Semifields in Class $\mathcal{F}_4^{(a)}$

G. L. Ebert*

Dept. of Math. Sci.
Univ. of Delaware
Newark, DE 19716, USA

ebert@math.udel.edu

G. Marino†

Dip. di Matematica
Seconda Univ. degli Studi di Napoli
I–81100 Caserta, Italy

giuseppe.marino@unina2.it

O. Polverino†

Dip. di Matematica
Seconda Univ. degli Studi di Napoli
I–81100 Caserta, Italy

olga.polverino@unina2.it

R. Trombetti†

Dip. di Matematica e Applicazioni
Univ. degli Studi di Napoli "Federico II"
I–80126 Napoli, Italy

rtrombet@unina.it

Submitted: Oct 3, 2008; Accepted: Apr 14, 2009; Published: Apr 30, 2009
Mathematics Subject Classification: 51E15

Abstract

The semifields of order q^6 which are two-dimensional over their left nucleus and six-dimensional over their center have been geometrically partitioned into six classes by using the associated linear sets in $PG(3, q^3)$. One of these classes has been partitioned further (again geometrically) into three subclasses. In this paper algebraic curves are used to construct two infinite families of odd order semifields belonging to one of these subclasses, the first such families shown to exist in this subclass. Moreover, using similar techniques it is shown that these are the only semifields in this subclass which have the right or middle nucleus which is two-dimensional over the center. This work is a non-trivial step towards the classification of all semifields that are six-dimensional over their center and two-dimensional over their left nucleus.

*This author acknowledges the support of NSA grant H98230-09-1-0074

†This work was supported by the Research Project of MIUR (Italian Office for University and Research) "Strutture geometriche, combinatoria e loro applicazioni" and by the Research group GNSAGA of INDAM

1 Introduction

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

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

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

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

$$\mathbb{K} = \{a \in \mathbb{N}_l \cap \mathbb{N}_m \cap \mathbb{N}_r \mid ab = ba,\ \forall b \in \mathbb{S}\}$$

are skewfields which are known, respectively, as the *left nucleus*, *middle nucleus*, *right nucleus* and *center* of the semifield. In the finite setting, which is the only setting considered in this paper, every skewfield is a field and thus we may assume that the center of our semifield is the finite field $\mathbb{F}_q$ of order q, where q is some power of the prime p. It is also important to note that a (finite) semifield is a vector space over its nuclei and its center.

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

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

for all $x, y \in \mathbb{S}$. From any pre-semifield, one can naturally construct a semifield which is isotopic to it (see [13]).

A pre-semifield $\mathbb{S}$, viewed as a vector space over some prime field $\mathbb{F}_p$, can be used to coordinatize an affine (and hence a projective) plane of order $|\mathbb{S}|$ (see [5] and [11]). Albert [1] showed that the projective planes coordinatized by $\mathbb{S}$ and $\mathbb{S}'$ are isomorphic if and only if the pre-semifields $\mathbb{S}$ and $\mathbb{S}'$ are isotopic, hence the importance of the notion of isotopism. Any projective plane $\pi(\mathbb{S})$ coordinatized by a semifield (or pre-semifield) is called a *semifield plane*.

Semifield planes are necessarily translation planes, and the *kernel* of a semifield plane, when treated as a translation plane, is the left nucleus of the coordinatizing semifield. A semifield plane is Desarguesian (classical) if and only if the coordinatizing semifield $\mathbb{S}$ is a field, in which case all nuclei as well as the center are equal to $\mathbb{S}$. As discussed in [2], any translation plane can be obtained from a spread of an odd dimensional projective space. The translation planes are isomorphic if and only if the corresponding spreads are projectively equivalent.

If the semifield is two-dimensional over its left nucleus, say $\mathbb{F}_{q^n}$, then the corresponding semifield plane will arise from a line spread of $PG(3, q^n)$. This spread can be represented by a *spread set of linear maps*, as described and fully discussed in [6]. In short, such a spread of linear maps consists of a set S of q^{2n} linearized polynomials of the form

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

for some $\delta, \zeta \in \mathbb{F}_{q^{2n}}$, with the following properties:

P1 S is closed under addition and $\mathbb{F}_q$–scalar multiplication, with the usual point-wise operations on functions.

P2 $\mathbb{F}_q$ is the largest subfield of $\mathbb{F}_{q^n}$ with respect to which S is a vector subspace of the vector space of all $\mathbb{F}_{q^n}$–linear maps of $\mathbb{F}_{q^{2n}}$.

P3 Every nonzero map in S is non-singular (that is, invertible).

Moreover, if we assume δ and ζ are nonzero to avoid trivialities, it is straightforward to show that

$$\varphi_{\delta,\zeta} \text{ is non-singular} \Leftrightarrow N\left(\frac{\delta}{\zeta}\right) \neq 1, \tag{1}$$

where N is the norm from $\mathbb{F}_{q^{2n}}$ to $\mathbb{F}_{q^n}$.

From the above properties for the q^{2n} maps in S, we know that there is a unique element $\varphi \in S$ such that $\varphi(1) = y$ for each element $y \in \mathbb{F}_{q^{2n}}$. We call this uniquely determined map φ_y, and thus there is a natural one-to-one correspondence between the linear maps in S and the elements of the field $\mathbb{F}_{q^{2n}}$. If we now define an algebraic structure $\mathbb{S} = (\mathbb{F}_{q^{2n}}, +, \circ)$, where $+$ is the sum operation in the field $\mathbb{F}_{q^{2n}}$ and $\circ$ is defined as

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

it turns out (for instance, see [12]) that $\mathbb{S}$ is a semifield with identity 1 and left nucleus $\mathbb{F}_{q^n}$ that is isotopic to the semifield of order q^{2n} which with we began.

The general classification of finite semifields appears to be way beyond reach at this point in time. However, some progress has been made in the case when the semifield is two-dimensional over its left nucleus $\mathbb{F}_{q^n}$, where as always we assume the center of the semifield $\mathbb{F}_q$. In fact, the complete classification for $n = 2$ is given in [4]. For $n = 3$ ([16]), the semifields of order q^6 which are two-dimensional over their left nucleus and six-dimensional over their center have been geometrically partitioned into six classes $\mathcal{F}_0, \mathcal{F}_1, \cdots, \mathcal{F}_5$ by using the associated *linear sets* in $PG(3, q^3)$ (see [4] or [12] and see [18] for a more general discussion on linear sets). In [16] the classes $\mathcal{F}_0, \mathcal{F}_1$, and $\mathcal{F}_2$ are completely characterized.

