Discrete Mathematics 310 (2010) 3108–3113

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

A new semifield of order 2^{10}

Giuseppe Marino [a,*], Rocco Trombetti [b]

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

[b] Università degli Studi di Napoli "Federico II", Dipartimento di Matematica e Applicazioni, I–80126 Napoli, Italy

ARTICLE INFO

Article history:
Received 25 September 2008
Received in revised form 27 April 2009
Accepted 12 May 2009
Available online 6 June 2009

Keywords:
Semifield
Linearized polynomial
Linear set

ABSTRACT

In [G. Lunardon, Semifields and linear sets of $PG(1, q^t)$, Quad. Mat., Dept. Math., Seconda Univ. Napoli, Caserta (in press)], G. Lunardon has exhibited a construction method yielding a theoretical family of semifields of order q^{2n}, $n > 1$ and n odd, with left nucleus $\mathbb{F}_{q^n}$, middle and right nuclei both $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$. When $n = 3$ this method gives an alternative construction of a family of semifields described in [N.L. Johnson, G. Marino, O. Polverino, R. Trombetti, On a generalization of cyclic semifields, J. Algebraic Combin. 26 (2009), 1–34], which generalizes the family of cyclic semifields obtained by Jha and Johnson in [V. Jha, N.L. Johnson, Translation planes of large dimension admitting non-solvable groups, J. Geom. 45 (1992), 87–104]. For $n > 3$, no example of a semifield belonging to this family is known.

In this paper we first prove that, when $n > 3$, any semifield belonging to the family introduced in the second work cited above is not isotopic to any semifield of the family constructed in the former. Then we construct, with the aid of a computer, a semifield of order 2^{10} belonging to the family introduced by Lunardon, which turns out to be non-isotopic to any other known semifield.

1. Introduction

A *finite semifield* $\mathbb{S}$ is a finite algebraic structure satisfying all the axioms for a skewfield except (possibly) associativity. The subsets $\mathbb{N}_l = \{a \in \mathbb{S} \mid (ab)c = a(bc),\ \forall b, c \in \mathbb{S}\}$, $\mathbb{N}_m = \{b \in \mathbb{S} \mid (ab)c = a(bc),\ \forall a, c \in \mathbb{S}\}$, $\mathbb{N}_r = \{c \in \mathbb{S} \mid (ab)c = a(bc),\ \forall a, b \in \mathbb{S}\}$ and $\mathcal{K} = \{a \in \mathbb{N}_l \cap \mathbb{N}_m \cap \mathbb{N}_r \mid ab = ba,\ \forall b \in \mathbb{S}\}$ are fields and are known, respectively, as the *left nucleus*, the *middle nucleus*, the *right nucleus* and the *center* of $\mathbb{S}$. A finite semifield is a vector space over each of its nuclei and its center (for more details on semifields see e.g. [5,10]). If $\mathbb{S}$ satisfies all the axioms of a semifield except possibly the existence of the identity element for the multiplication, then $\mathbb{S}$ is called *pre-semifield*. Throughout this paper, we will assume the center of our semifields to be the Galois Field $\mathbb{F}_q$, where $q = p^h$, and the term (pre-)semifield will be always used to denote a finite (pre-)semifield.

Two pre-semifields, say $\mathbb{S} = (\mathbb{S}, +, \circ)$ and $\mathbb{S}' = (\mathbb{S}', +, \circ')$, are said to be *isotopic* if there exist three $\mathbb{F}_p$-linear maps g_1, g_2 and g_3 from $\mathbb{S}$ to $\mathbb{S}'$ such that

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

for all $x, y \in \mathbb{S}$.

From any pre-semifield, one can naturally construct a semifield which is isotopic to it.

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

* Corresponding author.
E-mail addresses: giuseppe.marino@unina2.it (G. Marino), rtrombet@unina.it (R. Trombetti).

