_0^q + \beta_1^q x \cdots + \beta_{\frac{n-3}{2}}^q x^{\frac{n-3}{2}}) \text{ and}$$

$$h(x) = (\alpha_0 + \alpha_1 x + \cdots + \alpha_{\frac{n-1}{2}} x^{\frac{n-1}{2}}),\ \hat{h}(x) = (\alpha_0^q + \alpha_1^q x + \cdots + \alpha_{\frac{n-1}{2}}^q x^{\frac{n-1}{2}}).$$

Equality (4.4) becomes

$$f(x)g(x)\hat{g}(x) = h(x)\hat{h}(x).$$

Note that $g\hat{g}$ and $h\hat{h}$ are elements of $\mathbb{F}_q[x]$ and a root in $\mathbb{F}_q$ of a polynomial of this type always has even algebraic multiplicity. Indeed, if $a \in \mathbb{F}_q$, then $(x-a)^s | h(x)$ if and only if $(x-a)^s | \hat{h}(x)$. Hence, in our hypotheses, if x_0 is a root of $f(x)$ in $\mathbb{F}_q[x]$, then x_0 has odd algebraic multiplicity as a root of $f(x)g(x)\hat{g}(x)$ and, on the other hand, it has even algebraic multiplicity as a root of the polynomial $h(x)\hat{h}(x)$, a contradiction. □

We now give the proof of Theorem 4.

Proof (Theorem 4) By Proposition 1, $\mathbb{S}_{u,b}$ is not a semifield if and only if there exist $\alpha_i, \beta_i \in \mathbb{F}_{q^2}$, not all zero, such that

$$N(b)N(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}}) = N(\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}}),$$

i.e.

$$\begin{aligned}(A + Bu + Cu^2)&(\beta_0 + \beta_1 u + \cdots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})(\beta_0^q + \beta_1^q u + \cdots + \beta^q_{\frac{n-3}{2}} u^{\frac{n-3}{2}})\\ &= (\alpha_0 + \alpha_1 u + \cdots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}})(\alpha_0^q + \alpha_1^q u + \cdots + \alpha^q_{\frac{n-1}{2}} u^{\frac{n-1}{2}}). \qquad (4.5)\end{aligned}$$

Since the exponent of u in the above equality is at most $n-1$ and $\{1, u, \ldots, u^{n-1}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$, by (4.5) we have the following polynomial equality

$$\begin{aligned}(A + Bx + Cx^2)&(\beta_0 + \beta_1 x + \cdots + \beta_{\frac{n-3}{2}} x^{\frac{n-3}{2}})(\beta_0^q + \beta_1^q x + \cdots + \beta^q_{\frac{n-3}{2}} x^{\frac{n-3}{2}})\\ &= (\alpha_0 + \alpha_1 x + \cdots + \alpha_{\frac{n-1}{2}} x^{\frac{n-1}{2}})(\alpha_0^q + \alpha_1^q x + \cdots + \alpha^q_{\frac{n-1}{2}} x^{\frac{n-1}{2}}).\end{aligned}$$

By the previous lemma, this equality can occur if and only if $f(x)$ has either two coincident $\mathbb{F}_q$-roots or two conjugate $\mathbb{F}_{q^2}$-roots. Hence, since $C \neq 0$, we can say that $\mathbb{S}_{u,b}$ is a semifield if and only if the polynomial $A + Bx + Cx^2 \in \mathbb{F}_q[x]$ has two distinct roots in $\mathbb{F}_q$. □

So, if $\mathbb{S}_{u,b}$ is semifield of type $(*)$ of degree 2, from Proposition 3 it follows that $\mathbb{S}_{u,b}$ is never cyclic. However, as we shall see in the next section these semifields of degree 2 are isotopic to cyclic semifields.

Note that if $n = 3$, Theorem 4 gives a complete answer to the question (Q). In the case $n > 3$, it remains to investigate the possibility that $\mathbb{S}_{u,b}$ has degree greater than two and we deal with this problem in Section 6.

5 The question of isomorphisms

We start this section by observing that the geometric properties proved for any cyclic semifield spread (Theorem 2) hold true for any semifield spread of type $(*)$ as well.

We have the following

Lemma 6 *Let $\mathcal{S}_{u,b}$ and $\mathcal{S}_{u',b'}$ be two semifield spreads of type $(*)$. Suppose that $\mathcal{S}_{u,b}$ and $\mathcal{S}_{u',b'}$ are isomorphic, and let ϕ and ψ be the $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$ and τ the automorphism of $\mathbb{F}_{q^{2n}}$ such that*

$$S_{u',b'} = \{\phi \circ \varphi^\tau \circ \psi : \varphi \in S_{u,b}\}.$$

Then either

$$\phi : x \in \mathbb{F}_{q^{2n}} \mapsto Lx \in \mathbb{F}_{q^{2n}} \quad \textit{and} \quad \psi : x \in \mathbb{F}_{q^{2n}} \mapsto Mx \in \mathbb{F}_{q^{2n}}$$

where $LM = \lambda\beta$ with $\lambda \in \mathbb{F}^*_{q^n}$ and $\beta \in \mathbb{F}^*_{q^2}$, or

$$\phi : x \in \mathbb{F}_{q^{2n}} \mapsto L'x^{q^n} \in \mathbb{F}_{q^{2n}} \quad \textit{and} \quad \psi : x \in \mathbb{F}_{q^{2n}} \mapsto M'x^{q^n} \in \mathbb{F}_{q^{2n}},$$

where $L'M'^{q^n} = \lambda\beta$ with $\lambda \in \mathbb{F}^*_{q^n}$ and $\beta \in \mathbb{F}^*_{q^2}$.