The class $\mathcal{F}_4$ has been partitioned further (again geometrically) into three subclasses, denoted $\mathcal{F}_4^{(a)}$, $\mathcal{F}_4^{(b)}$ and $\mathcal{F}_4^{(c)}$. In [7] the generic multiplication is determined for each of these three subclasses, and several computer-generated examples of new semifields are presented that belong to these subclasses. In the present paper we use some ideas from algebraic curves to construct two infinite families for odd prime powers q belonging to the subclass $\mathcal{F}_4^{(a)}$, the first such infinite families.

Precisely, for any $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ (q odd), with minimal polynomial $x^3 - \sigma x - 1 \in \mathbb{F}_q[x]$, and for any $b \in \mathbb{F}_{q^6}^*$ such that $N(b) = b^{q^3+1} = \sigma^2 + 9u + 3\sigma u^2$, we get a semifield $\mathbb{S}_{u,b} = (\mathbb{F}_{q^6}, +, \circ)$ with multiplication given by

$$x \circ y = (\alpha + \beta u + \gamma u^2)x + b\gamma x^{q^3},$$

where $\alpha, \beta, \gamma \in \mathbb{F}_{q^2}$ are uniquely determined in such a way that $y = \alpha + \beta u + \gamma(b + u^2)$. Moreover, with the same choices of u and b we get a semifield $\overline{\mathbb{S}}_{u,b} = (\mathbb{F}_{q^6}, +, \circ)$ with multiplication given by

$$x \circ y = (\alpha + \beta u + \gamma u^2)x + b\gamma^q x^{q^3},$$

where $\alpha, \beta, \gamma \in \mathbb{F}_{q^2}$ are uniquely determined in such a way that $y = \alpha + \beta u + \gamma u^2 + b\gamma^q$.

Also, we are able to show that, when q is odd, up to isotopism, these are the only semifields in $\mathcal{F}_4^{(a)}$ which have the right or middle nucleus of order q^2. In particular, we are able to show that no such semifields exist when q is even. Thus this work is bringing us closer and closer to a complete classification in the case $n = 3$.

2 Two Infinite Families in Class $\mathcal{F}_4^{(a)}$

From now on, N will denote the norm function from $\mathbb{F}_{q^6}$ to $\mathbb{F}_{q^3}$. The following theorem in [7] provides the generic multiplication for a semifield of order q^6 belonging to class $\mathcal{F}_4^{(a)}$.

Theorem 2.1. ([7, Thm. 3.1]) *Let $\mathbb{S}_4^{(a)} = (\mathbb{F}_{q^6}, +, \circ)$ be a semifield belonging to $\mathcal{F}_4^{(a)}$. Then there exist $u, v \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$, $A, D \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^3}$, and $b, B, C \in \mathbb{F}_{q^6}^*$ with*

$$N(b) \notin \left\{ N\left(\frac{a_0 + a_1 u + A(a_2 + a_3 v) + a_4 B + a_5 C}{a_4 + a_5 D} \right) : a_i \in \mathbb{F}_q,\ (a_4, a_5) \neq (0,0) \right\}$$

such that $\{1, u, A, Av, B, C\}$ is a basis for $\mathbb{F}_{q^6}$ over $\mathbb{F}_q$ and, up to isotopy, the multiplication in $\mathbb{S}_4^{(a)}$ is given by

$$x \circ y = [(a_0 + a_1 u) + A(a_2 + a_3 v) + a_4 B + a_5 C]x + b(a_4 + a_5 D)x^{q^3}, \tag{2}$$

where $a_0, a_1, \cdots, a_5 \in \mathbb{F}_q$ are uniquely determined so that $y = a_0 + a_1 u + a_2 A + a_3 Av + a_4(B + b) + a_5(C + bD)$.

Conversely, Multiplication (2) subject to the conditions stated above defines a semifield of order q^6, with $\mathbb{N}_l = \mathbb{F}_{q^3}$ and center $\mathbb{F}_q$, belonging to the Family $\mathcal{F}_4^{(a)}$.

The next two results, also found in [7], determine precisely when such a semifield has the right nucleus of order q^2 or the middle nucleus of order q^2.

Theorem 2.2. ([7, Thm. 3.2]) *Using the notation of Theorem 2.1, the right nucleus of $\mathbb{S}_4^{(a)}$ has order at most q^2. Moreover, the right nucleus has order q^2 if and only if the following conditions are satisfied:*

(i) $[1, u, A, Av]_{\mathbb{F}_q} = [1, u]_{\mathbb{F}_{q^2}}$,

(ii) $D \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$,

(iii) $C \in DB + [1, u]_{\mathbb{F}_{q^2}}$.

In this case we have $\mathbb{N}_r = \mathbb{F}_{q^2}$, $\mathbb{N}_m = \mathbb{F}_q$ *and there exists some* $b' \in \mathbb{F}_{q^6}^*$ *with*

$$N(b') \notin \{N(\alpha + \beta u + u^2) \mid \alpha, \beta \in \mathbb{F}_{q^2}\} \tag{3}$$

such that multiplication (2) may be rewritten as

$$x \circ y = (\alpha + \beta u + \gamma u^2)x + \gamma b' x^{q^3}, \tag{4}$$

where $\alpha, \beta, \gamma \in \mathbb{F}_{q^2}$ *are uniquely determined so that* $y = \alpha + \beta u + \gamma(b' + u^2)$.

Conversely, Multiplication (4) subject to the conditions stated above defines a semifield of order q^6 *belonging to the Family* $\mathcal{F}_4^{(a)}$ *and having* $\mathbb{N}_l = \mathbb{F}_{q^3}$, $\mathbb{N}_r = \mathbb{F}_{q^2}$, $\mathbb{N}_m = \mathbb{K} = \mathbb{F}_q$.

Theorem 2.3. ([7, Thm. 3.3]) *Using the notation of Theorem 2.1, the middle nucleus of* $\mathbb{S}_4^{(a)}$ *has order at most* q^2. *Moreover, the middle nucleus has order* q^2 *if and only if the following conditions are satisfied:*

(i) $[1, u, A, Av]_{\mathbb{F}_q} = [1, u]_{\mathbb{F}_{q^2}}$,

(ii) $D \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$,

(iii) $C \in D^q B + [1, u]_{\mathbb{F}_{q^2}}$.

In this case we have $\mathbb{N}_r = \mathbb{F}_q$, $\mathbb{N}_m = \mathbb{F}_{q^2}$ *and there exists some* $b'' \in \mathbb{F}_{q^6}^*$ *with*

$$N(b'') \notin \{N(\alpha + \beta u + u^2) \mid \alpha, \beta \in \mathbb{F}_{q^2}\}$$

such that multiplication (2) may be rewritten as

$$x \circ y = (\alpha + \beta u + \gamma u^2)x + \gamma^q b'' x^{q^3}, \tag{5}$$

where $\alpha, \beta, \gamma \in \mathbb{F}_{q^2}$ *are uniquely determined so that* $y = \alpha + \beta u + \gamma u^2 + \gamma^q b''$.