0012-365X/$ – see front matter
doi:10.1016/j.disc.2009.05.013

Let b be an element of a semifield $\mathbb{S}$ with center $\mathbb{F}_q$. Then the map $\varphi_b: x \in \mathbb{S} \to xb \in \mathbb{S}$ is an $\mathbb{N}_l$-linear map, when $\mathbb{S}$ is regarded as left vector space over $\mathbb{N}_l$. The set $S = \{\varphi_b: b \in \mathbb{S}\}$ is called the *spread set of linear maps* of $\mathbb{S}$ and it satisfies the following properties: (i) $|S| = |\mathbb{S}|$, (ii) S is closed under addition and contains the zero map, (iii) any non-zero map of S is non-singular, i.e. it is invertible. Moreover, $\lambda\varphi_b = \varphi_{\lambda b}$ for any $\lambda \in \mathbb{F}_q$, i.e. S is an $\mathbb{F}_q$-vector subspace of the vector space $\mathbb{V}$ of all $\mathbb{N}_l$-linear maps of $\mathbb{S}$. If $\dim_{\mathbb{N}_l}\mathbb{S} = 2$, then $\mathbb{V}$ is a 4-dimensional vector space over $\mathbb{N}_l$ and S is an $\mathbb{F}_q$-vector subspace of $\mathbb{V}$ of dimension $2n$, where $n = [\mathbb{N}_l : \mathbb{F}_q]$. Then $\mathbb{N}_l \simeq \mathbb{F}_{q^n}$ and S defines in $\mathbb{P} = PG(\mathbb{V}, \mathbb{F}_{q^n}) = PG(3, q^n)$ an $\mathbb{F}_q$-*linear set* of rank $2n$, namely $L(\mathbb{S}) = L_S = \{\langle\varphi_b\rangle_{\mathbb{F}_{q^n}} : \varphi_b \in S \setminus \{0\}\}$. Since the linear maps defining $L(\mathbb{S})$ are invertible, the linear set $L(\mathbb{S})$ is disjoint from the hyperbolic quadric $\mathcal{Q} = Q^+(3, q^n)$ of $\mathbb{P}$ defined by the non-invertible maps of $\mathbb{V}$. Also, $\mathbb{S}$ is isotopic to a field if and only if $L(\mathbb{S})$ is a line of $\mathbb{P}$ external to the quadric $\mathcal{Q}$. These linear sets have been introduced by G. Lunardon in [15], associated with translation ovoids of $Q^+(5, q)$, and they have been studied in [4] (in terms of spread sets of matrices) associated with semifield spreads of $PG(3, q)$. Also in [4], the authors proved that if two semifields $\mathbb{S}_1$ and $\mathbb{S}_2$, 2-dimensional over their left nucleus and with center $\mathbb{F}_q$, are isotopic then the associated $\mathbb{F}_q$-linear sets of $\mathbb{P} = PG(3, q^n)$ are isomorphic with respect to the subgroup G of $P\Gamma O^+(4, q^n)$ fixing the reguli of the hyperbolic quadric $\mathcal{Q}$ of $\mathbb{P}$.

In [12], the authors introduced a family of semifields of order q^{2n}, $n > 1$ and n odd, with left nucleus $\mathbb{F}_{q^n}$, right and middle nuclei both $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$. Also in [12], for $n = 5$ and $q = 2$ and for $n = 5$ and $q = 4$, examples of such semifields were constructed, which are not isotopic to any other previously known semifield. Moreover in [13], G. Lunardon constructed a theoretical family of semifields of order q^{2n} having the same parameters as the ones belonging to the family appearing in [12]. When $n = 3$ these two families coincide and in this case all of the ensuing semifields are either cyclic or isotopic to cyclic semifields with the same nuclei (see [11, Thm. 2.9]). When $n > 3$, it is not known if the two families produce isotopic semifields.

In this paper we first prove that, when $n > 3$, no semifield belonging to the family introduced in [12] is isotopic to a semifield exhibited in [13]. Moreover we construct a semifield of order 2^{10} with left nucleus $\mathbb{F}_{2^5}$, right and middle nuclei both $\mathbb{F}_{2^2}$ and center $\mathbb{F}_2$, which provides an example belonging to the putative class constructed by Lunardon and which turns out to be non-isotopic to any other known semifield.