Proof Note that by (c) of Theorem 2, the Desarguesian spread $\mathcal{D}$ is the unique Desarguesian spread containing ℓ_∞ and ℓ_0 sharing $q^{n+1}+1$ lines with any semifield of type $(*)$. Moreover from (b) of Theorem 2 the $q+1$ reguli $\mathcal{R}_\alpha$ of $\mathcal{D}$ defined by the sets of $\mathbb{F}_{q^n}$-linear maps $R_\alpha = \{x \in \mathbb{F}_{q^{2n}} \to \lambda\alpha x \in \mathbb{F}_{q^{2n}} : \lambda \in \mathbb{F}_{q^n}\}$, $\alpha \in \mathbb{F}^*_{q^2}$, are the unique reguli of $\mathcal{D}$ sharing $q^{\frac{n+1}{2}}+1$ lines with any semifield of type $(*)$. Hence an isomorphism between $\mathcal{S}_{u,b}$ and $\mathcal{S}_{u',b'}$ must: (i) leave invariant the Desarguesian spread $\mathcal{D}$; (ii) leave invariant the set of the $q+1$ reguli $\{\mathcal{R}_\alpha : \alpha \in \mathbb{F}^*_{q^2}\}$. Let $\phi : x \in \mathbb{F}_{q^{2n}} \mapsto Lx + L'x^{q^n} \in \mathbb{F}_{q^{2n}}$ and $\psi : x \in \mathbb{F}_{q^{2n}} \mapsto Mx + M'x^{q^n} \in \mathbb{F}_{q^{2n}}$. From (i), we have $\phi \circ \varphi^\tau \circ \psi \in D = \{x \in \mathbb{F}_{q^{2n}} \mapsto \eta x \in \mathbb{F}_{q^{2n}} : \eta \in \mathbb{F}_{q^{2n}}\}$ for each $\varphi \in D$. If $\varphi : x \in \mathbb{F}_{q^{2n}} \mapsto \xi x \in \mathbb{F}_{q^{2n}}$, since

$$\phi \circ \varphi^\tau \circ \psi(x) = (L\xi^\tau M + L'\xi^{\tau q^n} M'^{q^n})x + (L\xi^\tau M' + L'\xi^{\tau q^n} M^{q^n})x^{q^n},$$

this implies that $L\xi^\tau M' + L'\xi^{\tau q^n} M^{q^n} = 0$ for any $\xi \in \mathbb{F}_{q^{2n}}$, which is equivalent to $LM' = L'M^{q^n} = 0$, i.e. either $L' = M' = 0$ or $L = M = 0$ (recall that ϕ and ψ are bijective maps). Now, from (ii) we have that for each $\alpha \in \mathbb{F}_{q^2}$, the map $\phi \circ \alpha^\tau \circ \psi$ must belong to $R_\gamma = \{x \in \mathbb{F}_{q^{2n}} \mapsto \lambda\gamma x \in \mathbb{F}_{q^{2n}} : \lambda \in \mathbb{F}_{q^n}\}$ for some $\gamma \in \mathbb{F}^*_{q^2}$. Since $\phi \circ \alpha^\tau \circ \psi(x) = \alpha^\tau LMx$ or $\phi \circ \alpha^\tau \circ \psi(x) = \alpha^{\tau q^n} L'M'^{q^n} x$, we have that either $LM = \lambda\beta$ or $L'M'^{q^n} = \lambda\beta$, with $\lambda \in \mathbb{F}^*_{q^n}$ and $\beta \in \mathbb{F}^*_{q^2}$. □

Remark 1 *From Lemma 6 it follows that if*

$$\phi : x \in \mathbb{F}_{q^{2n}} \mapsto Lx \in \mathbb{F}_{q^{2n}} \quad \textit{and} \quad \psi : x \in \mathbb{F}_{q^{2n}} \mapsto Mx \in \mathbb{F}_{q^{2n}}$$

where $LM = \lambda\beta$ with $\lambda \in \mathbb{F}^*_{q^n}$ and $\beta \in \mathbb{F}^*_{q^2}$, then

$$\begin{aligned} S_{u',b'} = \{x \in \mathbb{F}_{q^{2n}} \mapsto {} & (\alpha_0 + \alpha_1 u^\tau + \cdots + \alpha_{\frac{n-1}{2}} u^{\tau\frac{n-1}{2}})\lambda x \\ & + b^\tau \lambda M^{q^n-1}(\beta_0 + \beta_1 u^\tau + \cdots + \beta_{\frac{n-3}{2}} u^{\tau\frac{n-3}{2}})x^{q^n} \in \mathbb{F}_{q^{2n}} : \alpha_i, \beta_j \in \mathbb{F}_{q^2}\}, \end{aligned} \tag{5.1}$$

whereas if

$$\phi : x \in \mathbb{F}_{q^{2n}} \mapsto L'x^{q^n} \in \mathbb{F}_{q^{2n}} \quad \textit{and} \quad \psi : x \in \mathbb{F}_{q^{2n}} \mapsto M'x^{q^n} \in \mathbb{F}_{q^{2n}},$$

where $L'M'^{q^n} = \lambda\beta'$ *with* $\lambda \in \mathbb{F}^*_{q^n}$ *and* $\beta' \in \mathbb{F}^*_{q^2}$, *then*

$$S_{u',b'} = \{x \in \mathbb{F}_{q^{2n}} \mapsto (\alpha_0 + \alpha_1 u^\tau + \dots \alpha_{\frac{n-1}{2}} u^{\tau\frac{n-1}{2}})\lambda x$$
$$+ b^{\tau q^n}\lambda \frac{1}{M'^{q^n-1}}(\beta_0 + \beta_1 u^\tau + \dots + \beta_{\frac{n-3}{2}} u^{\tau\frac{n-3}{2}})x^{q^n} \in \mathbb{F}_{q^{2n}} : \alpha_i, \beta_j \in \mathbb{F}_{q^2}\}.$$

In the latter case $S_{u',b'}$ *can be obtained also by an isomorphism of the first type with* $M = b^\tau M'^{-1}$.

Hence via isomorphisms of second type we get the same semifield spread sets obtained via isomorphisms of the first type. So we can consider only isomorphisms of the first type, i.e. if $\mathcal{S}_{u',b'}$ is isomorphic to $\mathcal{S}_{u,b}$, then there exist $\lambda \in \mathbb{F}^*_{q^n}$, $M \in \mathbb{F}^*_{q^{2n}}$ and $\tau \in Aut(\mathbb{F}_{q^{2n}})$ such that

$$S_{u',b'} = \{x \in \mathbb{F}_{q^{2n}} \mapsto (\alpha_0 + \alpha_1 u^\tau + \dots + \alpha_{\frac{n-1}{2}} u^{\tau\frac{n-1}{2}})\lambda x$$
$$+ b^\tau \lambda M^{q^n-1}(\beta_0 + \beta_1 u^\tau + \dots + \beta_{\frac{n-3}{2}} u^{\tau\frac{n-3}{2}})x^{q^n} \in \mathbb{F}_{q^{2n}} : \alpha_i, \beta_j \in \mathbb{F}_{q^2}\}.$$

First we consider the case $\tau = 1$.