Conversely, Multiplication (5) subject to the conditions stated above defines a semifield of order q^6 *belonging to the Family* $\mathcal{F}_4^{(a)}$ *and having* $\mathbb{N}_l = \mathbb{F}_{q^3}$, $\mathbb{N}_m = \mathbb{F}_{q^2}$, $\mathbb{N}_r = \mathbb{K} = \mathbb{F}_q$.

Moreover, it should be noted that semifields with operation (5) are the transposes of semifields with operation (4) (see [7, Remark 3.4]).

In this section we show that there are two infinite families of semifields belonging to class $\mathcal{F}_4^{(a)}$, each semifield in the first family having right nucleus of order q^2, and each semifield in the second family having middle nucleus of order q^2. We begin with the following observation about finite fields.

Lemma 2.4. *For any prime power* q, *there is an irreducible monic polynomial in* $\mathbb{F}_q[x]$ *of the form*

$$f(x) = x^3 - \sigma x - 1,$$

for some $\sigma \in \mathbb{F}_q^*$.

Proof. The statement in the lemma is equivalent to the existence of an element $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ whose trace and norm over $\mathbb{F}_q$ are 0 and 1, respectively. Namely, the minimal polynomial for such an element u is the desired polynomial. And, indeed, such an element exists for any prime power q (for instance, see [17]). $\square$

In the proofs of our main results we will use some techniques involving algebraic curves. So, for the benefit of the reader, we now give some definitions and basic facts concerning algebraic plane curves.

Let X_0, X_1, X_2 be homogeneous projective coordinates of a plane $PG(2, K)$ over a field K. Let $F \in K[X_0, X_1, X_2]$ be a homogeneous polynomial of degree $n > 0$, and define

$$V(F) = \{P = (Y_0, Y_1, Y_2) \in PG(2, K) : F(Y_0, Y_1, Y_2) = 0\}.$$

We let (F) be the ideal generated by F in the polynomial ring $K[X_0, X_1, X_2]$. The pair $\Gamma = (V(F), (F))$ is an *algebraic plane curve* of $PG(2, K)$ with equation $F(\overline{X}) = F(X_0, X_1, X_2) = 0$ of *order* (or *degree*) n. We typically identify the curve $\Gamma = (V(F), (F))$ with the variety $V(F)$. If F is irreducible over K, then Γ is said to be *irreducible.* If F is irreducible over the algebraic closure $\hat{K}$ of K, then Γ is called *absolutely irreducible.*

Assume now that K is an algebraically closed field. Then any homogeneous polynomial $F(\overline{X})$ has a factorization $F = F_1 \cdot F_2 \cdot \ldots \cdot F_r$ into irreducible homogeneous factors, unique to within constant multiples. The irreducible curves $\Gamma_1, \ldots, \Gamma_r$ whose equations are $F_1(\overline{X}) = 0, \ldots, F_r(\overline{X}) = 0$, respectively, are called the *(irreducible) components* of the curve Γ whose equation is $F(\overline{X}) = 0$. An irreducible curve appearing more than once as a component of Γ is said to be a *multiple* component of Γ. A curve with two or more components is said to be *reducible.*

Let Γ be a curve of order n of $PG(2, K)$, and let ℓ be a line passing through the point P_0 of Γ which is not a component of the curve. The algebraic multiplicity of P_0 as a solution of the algebraic system given by the equations of Γ and ℓ is the *intersection number of* ℓ *and* Γ *in* P_0. The minimal m_0 of the intersection numbers of all the lines through P_0 is the *multiplicity of* P_0 *on* Γ, and we write $m_0 = m_{P_0}(\Gamma)$. Obviously, $1 \leq m_{P_0}(\Gamma) \leq n$. If $m_{P_0}(\Gamma) = 1$, then P_0 is a *simple* point of Γ; if $m_{P_0}(\Gamma) > 1$, then P_0 is a *singular* point of Γ. In particular, P_0 is a *double* point, *triple* point, *r–fold* point if $m_{P_0}(\Gamma) = 2$, $m_{P_0}(\Gamma) = 3$, $m_{P_0}(\Gamma) = r$, respectively. Any point belonging to a multiple component of Γ or to at least two components of Γ is a singular point of the curve. If $m_{P_0}(\Gamma) = r$, then any line ℓ through P_0 such that the intersection number of ℓ and Γ in P_0 is greater than r is called a *tangent to* Γ *at* P_0. An r–fold point P_0 of Γ admits at least one tangent and at most r tangents to Γ at P_0.

Now let $K = \mathbb{F}_q$ and let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_q$, where q is any prime power. The projective plane $PG(2, \mathbb{F})$ contains the finite planes $PG(2, q^i)$ for each $i \geq 1$. An *$\mathbb{F}_{q^i}$–rational point* of Γ is a point $P = (Y_0, Y_1, Y_2)$ in the plane $PG(2, q^i)$ such that $F(Y_0, Y_1, Y_2) = 0$.

To any absolutely irreducible curve Γ of $PG(2, q)$ is associated a non–negative integer g, called the *genus* of Γ ([10, Sec. 5]). It can be shown (see [10, pag. 135]) that if Γ

is an absolutely irreducible curve of order n and $P_1,\dots,P_h$ are its singular points with multiplicity $r_1,\dots,r_h$, respectively, the genus g of Γ satisfies the inequality

$$g \le \frac{(n-1)(n-2)-\sum_{i=1}^{h} r_i(r_i-1)}{2}. \tag{6}$$

Finally, let Γ be an absolutely irreducible curve of $PG(2,q)$, and let g be its genus. Denote by M_q the sum of the number of $\mathbb{F}_q$–rational simple points of Γ and the number of distinct tangents (over $\mathbb{F}_q$) to Γ at the singular $\mathbb{F}_q$–rational points of Γ. Then by the Hasse–Weil Theorem ([8, Section 2.9]) one obtains the following result:

$$q+1-2g\sqrt{q} \le M_q \le q+1+2g\sqrt{q}. \tag{7}$$

For further details on algebraic curves over finite fields see [8] and/or [10].

We now prove the following technical lemma, which will be used to show the existence of semifields in class $\mathcal{F}_4^{(a)}$.