2. Spread sets of linear maps and linear sets of $PG(1, q^{2n})$

Let $\Omega = PG(s-1, q^t) = PG(V, \mathbb{F}_{q^t})$, $q = p^h$, p prime, and let L be a set of points of Ω. The set L is said to be an $\mathbb{F}_q$-*linear* set of Ω if it is defined by the non-zero vectors of an $\mathbb{F}_q$-vector subspace U of V, i.e.,

$$L = L_U = \{\langle\mathbf{u}\rangle_{\mathbb{F}_{q^t}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}.$$

If $\dim_{\mathbb{F}_q} U = m$, we say that L has *rank* m. If L_U is an $\mathbb{F}_q$-linear set of Ω of rank m, we say that a point $P = \langle\mathbf{u}\rangle_{\mathbb{F}_{q^t}}$, $\mathbf{u} \in U$, of L_U has *weight* i in L_U (over $\mathbb{F}_q$) if $\dim_{\mathbb{F}_q}(\langle\mathbf{u}\rangle_{\mathbb{F}_{q^t}} \cap U) = i$ (for further details on linear sets see e.g. [17]).

A useful property proved in [11] (Property 3.1), is the following. Let $r = PG(R, \mathbb{F}_{q^t})$ be any line of Ω and $L = L_U$ be an $\mathbb{F}_q$-linear set of Ω. Then

$$r \subseteq L \Leftrightarrow \dim_{\mathbb{F}_q}(U \cap R) \geq t + 1, \tag{2.1}$$

when R is regarded as a $2t$-dimensional vector space over the subfield $\mathbb{F}_q$ (see also [17, Property 2.3]).

In [13, Thm. 3], the author considers a theoretical $\mathbb{F}_{q^2}$-linear set L of $PG(1, q^{2n})$ of rank n, where $n > 1$ is an odd integer, satisfying the following properties:

(P1) There exists an involutory semilinear collineation τ of $PG(1, q^{2n})$ and a point P of $PG(1, q^{2n})$ such that P and P^τ have weight $n-1$ and 1 in L (over $\mathbb{F}_{q^2}$), respectively.

(P2) L is disjoint from the Baer subline $PG(1, q^n)$ of $PG(1, q^{2n})$ fixed pointwise by τ.

In the same article (see [13, Thm. 4]) it is observed that the existence of such an $\mathbb{F}_{q^2}$-linear set L is equivalent to showing that a Kenstenband cap of $PG(n-1, q^2)$ is not a blocking set with respect to hyperplanes. Moreover, any such linear set, if it exists, defines a semifield $\mathbb{S}_L$ of order q^{2n} with $\mathbb{N}_l = \mathbb{F}_{q^n}$, $\mathbb{N}_r = \mathbb{N}_m = \mathbb{F}_{q^2}$ and center $\mathbb{F}_q$.

Remark 1. It should be noted that such a family of semifields $\mathbb{S}_L$ is theoretical in the sense that, for $n > 3$, it is not known whether an $\mathbb{F}_{q^2}$-linear set of $PG(1, q^{2n})$ satisfying Property (P1) and Property (P2) exists.

Now we construct the general form of an $\mathbb{F}_{q^2}$-linear set of $PG(1, q^{2n})$, $n > 1$ and n odd, satisfying Property (P1). Let $\mathbb{V}$ be the 2-dimensional vector space over $\mathbb{F}_{q^{2n}}$ of all the $\mathbb{F}_{q^n}$-linear maps of $\mathbb{F}_{q^{2n}}$ (i.e. $\mathbb{V}$ consists of the maps of the form $\varphi_{\xi,\eta}: x \mapsto \xi x + \eta x^{q^n}$, where ξ and η vary in $\mathbb{F}_{q^{2n}}$) and let $\mathbb{P} = PG(\mathbb{V}, \mathbb{F}_{q^{2n}}) = PG(1, q^{2n}) = \{\langle\varphi_{\xi,\eta}\rangle_{\mathbb{F}_{q^{2n}}} : \xi, \eta \in \mathbb{F}_{q^{2n}}\}$. Let τ be the involutory semilinear collineation of $\mathbb{P}$ induced by the map

$$\varphi_{\xi,\eta} \mapsto \varphi_{\eta^{q^n},\xi^{q^n}}.$$

It is easy to see that the Baer subline $\mathbb{P}'$ of $\mathbb{P}$ fixed pointwise by τ is

$$\mathbb{P}' = \{\langle\varphi_{\xi,\eta}\rangle_{\mathbb{F}_{q^{2n}}} : \xi, \eta \in \mathbb{F}_{q^{2n}},\ N(\xi) = N(\eta)\},$$

where N denotes the norm function of $\mathbb{F}_{q^{2n}}$ over $\mathbb{F}_{q^n}$.