Theorem 5 *If*

$$S_{u',b'} = \{x \in \mathbb{F}_{q^{2n}} \mapsto (\alpha_0 + \alpha_1 u + \dots + \alpha_{\frac{n-1}{2}} u^{\frac{n-1}{2}})\lambda x$$
$$+ b\lambda M^{q^n-1}(\beta_0 + \beta_1 u + \dots + \beta_{\frac{n-3}{2}} u^{\frac{n-3}{2}})x^{q^n} \in \mathbb{F}_{q^{2n}} : \alpha_i, \beta_j \in \mathbb{F}_{q^2}\}$$

then

$$u' = \frac{\alpha + \beta u}{\gamma + \delta u} \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q, \lambda = \frac{1}{\mu(\gamma + \delta u)^{\frac{n-1}{2}}} \quad \textit{and} \quad b' = \frac{bM^{q^n-1}}{\mu'(\gamma + \delta u)},$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{F}_{q^2}$, $(\gamma, \delta) \neq (0, 0)$, $\mu, \mu' \in \mathbb{F}^*_{q^2}$ *and* $M \in \mathbb{F}^*_{q^{2n}}$.

Proof Since

$$S_{u',b'} = \{x \in \mathbb{F}_{q^{2n}} \mapsto (\alpha_0 + \alpha_1 u' + \dots + \alpha_{\frac{n-1}{2}} u'^{\frac{n-1}{2}})x$$
$$+ b'(\beta_0 + \beta_1 u' + \dots + \beta_{\frac{n-3}{2}} u'^{\frac{n-3}{2}})x^{q^n} \in \mathbb{F}_{q^{2n}} : \alpha_i, \beta_j \in \mathbb{F}_{q^2}\},$$

our hypothesis occurs if and only if

$$[1, u', \dots, u'^{\frac{n-1}{2}}]_{\mathbb{F}_{q^2}} = \lambda[1, u, \dots, u^{\frac{n-1}{2}}]_{\mathbb{F}_{q^2}} \tag{5.2}$$

$$b'[1,u',\dots,u'^{\frac{n-3}{2}}]_{\mathbb{F}_{q^2}} = b\lambda M^{q^n-1}[1,u,\dots,u^{\frac{n-3}{2}}]_{\mathbb{F}_{q^2}}. \tag{5.3}$$

From (5.2) it follows that

$$\lambda = \frac{1}{D(u)}, \text{ where } D(u) = \bar{\alpha}_0 + \cdots + \bar{\alpha}_{\frac{n-1}{2}} u^{\frac{n-1}{2}} \text{ for some } \bar{\alpha}_i \in \mathbb{F}_{q^2}; \tag{5.4}$$

$$u'^i = \lambda E_i(u) = \frac{E_i(u)}{D(u)}, \text{where } E_i(u) = c_0^{(i)} + \cdots + c_{\frac{n-1}{2}}^{(i)} u^{\frac{n-1}{2}} \text{ for some } c_j^{(i)} \in \mathbb{F}_{q^2}. \tag{5.5}$$

From (5.3) it follows that

$$b' = b\lambda M^{q^n-1} A_0(u), \tag{5.6}$$

$$u'^i b' = b\lambda M^{q^n-1} A_i(u), \quad \text{for } i = 1,\dots,\tfrac{n-3}{2}, \tag{5.7}$$

where $A_i(u) = \gamma_0^{(i)} + \cdots + \gamma_{\frac{n-3}{2}}^{(i)} u^{\frac{n-3}{2}}$ for some $\gamma_j^{(i)} \in \mathbb{F}_{q^2}$ and $i = 0,\dots,\frac{n-3}{2}$.

Putting together (5.6) and (5.7) we have

$$u'^i = \frac{A_i(u)}{A_0(u)}, \quad \text{for } i = 1,\dots,\tfrac{n-3}{2}. \tag{5.8}$$

Moreover,

$$u'^i = u'^{i-1}u' = \frac{A_{i-1}(u)}{A_0(u)} \cdot \frac{A_1(u)}{A_0(u)}, \quad \text{for } i = 1,\dots,\tfrac{n-3}{2}$$

and so from (5.8) it follows

$$A_i(u)A_0(u) = A_1(u)A_{i-1}(u), \quad \text{for } i = 1,\dots,\tfrac{n-3}{2}. \tag{5.9}$$

Since the exponent of u in the above equality is at most $n-3$ and $\{1,u,\dots,u^{n-1}\}$ is an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$, by (5.9), we have the following polynomial equalities

$$A_i(x)A_0(x) = A_1(x)A_{i-1}(x), \quad \text{for } i = 1,\dots,\tfrac{n-3}{2}. \tag{5.10}$$

In particular for $i=2$, Equation (5.10) becomes

$$A_1^2(x) = A_0(x)A_2(x).$$

Let $A_1(x) = f_1(x)^{\varepsilon_1} \cdots f_t(x)^{\varepsilon_t}$ be the decomposition of $A_1(x)$ in irreducible factors of $\mathbb{F}_{q^2}[x]$ and let ε_i be the multiplicity of the factor $f_i(x)$.

CASE 1: $A_1(x) \not| A_0(x)$. In this case there exists an irreducible factor $f_i(x)$ such that $f_i^{\varepsilon_i} \not| A_0$ and hence from the above equality $f_i^{\varepsilon_i+1} | A_2$. From (5.10) with $i=3$, we have

$$A_0(x)A_3(x) = A_1(x)A_2(x)$$

and since $f_i^{\varepsilon_i}|A_1(x)$, $f_i^{\varepsilon_i}\not|A_0$, $f_i^{\varepsilon_i+1}|A_2$ then $f_i^{\varepsilon_i+2}|A_3$. After $\frac{n-3}{2}$ steps from (5.10) with $i=\frac{n-3}{2}$,

$$A_0(x)A_{\frac{n-3}{2}}(x)=A_1(x)A_{\frac{n-5}{2}}(x), \tag{5.11}$$

we have

$$f_i^{\varepsilon_i+\frac{n-5}{2}}|A_{\frac{n-3}{2}}$$

and since $\varepsilon_i\geq 1$ and $A_{\frac{n-3}{2}}(x)$ has degree at most $\frac{n-3}{2}$, we get $\varepsilon_i=1$ and f_i has degree 1, i.e.

$$A_{\frac{n-3}{2}}(x)=\xi f_i(x)^{\frac{n-3}{2}},$$

$\xi\in\mathbb{F}_{q^2}^*$.

Again from (5.11), we get

$$A_{\frac{n-5}{2}}(x)=\frac{A_0(x)\xi f_i(x)^{\frac{n-3}{2}}}{f_1(x)^{\varepsilon_1}\cdots f_{i-1}(x)^{\varepsilon_{i-1}}\cdot f_i(x)\cdot f_{i+1}(x)^{\varepsilon_{i+1}}\cdots f_t(x)^{\varepsilon_t}}$$

and hence $A_{\frac{n-5}{2}}(x)=f_i(x)^{\frac{n-5}{2}}\cdot e(x)$, where $e(x)$ is a polynomial of degree at most 1, which is not proportional to $f_i(x)$ and we also get

$$u'=\frac{A_1(u)}{A_0(u)}=\frac{A_{\frac{n-3}{2}}(u)}{A_{\frac{n-5}{2}}(u)}=\frac{d(u)}{e(u)},$$

where $d(u)=\xi f_i(u)$.