Lemma 2.5. *Let $PG(2,\mathbb{F})$ be the projective plane over the algebraic closure $\mathbb{F}$ of $\mathbb{F}_q$, with q an odd prime power. Let ρ be a nonsquare element of $\mathbb{F}_q$ and $\sigma \in \mathbb{F}_q^*$ as in Lemma 2.4. For each $A',B',C' \in \mathbb{F}_q$ consider the algebraic curve $\Gamma = \Gamma(A',B',C')$ of $PG(2,\mathbb{F})$ with affine equation*

$$\begin{aligned} f(x,y) = (x^2-\rho y^2)^3 - 2C'(x^2-\rho y^2)^2 - 2x(2\sigma x - B')(x^2-\rho y^2) - 8\rho y^2 x \\ -\rho(C'^2-4A')y^2 + (C'+2\sigma)^2x^2 - 2B'(C'+2\sigma)x + B'^2 = 0. \end{aligned} \tag{8}$$

If Γ has no $\mathbb{F}_q$–rational point off the line $y=0$, then either $(A',B',C') = (0,-1,-\sigma)$ or $(A',B',C') = (\sigma^2,8,2\sigma)$. In fact, $\Gamma(0,-1,-\sigma)$ and $\Gamma(\sigma^2,8,2\sigma)$ have no $\mathbb{F}_q$–rational points, either on or off the line $y=0$.

Proof. By the previous lemma there exists an element $u \in \mathbb{F}_{q^3}\setminus\mathbb{F}_q$ such that $u^3 = \sigma u + 1$. Denoting by Φ the semilinear collineation of the projective plane $PG(2,\mathbb{F})$ induced by the automorphism $x \mapsto x^q$, it is clear from Equation (8) that $\Gamma^\Phi = \Gamma$.

If $y=0$, then Equation (8) becomes

$$(x^3-(C'+2\sigma)x+B')^2 = 0.$$

Thus there are at most three affine points on Γ with $y=0$, namely $P_{\eta_i} = (\eta_i,0)$, where $\eta_i^3 - (C'+2\sigma)\eta_i + B' = 0$ for $i \in \{1,2,3\}$. Moreover, either at least one point P_{η_i} is an $\mathbb{F}_q$–rational point or P_{η_1}, P_{η_2} and P_{η_3} are three distinct $\mathbb{F}_{q^3}$–rational points conjugate over $\mathbb{F}_q$. In either case, a straightforward computation shows that these points are double points for Γ. Certainly, we see that Γ has at most three $\mathbb{F}_q$–rational points on the line $y=0$.

The curve Γ, expressed projectively, has two triple points, namely $P_\infty = (\xi,1,0)$ and $Q_\infty = (-\xi,1,0)$, where $\xi \in \mathbb{F}_{q^2}\setminus\mathbb{F}_q$ and $\xi^2 = \rho$ (hence $\xi^q = -\xi$). Note that these two points have coordinates in $\mathbb{F}_{q^2}$ and $Q_\infty = P_\infty^\Phi$. The tangents to Γ at P_∞ are

$$t_1\colon x - \xi y - u = 0,$$

$$t_2\colon x-\xi y-u^q=0,$$
$$t_3\colon x-\xi y-u^{q^2}=0,$$

and hence

$$t_4=t_1^{\Phi}\colon x+\xi y-u^q=0,$$
$$t_5=t_2^{\Phi}\colon x+\xi y-u^{q^2}=0,$$
$$t_6=t_3^{\Phi}\colon x+\xi y-u=0$$

are the tangents to Γ at Q_∞. Note that $\{t_1,t_2,t_3,t_4,t_5,t_6\}=\{t_1,t_1^{\Phi},t_1^{\Phi^2},t_1^{\Phi^3},t_1^{\Phi^4},t_1^{\Phi^5}\}$.

To prove the first assertion, we begin by assuming Γ has no $\mathbb{F}_q$–rational point with $y\neq 0$, and thus has at most three $\mathbb{F}_q$–rational points in total by our work above.

Suppose first that Γ is absolutely irreducible. Then, by (6) Γ has genus $g\leq 1$. From the Hasse–Weil lower bound (7), we thus have

$$M_q\geq q+1-2g\sqrt{q}\geq(\sqrt{q}-1)^2. \tag{9}$$

Since Γ has at most three $\mathbb{F}_q$–rational points (and they are double points for Γ), we have $M_q\leq 6$. This contradicts (9) when $q\geq 13$. As Magma [3] computations show that the first assertion stated in the lemma holds for $q<13$, we may assume for the remainder of the proof that Γ is absolutely reducible and $q\geq 13$.

Let $\mathcal{C}_n$ denote an absolutely irreducible component of Γ passing through the point P_∞, where $\mathcal{C}_n$ has order n for some $1\leq n\leq 5$.

$\boxed{\text{Case } n=1}$ Suppose first that there exists a line ℓ of $PG(2,\mathbb{F})$ contained in Γ and passing through the point P_∞. Since ℓ is a tangent to the curve Γ at P_∞, we know that $\ell=t_1^{\Phi^i}$ for some $i\in\{0,2,4\}$. Since $\Gamma^{\Phi}=\Gamma$, necessarily $\Gamma=t_1\cup t_1^{\Phi}\cup t_1^{\Phi^2}\cup t_1^{\Phi^3}\cup t_1^{\Phi^4}\cup t_1^{\Phi^5}$ and thus $t_1: x=\xi y+u$ is a component of Γ, i.e. the polynomial $f(\xi y+u,y)$ is the zero polynomial. By direct computation, recalling that $u^3=\sigma u+1$ and using the fact that $\{1,u,u^2\}$ are linearly independent over $\mathbb{F}_q$, we obtain in this case that $(A',B',C')=(0,-1,-\sigma)$.

$\boxed{\text{Case } n=2}$ Suppose next that there is an absolutely irreducible conic $\mathcal{C}_2$ in $PG(2,\mathbb{F})$ contained in Γ and passing through the point P_∞. There are many subcases to be considered. If $\mathcal{C}_2^{\Phi}=\mathcal{C}_2$, then $\mathcal{C}_2$ has $q+1$ $\mathbb{F}_q$–rational points, a contradiction. Hence we may assume that $\mathcal{C}_2^{\Phi}\neq\mathcal{C}_2$. Moreover, if $\mathcal{C}_2^{\Phi^2}=\mathcal{C}_2$, then $\mathcal{C}_2$ is represented by an equation with coefficients in $\mathbb{F}_{q^2}$, up to a nonzero scalar. Hence, since P_∞ is a simple point for $\mathcal{C}_2$, one of the tangents to Γ at P_∞ should be represented by an equation whose coefficients are in $\mathbb{F}_{q^2}$ (up to a nonzero scalar), a contradiction.