From (5.5), for $i=\frac{n-1}{2}$ we get

$$u'^{\frac{n-1}{2}}=\frac{E_{\frac{n-1}{2}}(u)}{D(u)}$$

and hence

$$d(u)^{\frac{n-1}{2}}D(u)=e(u)^{\frac{n-1}{2}}E_{\frac{n-1}{2}}(u).$$

From the above equality it follows the polynomial equality

$$d(x)^{\frac{n-1}{2}}D(x)=e(x)^{\frac{n-1}{2}}E_{\frac{n-1}{2}}(x).$$

Since $d(x)$ and $e(x)$ are not proportional, then $D(x)=\mu e(x)^{\frac{n-1}{2}}$, where $\mu\in\mathbb{F}_{q^2}^*$. Hence $\lambda=\frac{1}{\mu e(u)^{\frac{n-1}{2}}}$.

Since $A_{\frac{n-5}{2}}(x)=f_i(x)^{\frac{n-5}{2}}\cdot e(x)$, from Equalities (5.9) and going backward we get $A_0(u)=\frac{e(u)^{\frac{n-3}{2}}}{\xi^{\frac{n-5}{2}}}$. So from (5.6), we have $b'=\frac{bM^{q^n-1}}{\mu' e(u)}$, where $\mu'=\mu\xi^{\frac{n-5}{2}}$.

CASE 2: $A_1(x)|A_0(x)$**.** In this case $\deg A_1(x) < \deg A_0(x)$, otherwise $u' \in \mathbb{F}_q$, hence $\deg A_1(x) \leq \frac{n-5}{2}$. From (5.10), we get

$$A_{i-1}(x) = A_i(x)\frac{A_0(x)}{A_1(x)}$$

and hence

$$\deg A_{i-1}(x) \geq \deg A_i(x) + 1 \quad \text{for } i = 1, \dots, \tfrac{n-3}{2}. \tag{5.12}$$

From (5.12), with $i = \frac{n-3}{2}$ and $i = \frac{n-5}{2}$ we get

$$\deg A_{\frac{n-5}{2}}(x) \geq \deg A_{\frac{n-3}{2}}(x) + 1,$$

$$\deg A_{\frac{n-7}{2}}(x) \geq \deg A_{\frac{n-5}{2}}(x) + 1 \geq \deg A_{\frac{n-3}{2}}(x) + 2,$$

and after $\frac{n-7}{2}$ steps we get

$$\frac{n-5}{2} \geq \deg A_1(x) \geq \deg A_{\frac{n-3}{2}}(x) + \frac{n-5}{2}.$$

This implies that $A_{\frac{n-3}{2}}(x)$ is a constant polynomial, say $\bar{\beta}$,

$$\deg A_1(x) = \frac{n-5}{2} \quad \text{and} \quad \deg A_0(x) = \frac{n-3}{2}.$$

Let

$$e(x) = \frac{A_0(x)}{A_1(x)}.$$

Using Equalities (5.10), we get

$$A_0(x) = e(x)^{\frac{n-3}{2}}\bar{\beta}.$$

From Equality (5.5) for $i = \frac{n-1}{2}$, arguing as in Case 1, we get

$$\lambda = \frac{1}{\mu e(u)^{\frac{n-1}{2}}},$$

for some $\mu \in \mathbb{F}^*_{q^2}$.
Using (5.6), we get

$$b' = \frac{bM^{q^n-1}}{\mu' e(u)},$$

where $\mu' = \frac{\mu}{\bar{\beta}}$. □

Now we are able to prove

Theorem 6 *The semifield spreads $\mathcal{S}_{u,b}$ and $\mathcal{S}_{u',b'}$ are isomorphic, if and only if*

$$u' = \frac{\alpha + \beta u^\tau}{\gamma + \delta u^\tau} \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q,\ \lambda = \frac{1}{\mu(\gamma + \delta u^\tau)^{\frac{n-1}{2}}}\ \text{ and }\ b' = \frac{b^\tau M^{q^n - 1}}{\mu'(\gamma + \delta u^\tau)},$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{F}_{q^2}$, $(\gamma, \delta) \neq (0,0)$, $\mu, \mu' \in \mathbb{F}^*_{q^2}$, $M \in \mathbb{F}^*_{q^{2n}}$ and $\tau \in Aut(\mathbb{F}_{q^{2n}})$.

In addition if $\mathcal{S}_{u,b}$ and $\mathcal{S}_{u',b'}$ are isotopic and $\mathcal{S}_{u,b}$ is cyclic, then

$$N(b') = A + Bu' + Cu'^2,$$

where either $C = 0$ or the polynomial $A + Bx + Cx^2 \in \mathbb{F}_q[x]$ has two distinct roots in $\mathbb{F}_q$.

Proof If the semifield spreads $\mathcal{S}_{u,b}$ and $\mathcal{S}_{u',b'}$ are isomorphic then there exist $\lambda \in \mathbb{F}^*_{q^n}$, $M \in \mathbb{F}^*_{q^{2n}}$ and $\tau \in Aut(\mathbb{F}_{q^{2n}})$ such that

$$S_{u',b'} = \{x \in \mathbb{F}_{q^{2n}} \mapsto (\alpha_0 + \alpha_1 u^\tau + \cdots + \alpha_{\frac{n-1}{2}} u^{\tau \frac{n-1}{2}})\lambda x$$
$$+ b^\tau \lambda M^{q^n - 1}(\beta_0 + \beta_1 u^\tau + \cdots + \beta_{\frac{n-3}{2}} u^{\tau \frac{n-3}{2}}) x^{q^n} \in \mathbb{F}_{q^{2n}} : \alpha_i, \beta_j \in \mathbb{F}_{q^2}\}.$$

Also, $S_{u',b'}$ and S_{u^τ, b^τ} satisfy the assumptions of Theorem 5, so we get

$$u' = \frac{\alpha + \beta u^\tau}{\gamma + \delta u^\tau} \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q,\ \lambda = \frac{1}{\mu(\gamma + \delta u^\tau)^{\frac{n-1}{2}}}\ \text{ and }\ b' = \frac{b^\tau M^{q^n - 1}}{\mu'(\gamma + \delta u^\tau)},$$

where $\alpha, \beta, \gamma, \delta, \mu, \mu' \in \mathbb{F}_{q^2}$ and $M \in \mathbb{F}^*_{q^{2n}}$.

Now, let $S_{u,b}$ be a spread set of linear maps defining the cyclic semifield spread $\mathcal{S}_{u,b}$ with $N(b) = u$, then from $u' = \frac{\alpha + \beta u^\tau}{\gamma + \delta u^\tau}$ we get $u^\tau = \frac{\alpha - u'\gamma}{\delta u' - \beta}$ and hence

$$b' = b^\tau M^{q^n - 1} \frac{\delta u' - \beta}{\mu'(\delta\alpha - \gamma\beta)}.$$

This implies that

$$N(b') = \frac{(\alpha - u'\gamma)(\delta^q u' - \beta^q)}{(\mu'(\delta\alpha - \gamma\beta))^{q+1}}.$$

Note that since $u' \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$, then α/γ and β^q/δ^q are distinct elements of $\mathbb{F}_q$.

Conversely, suppose that

$$u' = \frac{\alpha + \beta u^\tau}{\gamma + \delta u^\tau},\ \alpha, \beta, \gamma, \delta \in \mathbb{F}_{q^2},\ (\gamma, \delta) \neq (0,0)\ \text{ and }\ b' = \frac{b^\tau M^{q^n - 1}}{\mu'(\gamma + \delta u^\tau)},$$

with $\mu' \in \mathbb{F}^*_{q^2}$, $M \in \mathbb{F}^*_{q^{2n}}$ and $\tau \in Aut(\mathbb{F}_{q^{2n}})$.

Let $S_{u,b}$ and $S_{u',b'}$ be the sets of the $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$ defining $\mathcal{S}_{u,b}$ and $\mathcal{S}_{u',b'}$, respectively. It is sufficient to prove that there exist $\lambda \in \mathbb{F}^*_{q^n}$, $M \in \mathbb{F}^*_{q^{2n}}$ and an automorphism τ of $\mathbb{F}_{q^{2n}}$, such that

$$S_{u',b'} = \{x \in \mathbb{F}_{q^{2n}} \mapsto (\alpha_0 + \alpha_1 u^\tau + \cdots + \alpha_{\frac{n-1}{2}} u^{\tau \frac{n-1}{2}})\lambda x \\ + b^\tau \lambda M^{q^n-1}(\beta_0 + \beta_1 u^\tau + \cdots + \beta_{\frac{n-3}{2}} u^{\tau \frac{n-3}{2}})x^{q^n} \in \mathbb{F}_{q^{2n}} : \alpha_i, \beta_j \in \mathbb{F}_{q^2}\}.$$

We first suppose that

$$u' = \frac{1}{\gamma + \delta u^\tau},$$

with $\gamma, \delta \in \mathbb{F}_{q^2}$ and $\delta \neq 0$; note that since $\gamma + \delta u^\tau$ belong to F_{q^n}, then γ and δ must belong to $\mathbb{F}_q$. Let

$$\lambda = \frac{1}{(\gamma + \delta u^\tau)^{\frac{n-1}{2}}}$$

and observe that for any $i = 1, \ldots, \frac{n-1}{2}$, we get

$$u'^i = \frac{1}{(\gamma + \delta u^\tau)^i} = \frac{1}{(\gamma + \delta u^\tau)^{\frac{n-1}{2}}}(\gamma + \delta u^\tau)^{\frac{n-1}{2}-i}$$

and hence

$$u'^i \in \frac{1}{(\gamma + \delta u^\tau)^{\frac{n-1}{2}}}[1, u^\tau, \ldots, u^{\tau \frac{n-1}{2}}]_{\mathbb{F}_{q^2}}.$$

Moreover, it can be seen that since $1, u, \ldots, u^{\frac{n-1}{2}}$ are independent over $\mathbb{F}_{q^2}$ then $1, u^\tau, \ldots, u^{\tau \frac{n-1}{2}}$ are independent over $\mathbb{F}_{q^2}$ as well. So

$$[1, u', \ldots, u'^{\frac{n-1}{2}}]_{\mathbb{F}_{q^2}} = \lambda[1, u^\tau, \ldots, u^{\tau \frac{n-1}{2}}]_{\mathbb{F}_{q^2}}.$$

Similar arguments show that

$$b'[1, u', \ldots, u'^{\frac{n-3}{2}}]_{\mathbb{F}_{q^2}} = \frac{b^\tau M^{q^n-1}}{(\gamma + \delta u^\tau)^{\frac{n-1}{2}}}[1, u^\tau, \ldots, u^{\tau \frac{n-3}{2}}]_{\mathbb{F}_{q^2}}$$

and so we have the result.

Now, suppose that

$$u' = \frac{\alpha + \beta u^\tau}{\gamma + \delta u^\tau}$$

and let

$$u'' = \frac{1}{\gamma + \delta u^\tau}.$$

For the previous case $\mathcal{S}_{u,b}$ is isomorphic to $\mathcal{S}_{u'',b'}$. Also,

$$u' = \frac{\alpha\delta - \gamma\beta}{\delta} u'' + \frac{\beta}{\delta}.$$

So by Proposition 2 $S_{u',b'} = S_{u'',b'}$ and then $\mathcal{S}_{u,b}$ and $\mathcal{S}_{u',b'}$ are isomorphic. □

We finish this section with the following

Corollary 2 *Let $\mathbb{S}_{u,b}$ be a semifield of type $(*)$ with degree $t > 1$. Then $\mathbb{S}_{u,b}$ is isotopic to a cyclic semifield if and only if $t = 2$.*

Proof The necessary condition follows from Theorem 6. Now, suppose that $\mathbb{S}_{u,b}$ has degree 2. Then by Theorem 4, $N(b) = (\alpha + \beta u)(\gamma + \delta u)$ with $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$ and $\beta\delta \neq 0$. Set $u' = \frac{1}{\gamma+\delta u}$ and $b' = \frac{bM^{q^n-1}}{\mu'(\gamma+\delta u)}$, where $\mu' \in \mathbb{F}^*_{q^2}$ and $M \in \mathbb{F}^*_{q^{2n}}$. Then, again from Theorem 6 it follows that $\mathbb{S}_{u,b}$ and $\mathbb{S}_{u',b'}$ are isotopic and since $N(b') = \frac{\beta+(\alpha\delta-\gamma)u'}{\mu'^{q+1}\delta}$, then $\mathbb{S}_{u',b'}$ is cyclic. □