It follows that, in the $n=2$ case, we have $\mathcal{C}_2\neq\mathcal{C}_2^{\Phi}$ and $\mathcal{C}_2\neq\mathcal{C}_2^{\Phi^2}$. Again using $\Gamma^{\Phi}=\Gamma$ and $Q_\infty=P_\infty^{\Phi}$, we obtain

$$\Gamma=\mathcal{C}_2\cup\mathcal{C}_2^{\Phi}\cup\mathcal{C}_2^{\Phi^2},\quad \mathcal{C}_2=\mathcal{C}_2^{\Phi^3},\quad \{P_\infty,Q_\infty\}\subseteq\mathcal{C}_2\cap\mathcal{C}_2^{\Phi}\cap\mathcal{C}_2^{\Phi^2},$$

where both P_∞ and Q_∞ are simple points of the conics $\mathcal{C}_2$, $\mathcal{C}_2^{\Phi}$ and $\mathcal{C}_2^{\Phi^2}$. Moreover, in this case Γ has no $\mathbb{F}_q$–rational point. Indeed, if at least one of the points P_{η_i} $(i=1,2,3)$

were an $\mathbb{F}_q$–rational point, it would belong to all of the conics $\mathcal{C}_2$, $\mathcal{C}_2^{\Phi}$ and $\mathcal{C}_2^{\Phi^2}$ and so would be a triple point for Γ, a contradiction. Hence the points P_{η_i} $(i = 1, 2, 3)$ are three distinct $\mathbb{F}_{q^3}$–rational points of Γ and they are conjugate over $\mathbb{F}_q$. Also, since $\mathcal{C}_2 = \mathcal{C}_2^{\Phi^3}$, if we denote by t the tangent to $\mathcal{C}_2$ at P_∞ (respectively Q_∞), then t^{Φ^3} is the tangent to $\mathcal{C}_2$ at Q_∞ (respectively P_∞).

Thus we may assume that $\mathcal{C}_2$ belongs to the pencil of conics passing through P_∞ and Q_∞ and whose tangents at P_∞ and Q_∞ are

$$t_1 \colon x - \xi y - u = 0 \quad \text{and} \quad t_1^{\Phi^3} \colon x + \xi y - u = 0,$$

respectively. Hence, the conic $\mathcal{C}_2$ has affine equation

$$\mathcal{C}_2 : x^2 - \rho y^2 - 2ux + F = 0$$

for some $F \in \mathbb{F}_{q^3}$ and, consequently,

$$\mathcal{C}_2^{\Phi} \colon x^2 - \rho y^2 - 2u^q x + F^q = 0,$$

$$\mathcal{C}_2^{\Phi^2} \colon x^2 - \rho y^2 - 2u^{q^2} x + F^{q^2} = 0.$$

Now, observe that the line $y = 0$ intersects the conic $\mathcal{C}_2^{\Phi^i}$ $(i = 0, 1, 2)$ at the affine points $P_1^{\Phi^i} = (u^{q^i} + \sqrt{u^{2q^i} - F^{q^i}}, 0)$ and $P_2^{\Phi^i} = (u^{q^i} - \sqrt{u^{2q^i} - F^{q^i}}, 0)$. On the other hand, the line $y = 0$ intersects the curve Γ in the three distinct affine $\mathbb{F}_{q^3}$–rational points P_{η_1}, $P_{\eta_1}^{\Phi}$ and $P_{\eta_1}^{\Phi^2}$ as previously defined, where

$$\eta_1^3 - (C' + 2\sigma)\eta_1 + B' = 0. \tag{10}$$

It follows that $\{P_1, P_2, P_1^{\Phi}, P_2^{\Phi}, P_1^{\Phi^2}, P_2^{\Phi^2}\} = \{P_{\eta_1}, P_{\eta_1}^{\Phi}, P_{\eta_1}^{\Phi^2}\}$, and by (10) we know that

$$Tr_{q^3/q}(\eta_1) = \eta_1 + \eta_1^q + \eta_1^{q^2} = 0. \tag{11}$$

Hence we see that we must have $P_1 = P_2$ or $P_1 = P_2^{\Phi}$ or $P_1 = P_2^{\Phi^2}$. (Note that if $P_1 = P_1^{\Phi}$ or $P_1 = P_1^{\Phi^2}$, then P_1 is an $\mathbb{F}_q$–rational point of Γ, a contradiction.) If $P_1 = P_2$, then $F = u^2$ and hence $\mathcal{C}_2 \colon (x - u)^2 - \rho y^2 = 0$. But then $\mathcal{C}_2$ is a reducible conic, a contradiction. Thus $P_1 \neq P_2$, and so either $P_1 = P_2^{\Phi}$ or $P_1 = P_2^{\Phi^2}$. If $P_1 = P_2^{\Phi}$, since Γ has no $\mathbb{F}_q$–rational points, the three distinct $\mathbb{F}_{q^3}$–rational intersection points of Γ and the line $y = 0$ are $\{P_1, P_2, P_1^{\Phi}\}$. Then by (11) we obtain

$$(u + \sqrt{u^2 - F}) + (u - \sqrt{u^2 - F}) + (u^q + \sqrt{u^{2q} - F^q}) = 0,$$

and thus

$$F = -4(u^{2q^2} + u^{q^2+1}) = -4u^{q^2}(u^{q^2} + u) = 4u^{q^2+q} = \frac{4}{u},$$

recalling that $N(u) = 1$ and $Tr_{q^3/q}(u) = 0$. Arguing in the same way, if $P_1 = P_2^{\Phi^2}$, then also $F = \frac{4}{u}$.

In summary, if $P_1 \neq P_2$, then the conic $\mathcal{C}_2$ is absolutely irreducible and has the affine equation

$$x^2 - \rho y^2 - 2ux + \frac{4}{u} = 0.$$

Recalling that $\Gamma = \mathcal{C}_2 \cup \mathcal{C}_2^{\Phi} \cup \mathcal{C}_2^{\Phi^2}$, it is now easy to see that

$$\mathcal{C}_2 \cap \mathcal{C}_2^{\Phi} \cap \mathcal{C}_2^{\Phi^2} = \{P_\infty, Q_\infty\}.$$

Since $\mathcal{C}_2$ is a component of Γ, we obtain from Equation (8) that $(A', B', C') = (\sigma^2, 8, 2\sigma)$. It should be noted that this computation uses $\frac{1}{u} = u^2 - \sigma$ and the fact that $\{1, u, u^2\}$ are linearly independent over $\mathbb{F}_q$.