Corollary 3 *If $\mathcal{S}_{u,b}$ is a semifield spread of type $(*)$, then the transpose $\hat{\mathcal{S}}_{u,b}$ is isomorphic to $\mathcal{S}_{u,b}$.*

Proof By arguments of Section 2, the transpose $\hat{\mathcal{S}}_{u,b}$ of the semifield spread $\mathcal{S}_{u,b}$ of type $(*)$ is defined by the spread set of $\mathbb{F}_{q^n}$-linear maps $S_{u,b^{q^n}}$. Now the result follows from Theorem 6 with $u' = u$, $b' = bb^{q^n-1}$, $\lambda = 1$ and $\tau = 1$. □

6 New semifields of order 4^5 and order 16^5

Let $\mathbb{S}_{u,b}$ be a semifield of type $(*)$. If $n = 3$, then $\mathbb{S}_{u,b}$ has degree 1 or 2 and so it is either a cyclic semifield or isotopic to a cyclic semifield. If $n > 3$ (n odd), then $\mathbb{S}_{u,b}$ could have degree $t \geq 3$. By Corollary 2, such a semifield $\mathbb{S}_{u,b}$ would not be isotopic to a cyclic semifield. So the question is: are there some pairs (u, b) such that $b \notin P(u)$ and $\mathbb{S}_{u,b}$ has degree $t \geq 3$?

Computing results show that if $q = 2$ or $q = 4$ and $n = 5$, there exist semifields $\mathbb{S}_{u,b}$ of type $(*)$ with degree > 2.

Indeed, let ω denote a primitive element of $\mathbb{F}_{2^5}$ with minimal polynomial $x^5 + x^2 + 1 \in \mathbb{F}_2[x]$. By using the software package MAGMA [7] we have

$$\mathbb{F}_{2^5} \setminus P(\omega) = \{\omega, \omega^{18}, \omega^{19}, \omega^{21}\}.$$

The elements ω and ω^{18} produce cyclic semifields, the element ω^{19} produces semifields of degree 2 (hence semifields isotopic to cyclic semifields), whereas ω^{21} produces semifields of degree 4. Indeed,

$$\omega^{21} = \omega^3 + \omega^4.$$

Hence, the semifield $\mathbb{S}_{\omega,b}$, with $b \in \mathbb{F}_{2^{10}}$ such that $N(b) = b^{33} = \omega^{21}$, is of degree 4 and by Corollary 2 is not isotopic to a cyclic semifield.

Let now $q = 4$ and let ω be a primitive element of $\mathbb{F}_{4^5}$ with minimal polynomial $x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$ over $\mathbb{F}_2$. MAGMA computational results show that the elements of $\mathbb{F}_{4^5} \setminus P(\omega^{11})$ which produce semifields $\mathbb{S}_{\omega^{11},b}$ of degree greater than 2 are

$$\omega^{176} = \xi(\omega^{11})^3 + (\omega^{11})^4, \quad \omega^{517} = \xi^2(\omega^{11})^3 + \xi(\omega^{11})^4, \quad \omega^{858} = (\omega^{11})^3 + \xi^2(\omega^{11})^4,$$

where $\xi = \omega^{341} \in \mathbb{F}_4$. Hence, the semifields $\mathbb{S}_{\omega^{11},b}$, with $b \in \mathbb{F}_{2^{10}}$ such that

$$N(b) = b^{1025} \in \{\omega^{176}, \omega^{517}, \omega^{858}\}$$

are of degree 4 and by Corollary 2 they are not isotopic to cyclic semifields. So we have

Theorem 7 *For $q = 2$ and $n = 5$, $q = 4$ and $n = 5$ there exist semifields of type* $(*)$ *not isotopic to cyclic semifields.*

From a given semifield $\mathbb{S}$, by the so called Knuth operations (transpose and dual), it is possible to construct six semifields, one of which is the original. We will call these six semifields *derivatives* of $\mathbb{S}$. The group S_3 permutes the nuclei (up to isomorphisms) of the six derivatives [18, Sec. 6].

In what follows we will prove that our examples are not isotopic to any derivative of a known semifield.

Theorem 8 *The semifields of order* 4^5 *and the semifields of order* 16^5 *exhibited above are new.*

Proof The examples exhibited above have left nucleus $\mathbb{F}_{q^5}$, right and middle nuclei $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$ ($q \in \{2, 4\}$) (see Proposition 1). A symplectic semifield has right and middle nuclei both isomorphic to the center [15, 18], while a semifield isotopic to a commutative semifield has left and right nuclei both isomorphic to the center. Hence, our examples are isotopic neither to a derivative of a symplectic semifield nor to a derivative of a commutative semifield. These arguments and the even characteristic allow us to say that our examples are not isotopic to a generalized Dickson semifield, to any semifield of type B, F, C listed in Section 10 and to any of their derivatives.

Since a Knuth semifield of type (17), (18) or (19) (see [8, pag. 241]) is 2-dimensional over at least two of its nuclei and since a Knuth semifield of type (20) (see [8, pag. 242]) has the three nuclei equal to the center, then our examples are not isotopic to any derivative of such semifields.

Moreover, a Sandler semifield has order q^{m^2}, left nucleus and center of order q (see [8, pag. 243] and [22, Thm. 1]); hence, again by comparing the nuclei, one can see that our semifields are not isotopic to any derivative of a Sandler semifield.

Also, the multiplication of a Generalized Twisted Field of order q depends on two automorphisms of $\mathbb{F}_q$, say S and T with $S \neq I$, $T \neq I$ and $S \neq T$ and $|N_l| = |Fix\ T|$, $|N_r| = |Fix\ S|$ and $|N_m| = |Fix\ ST^{-1}|$ (see [1, Lemma 1]). If a derivative of such a semifield was isotopic to one of our examples then it would have order s^{2n} (n odd), two of its nuclei both of order s^2 and the other one of order s^n; and this is not possible.

Finally, since the transpose is the unique Knuth operation leaving invariant the dimension over the left nucleus and interchanging the dimensions over the other nuclei and since the transpose of a cyclic semifield is a cyclic semifield as well (see Corollary 1), our examples cannot be the derivatives of a cyclic semifield. So, by these arguments and by Theorem 7, we have the assert. □

Moreover, computations using the program Magma show that

Theorem 9 *For* $(q,n)\in\{(3,5),(2,7),(2,9)\}$ *semifields* $\mathbb{S}_{u,b}$ *of type* $(*)$ *of degree* $t>2$ *do not exist.*

7 The number of non-isomorphic semifield spreads $\mathcal{S}_{u,b}$ with degree ≤ 2

Let $\mathcal{S}_{u,b}$ be a cyclic semifield spread, then a semifield spread $\mathcal{S}_{u',b'}$ is isomorphic to $\mathcal{S}_{u,b}$ if and only if

$$u'=\frac{\alpha+\beta u^{\tau}}{\gamma+\delta u^{\tau}}\quad\text{and}\quad b'=\frac{b^{\tau}M^{q^n-1}}{\mu'(\gamma+\delta u^{\tau})},$$

where $\alpha,\beta,\gamma,\delta\in\mathbb{F}_{q^2}$, $(\gamma,\delta)\neq(0,0)$, $\mu,\mu'\in\mathbb{F}^*_{q^2}$ and $M\in\mathbb{F}^*_{q^{2n}}$.