$\boxed{\text{Case } n = 3}$ Since $\Gamma^{\Phi} = \Gamma$, the cubic $\mathcal{C}_3^{\Phi}$ must be a component of Γ. If $\mathcal{C}_3^{\Phi} = \mathcal{C}_3$, then $\mathcal{C}_3$ is an irreducible cubic over $\mathbb{F}_q$, and $\Gamma = \mathcal{C}_3 \cup \mathcal{C}_3'$, where $\mathcal{C}_3'$ is another (possibly reducible) cubic over $\mathbb{F}_q$. Since $\mathcal{C}_3$ has genus $g \leq 1$, from the Hasse–Weil lower bound (9) with $q \geq 13$, we get a contradiction. It follows that $\mathcal{C}_3^{\Phi} \neq \mathcal{C}_3$ and $\Gamma = \mathcal{C}_3 \cup \mathcal{C}_3^{\Phi}$, with $\mathcal{C}_3^{\Phi^2} = \mathcal{C}_3$, i.e. $\mathcal{C}_3$ is represented by an equation with coefficients in $\mathbb{F}_{q^2}$, up to a nonzero scalar. Again, since the point P_∞ is an ordinary triple point for Γ and since $\mathcal{C}_3$ is absolutely irreducible, we get that P_∞ is a simple point of either $\mathcal{C}_3$ or $\mathcal{C}_3^{\Phi}$. Hence one of the tangents to Γ at P_∞ should be represented by an equation whose coefficients are in $\mathbb{F}_{q^2}$ (up to a nonzero scalar), a contradiction.

$\boxed{\text{Case } n = 4}$ Since $\Gamma^{\Phi} = \Gamma$, we obtain $\Gamma = \mathcal{C}_4 \cup \mathcal{C}$, where $\mathcal{C}$ is a conic (possibly reducible) of the projective plane $PG(2, \mathbb{F})$, such that $\mathcal{C}^{\Phi} = \mathcal{C}$ and $\mathcal{C}_4^{\Phi} = \mathcal{C}_4$. Since P_∞ and Q_∞ are triple points of Γ and $\mathcal{C}_4$ is irreducible, at least one of P_∞ and Q_∞ is on the conic $\mathcal{C}$. Thus, if $\mathcal{C}$ is reducible, at least one of its linear components must pass through P_∞ or Q_∞ and hence must be the line $t_1^{\Phi^i}$, for some $i \in \{0, \ldots, 5\}$, i.e. Γ is the union of the six lines $t_1, t_1^{\Phi}, \ldots, t_1^{\Phi^5}$, a contradiction. Therefore $\mathcal{C}$ is absolutely irreducible, and thus since $\mathcal{C}^{\Phi} = \mathcal{C}$, it must have $q + 1$ $\mathbb{F}_q$–rational points, again a contradiction.

$\boxed{\text{Case } n = 5}$ Finally, suppose that Γ is the union of $\mathcal{C}_5$ and a linear component. Since $\Gamma^{\Phi} = \Gamma$, the curve Γ has at least $q+1$ $\mathbb{F}_q$–rational points (which belong to the linear component), again a contradiction.

Thus we have shown that if Γ has no $\mathbb{F}_q$–rational point with $y \neq 0$, then necessarily $(A', B', C') = (0, -1, -\sigma)$ or $(A', B', C') = (\sigma^2, 8, 2\sigma)$, proving the first statement of the lemma.

Moreover, if $(A', B', C') = (0, -1, -\sigma)$, then $\Gamma = t_1 \cup t_1^{\Phi} \cup t_1^{\Phi^2} \cup t_1^{\Phi^3} \cup t_1^{\Phi^4} \cup t_1^{\Phi^5}$, where $t_1 : x = \xi y + u$. And if $(A', B', C') = (\sigma^2, 8, 2\sigma)$, then $\Gamma = \mathcal{C}_2 \cup \mathcal{C}_2^{\Phi} \cup \mathcal{C}_2^{\Phi^2}$, where $\mathcal{C}_2 : x^2 - \rho y^2 - 2ux + \frac{4}{u} = 0$. In both these cases the curve Γ has no $\mathbb{F}_q$–rational point, either on or off the line $y = 0$, proving the second statement of the lemma. $\square$

We now use the above results to prove the following theorem.

Theorem 2.6. *Assume that q is an odd prime power. Let $u \in \mathbb{F}_{q^3} \backslash \mathbb{F}_q$ such that $u^3 = \sigma u + 1$ for some $\sigma \in \mathbb{F}_q^*$, and let*

$$P(u) = \{N(\alpha + \beta u + u^2) \colon \alpha, \beta \in \mathbb{F}_{q^2}\}.$$

Then there exists a unique non-zero element η in $\mathbb{F}_{q^3} \setminus P(u)$. In fact, $\eta = \sigma^2 + 9u + 3\sigma u^2$.

Proof. Let η be an element of $\mathbb{F}_{q^3}$ and uniquely express $\eta = A + Bu + Cu^2$ for some $A, B, C \in \mathbb{F}_q$. Then $\eta \in P(u)$ if and only if

$$A + Bu + Cu^2 = (\alpha^q + \beta^q u + u^2)(\alpha + \beta u + u^2) \tag{12}$$

for some $\alpha, \beta \in \mathbb{F}_{q^2}$. Taking into account that $u^4 = u + \sigma u^2$ and $\{1, u, u^2\}$ is an $\mathbb{F}_q$–basis of $\mathbb{F}_{q^3}$, we see that (12) is satisfied if and only if the system

$$\begin{cases} \alpha^{q+1} + (\beta + \beta^q) & = & A \\ \alpha\beta^q + \alpha^q\beta + \sigma(\beta + \beta^q) + 1 & = & B \\ \alpha + \alpha^q + \beta^{q+1} + \sigma & = & C \end{cases} \tag{13}$$

admits a solution $(\alpha, \beta) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$.

Now, let ξ be an element of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $\xi^2 = \rho$, where ρ is a nonsquare in $\mathbb{F}_q$. Taking $\{1, \xi\}$ as a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, we may write $\alpha = w + z\xi$ and $\beta = x + y\xi$ for unique choices of $w, z, x, y \in \mathbb{F}_q$. Hence, System (13) becomes

$$\begin{cases} w^2 - z^2\rho + 2x & = & A' \\ 2(xw - zy\rho) + 2x\sigma & = & B' \\ 2w + x^2 - \rho y^2 & = & C', \end{cases} \tag{14}$$

where $A' = A$, $B' = B - 1$ and $C' = C - \sigma$. That is, Equality (12) is satisfied if and only if System (14) admits a solution $(w, z, x, y) \in \mathbb{F}_q^4$. That is, $\eta \in P(u)$ if and only if System (14) has a common solution.