Among these the cyclic ones are obtained with $u\prime=u^{\tau}$ or $u'=\frac{1}{u^{\tau}}$ with $\tau\in Aut(\mathbb{F}_{q^{2n}})$ and $b'=\frac{b^{\tau}M^{q^n-1}}{\mu'}$ or $b'=\frac{b^{\tau}M^{q^n-1}}{\mu'u^{\tau}}$. Note that since $u\in\mathbb{F}_{q^n}$, then the order of the orbit of u under the action of $Aut(\mathbb{F}_{q^{2n}})$ is at most nh, where $q=p^h$. Recalling that $\mathbb{S}_{u,b}=\mathbb{S}_{u,\xi b}$, with $\xi\in\mathbb{F}^*_{q^2}$ and that the number of b's with the same norm over $\mathbb{F}_{q^n}$, non-proportional in $\mathbb{F}_{q^2}$ is $\frac{q^n+1}{q+1}$, we have that the number of cyclic semifield spreads isomorphic to $\mathcal{S}_{u,b}$ is at most $2nh\frac{q^n+1}{q+1}$. By Corollary 2 any semifield spread $\mathcal{S}_{u,b}$ of type $(*)$ with degree ≤ 2 is isomorphic to a cyclic one. So the number of non-isomorphic semifield spreads of type $(*)$ with degree ≤ 2 coincides with the number of non-isomorphic cyclic semifield spreads.

Since $\{1,u,\dots,u^{n-1}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ if and only if u does not belong to any proper subfield of $\mathbb{F}_{q^n}$ and since two cyclic semifield spreads $\mathcal{S}_{u,b}$ and $\mathcal{S}_{u',b'}$ are the same if and only if $u'=\alpha+\beta u$, $\beta\neq 0$ (see Proposition 2), the number of distinct cyclic semifield spreads $\mathcal{S}_{u,b}$ is $\frac{q^n-\theta}{q(q-1)}\cdot\frac{q^n+1}{q+1}$ where θ is the size of the union of the proper subfields of $\mathbb{F}_{q^n}$. In this way we have proved the following

Theorem 10 *The number of non-isomorphic semifield spreads of type* $(*)$ *with degree at most* 2 *is at least*

$$\frac{q^n-\theta}{q(q-1)2nh}.$$

In particular if n is a prime, then $\theta=q$ *and this lower bound is*

$$\frac{q^{n-1}-1}{2(q-1)nh}.$$

8 Net replacement interpretation

We have given a variety of constructions of semifields with spread sets of the following general form:

$$x=0, y=(\alpha_0+\alpha_1u+\cdots+\alpha_{\frac{n-1}{2}}u^{\frac{n-1}{2}})x+b(\beta_0+\beta_1u\cdots+\beta_{\frac{n-3}{2}}u^{\frac{n-3}{2}})x^{q^n},$$
$$\alpha_i,\beta_j\in\mathbb{F}_{q^2}, i,j=0,1,\dots,n-1,$$

where b is a fixed element of $\mathbb{F}_{q^{2n}}$. Consider the partial spread where $\beta_j=0$ for all $j=0,1,2,\dots,\frac{n-3}{2}$. Let $\mathcal{D}$ denote that Desarguesian spread of order q^{2n} given by

$$\left\{x=0, y=xm; m\in\mathbb{F}_{q^{2n}}\right\}.$$

By Theorem 2, any semifield spread $\mathcal{S}_{u,b}$ of type $(*)$ has a Desarguesian partial spread in common with $\mathcal{D}$; i.e.

$$x=0, y=(\alpha_0+\alpha_1u+\cdots+\alpha_{\frac{n-1}{2}}u^{\frac{n-1}{2}})x; \alpha_i\in\mathbb{F}_{q^2}; i=0,1,\dots,\frac{n-1}{2}.$$

Furthermore, we note that any other component of the semifield spread corresponds to a Baer subplane of the Desarguesian affine plane defined by $\mathcal{D}$. Write

$$\begin{aligned}\mathbb{F}_{q^{2n}}&=\left\langle\alpha_0+\alpha_1u+\cdots+\alpha_{\frac{n-1}{2}}u^{\frac{n-1}{2}}\right\rangle\oplus\left\langle\beta_0u^{\frac{n+1}{2}}+\beta_1u^{\frac{n+3}{2}}\cdots+\beta_{\frac{n-3}{2}}u^{n-1}\right\rangle\\&=V_\alpha\oplus V_\beta.\end{aligned}$$

Hence, we have a replacement net of degree $q^{2n}-q^{n+1}$ of the net

$$\left\{y=xm; m\in V_\alpha\oplus V_\beta-V_\alpha\right\}$$

in the Desarguesian plane defined by $\mathcal{D}$.

Hence, we obtain:

Theorem 11 *The semifields of order q^{2n} constructed here may be constructed from a Desarguesian affine plane of order q^{2n} by the net replacement of a net of degree $q^{2n}-q^{n+1}$.*

9 More semifield spreads by algebraic lifting

We note that the construction process of 'algebraic lifting' produces from any spread in $PG(3,h)$ a corresponding spread in $PG(3,h^2)$. Furthermore, the process constructs a semifield spread from any additive spread set. Hence, we obtain new classes of semifields of order q^{4n}, for n odd with spreads in $PG(3,q^{2n})$ from any of the constructed cyclic or non-cyclic semifields of order q^{2n}, since the spreads constructed above are all in $PG(3,q^n)$.

Note that the non-cyclic semifields planes are isomorphic to cyclic semifield planes but algebraic lifting is an algebraic process. Hence, non-cyclic semifield planes and cyclic semifield planes probably do not lift to isomorphic semifield planes.

10 The known finite semifields

In Jha and Johnson [11], there are a variety of constructions of cyclic semifield planes. One construction is relevant in the work presented here. Let $\ell = \mathrm{lcm}(m,n)$, $m,n > 1$ be integers, and $\ell > 1$. Consider the mapping T :

$$T : x \to \omega x^{q^n},$$

where ω is a primitive element of $\mathbb{F}_{q^\ell}$. Then (see Theorem 2 [11]), Jha and Johnson show that there is an associated cyclic semifield plane, called the 'Jha-Johnson cyclic semifield (q,m,n)'. Here the middle and right nuclei contain $\mathbb{F}_{q^m}$ and the left nucleus (kernel) is $\mathbb{F}_{q^n}$ (actually this is the dual semifield to the semifield constructed by Jha and Johnson). When $m = 2$ and n is odd, we obtain a cyclic semifield of order q^{2n} with kernel $\mathbb{F}_{q^n}$ and middle and right nuclei $\mathbb{F}_{q^2}$. Hence, some of the semifields constructed in this article are Jha-Johnson cyclic semifields. The constructions here require a basis $\{1, u, u^2, \dots, u^{n-1}\}$ for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and an element b such that $b^{q^n+1} = u$, so any element u in $\mathbb{F}_{q^n}$ not belonging to any proper subfield of $\mathbb{F}_{q^n}$, will suffice. Here we also give a generalization of such a family (see Section 4) obtaining new examples for $q = 2$ and $n = 5$, $q = 4$ and $n = 5$.

To better view the place of the present class within the known classes, we list here the known examples. This information comes from the text "A Handbook of Finite Translation Planes," of M. Biliotti, V. Jha, and N.L. Johnson, which had been published by Taylor Books in January of 2007.

The known finite semifields and general construction processes are as follows: (the classes are not necessarily disjoint, see C and D).

Known Semifields:

B: Knuth binary semifields

F: Flock semifields and their 5th cousins:

F_1: Kantor–Knuth

F_2: Cohen–Ganley, 5th cousin: Payne–Thas.

F_3: Penttila–Williams symplectic semifield order 3^5, 5th cousin, Bader, Lunardon, Pinneri flock semifield

C: Commutative semifields/symplectic semifields.

C_1: Kantor–Williams Desarguesian Scions (symplectic), Kantor–Williams commutative semifields

C_2: Ganley commutative semifields and symplectic cousins

C_3: Coulter–Matthews commutative semifields and symplectic cousins

D: Generalized Dickson/Knuth/Hughes–Kleinfeld semifields

S: Sandler semifields

JJ: Jha–Johnson cyclic semifields (generalizes Sandler, also of type $S(\omega,m,n)$, or p-primitive type 1, or q-primitive type 2)

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

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

T: Generalized twisted fields
JH: Johnson–Huang 8 semifields of order 8^2
CF: Cordero–Figueroa semifield of order 3^6
General Construction Processes:
L: Algebraically lifted semifields

The algebraically lifted Desarguesian spreads are completely determined. These are also known as Cordero–Figueroa/Boerner–Lantz semifield planes for q odd or the Cardinali, Polverino, Trombetti semifield planes for q even

M: The middle-nucleus semifields by distortion-derivation
C: $GL(2,q)-q^3$ plane construction of Jha–Johnson.

Finally, we recall that there are two other constructions producing semifields starting from a given one. Both these constructions can be applied if the starting semifield is 2-dimensional over its left nucleus (see [17, Sec. 10] and [4, Sec. 6]). Recently, in [19], it has been proven that, up to a Knuth operation, these two constructions are equivalent.

References

1. Albert, A.A.: Isotopy for generalized twisted fields. An. Acad. Bras. C. **33**, 265–275 (1961)
2. Ball, S., Bamberg, J., Lavrauw, M., Penttila, T.: Symplectic spreads. Designs Codes Cryptogr. **32**(1–3), 9–14 (2004)
3. Ball, S., Brown, M.R.: The six semifield planes associated with a semifield flock. Adv. Math. **189**(1), 68–87 (2004)
4. Ball, S., Ebert, G.L., Lavrauw, M.: A geometric construction of finite semifields. J. Algebra **311**, 117–129 (2007)
5. Biliotti, M., Jha, V., Johnson, N.L.: The collineation groups of generalized twisted field planes. Geom. Dedic. **76**(1), 97–126 (1999)
6. Biliotti, M., Jha, V., Johnson, N.L.: Foundations of Translation Planes. Monographs and Textbooks in Pure and Applied Mathematics, vol. 243. Dekker, New York (2001)
7. Cannon, J., Playoust, C.: An Introduction to MAGMA. University of Sydney Press, Sydney (1993)
8. Dembowski, P.: Finite Geometries. Springer, Berlin (1968)
9. Ganley, M.J., Jha, V., Johnson, N.L.: The translation planes admitting a nonsolvable doubly transitive line-sized orbit. J. Geom. **69**(1–2), 88–109 (2000)
10. Jha, V., Johnson, N.L.: On the nuclei of semifields and Cofman's many-subplane problem. Abh. Math. Semin. Univ. Hamb. **57**, 127–137 (1987)
11. Jha, V., Johnson, N.L.: 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**(1), 1–35 (1989)
12. Jha, V., Johnson, N.L.: A geometric characterization of generalized Desarguesian planes. Atti Semin. Mat. Fis. Univ. Modena **38**(1), 71–80 (1990)
13. Jha, V., Johnson, N.L.: Translation planes of large dimension admitting nonsolvable groups. J. Geom. **45**(1–2), 87–104 (1992)
14. Johnson, N.L., Marino, G., Polverino, O., Trombetti, R.: Semifields of order q^6 with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$. Finite Fields Appl. (to appear) (available online 8 May 2007)
15. Johnson, N.L., Vega, O.: Symplectic spreads and symplectically paired spreads. Note Mat. **26**, 105–111 (2006)
16. Kantor, W.M.: Commutative semifields and symplectic spreads. J. Algebra **270**(1), 96–114 (2003)
17. Lunardon, G.: Translation ovoids. J. Geom. **76**, 200–215 (2003)
18. Lunardon, G.: Symplectic spreads and finite semifields. Des. Codes Cryptogr. **44**(1–3), 39–48 (2007)

19. Lunardon, G., Marino, G., Polverino, O., Trombetti, R.: Translation dual of a semifield. J. Comb. Theory Ser. A (to appear)
20. Marino, G., Polverino, O., Trombetti, R.: On $\mathbb{F}_q$-linear sets of $PG(3, q^3)$ and semifields. J. Comb. Theory, Ser. A **114**, 769–788 (2007)
21. Sandler, R.: A note on some new finite division ring planes. Trans. Am. Math. Soc. **104**, 528–531 (1962)
22. Sandler, R.: Autotopism groups of some finite non-associative algebras. Am. J. Math. **84**, 239–264 (1962)