From the second and third equations of (14), for any common solution we may solve for w and z in terms of x and y, provided $y \neq 0$. Substituting into the first equation of (14), we see that if (12) is satisfied for some $\alpha = w + z\xi$ and $\beta = x + y\xi$ with $y \neq 0$, then the algebraic curve Γ_η of the projective plane $PG(2, \mathbb{F})$ with affine equation

$$\begin{gathered} (x^2 - \rho y^2)^3 - 2C'(x^2 - \rho y^2)^2 - 2x(2\sigma x - B')(x^2 - \rho y^2) - 8\rho y^2 x \\ -\rho(C'^2 - 4A')y^2 + (C' + 2\sigma)^2 x^2 - 2B'(C' + 2\sigma)x + B'^2 = 0 \end{gathered}$$

has the $\mathbb{F}_q$–rational point (x, y). Conversely, if Γ_η has an affine $\mathbb{F}_q$–rational point (x, y) with $y \neq 0$, then we may reverse the above steps to see that necessarily $\eta = A + Bu + Cu^2 \in P(u)$.

Hence, if the element $\eta = A + Bu + Cu^2 \in \mathbb{F}_{q^3}$ does not belong to the set $P(u)$, then Γ_η has no $\mathbb{F}_q$–rational point with $y \neq 0$. From the first statement of Lemma 2.5, this implies that either $(A', B', C') = (0, -1, -\sigma)$ or $(A', B', C') = (\sigma^2, 8, 2\sigma)$; that is, we must have either $(A, B, C) = (0, 0, 0)$ or $(A, B, C) = (\sigma^2, 9, 3\sigma)$. Hence the only possible nonzero element of $\mathbb{F}_{q^3} \setminus P(u)$ is the element $\sigma^2 + 9u + 3\sigma u^2$. It remains to show that indeed this element is not in $P(u)$.

Thus we let $\bar{\eta} = \sigma^2 + 9u + 3\sigma u^2$. From our work above it suffices to show that the resulting system (14) does not have a common solution. Putting $A' = \sigma^2$, $B' = 8$ and $C' = 2\sigma$, System (14) becomes

$$\begin{cases} w^2 - z^2\rho + 2x & = & \sigma^2 \\ 2(xw - zy\rho) + 2x\sigma & = & 8 \\ 2w + x^2 - \rho y^2 & = & 2\sigma. \end{cases} \tag{15}$$

A solution $(w, z, x, y) \in \mathbb{F}_q^4$ with $y \neq 0$ would correspond to an $\mathbb{F}_q$–rational point (x, y), off the line $y = 0$, of the algebraic curve $\Gamma_{\bar{\eta}} = \Gamma(\sigma^2, 8, 2\sigma)$ in the projective plane $PG(2, \mathbb{F})$. This contradicts the second statement of Lemma 2.5, and hence such a common solution does not exist.

Finally, with $y = 0$, System (15) becomes

$$\begin{cases} w^2 - z^2\rho + 2x & = & \sigma^2 \\ 2xw + 2x\sigma & = & 8 \\ 2w + x^2 & = & 2\sigma, \end{cases}$$

which is equivalent to

$$\begin{cases} w^2 - z^2\rho + 2x & = & \sigma^2 \\ x^3 - 4\sigma x + 8 & = & 0 \\ w = -x^2/2 + \sigma. \end{cases} \tag{16}$$

If there were a solution $(w, z, x, 0) \in \mathbb{F}_q^4$ of System (16), then the curve $\Gamma_{\bar{\eta}}$ would have an $\mathbb{F}_q$–rational point on the line $y = 0$, and again we get a contradiction to the second statement of Lemma 2.5, completing the proof of the theorem. $\square$

Using the above highly technical results, we are now able to show the existence of two infinite families of semifields belonging to $\mathcal{F}_4^{(a)}$.

Theorem 2.7. *For any odd prime power q, there exists a semifield belonging to class $\mathcal{F}_4^{(a)}$ with $\mathbb{N}_r = \mathbb{F}_{q^2}$ and $\mathbb{N}_m = \mathbb{F}_q$.*

Proof. Choose u to be an element in $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ whose minimal polynomial over $\mathbb{F}_q$ is of the form $f(x) = x^3 - \sigma x - 1$, for some $\sigma \in \mathbb{F}_q^*$, as in the proof of Lemma 2.4. Let $\eta = \sigma^2 + 9u + 3\sigma u^2$, and choose $b' \in \mathbb{F}_{q^6}^*$ so that $N(b') = \eta$. Defining multiplication as in Equation (4), we obtain a semifield of the desired type by Theorem 2.6 and Theorem 2.2. In particular, we may choose $v = u$, $A = D \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $B = u^2$ and $C = Du^2$ in the notation of Theorem 2.1 to obtain such a semifield. $\square$

In a similar way, using Theorem 2.6 and Theorem 2.3, we obtain the following result.

Theorem 2.8. *For any odd prime power q, there exists a semifield belonging to class $\mathcal{F}_4^{(a)}$ with $\mathbb{N}_r = \mathbb{F}_q$ and $\mathbb{N}_m = \mathbb{F}_{q^2}$.* $\square$

We do not have similar construction for q even since Theorem 2.6 does not hold in this case, as we now show. We first prove the following lemma.

Lemma 2.9. *Let $PG(2,\mathbb{F})$ be the projective plane over the algebraic closure $\mathbb{F}$ of $\mathbb{F}_q$, with q even. Let ρ be an element of $\mathbb{F}_q$ with $Tr_{q/2}(\rho)=1$ and $\sigma\in\mathbb{F}_q^*$ as in Lemma 2.4. For any $A',B',C'\in\mathbb{F}_q$ consider the algebraic curve $\Gamma=\Gamma(A',B',C')$ of $PG(2,\mathbb{F})$ with affine equation*

$$\begin{aligned}(x^2+xy+y^2\rho)^3+(B'y+\sigma y^2+C'^2)(x^2+xy+y^2\rho)+y^3\\+(\sigma^2+C'\sigma+A')y^2+B'C'y+B'^2=0.\end{aligned}\tag{17}$$

Then Γ has no $\mathbb{F}_q$–rational point off the line $y=0$ if and only if $(A',B',C')=(0,1,\sigma)$. Moreover, Γ has at most three $\mathbb{F}_q$–rational points on the the line $y=0$.

Proof. The proof proceeds exactly as it did for Lemma 2.5. However, since all fields under consideration now have characteristic 2, the computational results are different.

Let ξ be an element of $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ such that $\xi^2+\xi+\rho=0$ (hence $\xi^q=\xi+1$). The curve Γ has two ordinary triple points, which now have coordinates $P_\infty=(\xi,1,0)$ and $Q_\infty=(\xi+1,1,0)$. As before, these coordinates are in $\mathbb{F}_{q^2}$ and $Q_\infty=P_\infty^\Phi$. The tangents to Γ at P_∞ are

$$\begin{aligned}t_1&\colon x+\xi y+u=0,\\t_2&\colon x+\xi y+u^q=0,\\t_3&\colon x+\xi y+u^{q^2}=0,\end{aligned}$$

and the tangents to Γ at Q_∞ are

$$\begin{aligned}t_4=t_1^\Phi&\colon x+(\xi+1)y+u^q=0,\\t_5=t_2^\Phi&\colon x+(\xi+1)y+u^{q^2}=0,\\t_6=t_3^\Phi&\colon x+(\xi+1)y+u=0.\end{aligned}$$

As in the previous proof, $\{t_1,t_2,t_3,t_4,t_5,t_6\}=\{t_1,t_1^\Phi,t_1^{\Phi^2},t_1^{\Phi^3},t_1^{\Phi^4},t_1^{\Phi^5}\}$.

Equation (17) reduces to

$$(x^3+C'x+B')^2=0$$

when $y=0$. Hence Γ has at most three $\mathbb{F}_q$–rational points on the line $y=0$; namely, the only possibilities are the points $P_{\eta_i}=(\eta_i,0,1)$ with $\eta_i^3+C'\eta_i+B'=0$ ($i\in\{1,2,3\}$). This proves the second assertion of the lemma. Moreover, a direct computation shows that each P_{η_i}, for $i=1,2,3$, is a double point of Γ.

We now assume that Γ has no $\mathbb{F}_q$–rational point with $y\neq 0$. In the present setting (q even), the Hasse-Weil bound shows that Γ is reducible if $q\geq 16$, and Magma [3] computations show that the result stated in the proposition holds for $q\leq 8$. Thus, as in the previous argument, we are reduced to studying the cases where Γ is either the union of the six tangents $t_1,\ldots,t_1^{\Phi^5}$ or the union of three absolutely irreducible conics which are conjugate over $\mathbb{F}_q$ (since the other cases can be dealt with as in Lemma 2.5).

In the first case, exactly as in the proof of Lemma 2.6, requiring $t_1: x=\xi y+u$ to be a component of Γ implies from Equation (17) that

$$(u^2+uy)^3+(B'y+\sigma y^2+C'^2)(u^2+uy)+y^3+(\sigma^2+C'\sigma+A')y^2+B'C'y+B'^2=0$$

for all $y \in \mathbb{F}$, and hence (using $u^3 = \sigma u + 1$) we obtain the system of equations

$$\begin{cases} (1+B')u + \sigma^2 + C'\sigma + A' = 0 \\ (B'+1)u^2 + (C'^2+\sigma^2)u + B'C' = 0 \\ (C'^2+\sigma^2)u^2 + B'^2 + 1 = 0. \end{cases}$$

The linear independence of $\{1, u, u^2\}$ over $\mathbb{F}_q$ implies that the unique solution to this system is $(A', B', C') = (0, 1, \sigma)$.

In the second case, Γ is the union of three absolutely irreducible conics with affine equations

$$\begin{aligned} \mathcal{C}_2 &: \ x^2 + xy + \rho y^2 + uy + F = 0, \\ \mathcal{C}_2^q &: \ x^2 + xy + \rho y^2 + u^q y + F^q = 0, \\ \mathcal{C}_2^{q^2} &: \ x^2 + xy + \rho y^2 + u^{q^2} y + F^{q^2} = 0, \end{aligned}$$

where F is some element of $\mathbb{F}_{q^3}$. As in the proof of Lemma 2.5, in this case the curve Γ has no $\mathbb{F}_q$–rational point whatsoever, and hence $F \notin \mathbb{F}_q$ (else $(\sqrt{F}, 0)$ would be an $\mathbb{F}_q$–rational point).

Requiring $\mathcal{C}_2$ to be a component of Γ implies that

$$(uy+F)^3 + (B'y + \sigma y^2 + C'^2)(uy+F) + y^3 + (\sigma^2 + C'\sigma + A')y^2 + B'C'y + B'^2 = 0$$

for all $y \in \mathbb{F}$, and thus

$$\begin{aligned} (u^3+\sigma u+1)y^3 + (3Fu^2 + B'u + \sigma F + \sigma^2 + C'\sigma + A')y^2 & \\ +(3F^2u + B'F + C'^2u + B'C')y + (F^3 + FC'^2 + B'^2) &= 0 \end{aligned}$$

for all $y \in \mathbb{F}$. Hence

$$Fu^2 + B'u + \sigma F + \sigma^2 + \sigma C' + A' = 0, \tag{18}$$

$$(F+C')(B' + (F+C')u) = 0, \tag{19}$$

$$F^3 + FC'^2 + B'^2 = 0. \tag{20}$$

We now express F as $F = \alpha + \beta u + \gamma u^2$, for uniquely determined elements $\alpha, \beta, \gamma \in \mathbb{F}_q$ with $(\alpha, \beta, \gamma) \neq (0,0,0)$. Since $Tr_{q^3/q}(u) = 0$ by assumption, this expression implies that $Tr_{q^3/q}(F) = 3\alpha$. However, as $F \notin \mathbb{F}_q$, Equation (20) implies that $Tr_{q^3/q}(F) = 0$, and therefore $\alpha = 0$ as the characteristic of $\mathbb{F}_q$ is not 3.

Again using the facts that $F \notin \mathbb{F}_q$ and q is even, we see from Equation (19) that $Fu = B' + C'u$ and hence $F = C' + B'\sigma + B'u^2$, since $u^3 = \sigma u + 1$. It follows from the uniquely determined expression for F in the previous paragraph that $\beta = 0$, $C' = B'\sigma$, and $\gamma = B' \neq 0$. That is, $F = B'u^2$. Since $N(u) = 1$ by assumption, we have $N(F) = N(B') = B'^3$. However, we know that $N(F) = B'^2$ from Equation (20) and thus $B' = 1$. Hence $F = u^2$ and $C' = \sigma$. Now from Equation (18), using the fact that $u^3 + \sigma u + 1 = 0$, we see that $A' = 0$. Substituting $F = u^2$ in the equation of $\mathcal{C}_2$ we get that $\mathcal{C}_2 = t_1 \cup t_6$, i.e. a contradiction.

Thus we have shown that if Γ contains no $\mathbb{F}_q$–rational point with $y \neq 0$, then necessarily $(A', B', C') = (0, 1, \sigma)$.

Conversely, if $(A', B', C') = (0, 1, \sigma)$, then $\Gamma = t_1 \cup t_1^{\Phi} \cup t_1^{\Phi^2} \cup t_1^{\Phi^3} \cup t_1^{\Phi^4} \cup t_1^{\Phi^5}$, where $t_1 : x = \xi y + u$, and direct computations show that Γ has no $\mathbb{F}_q$–rational point. Hence certainly Γ has no $\mathbb{F}_q$–rational point with $y \neq 0$, completing the proof of the lemma. $\square$

Now we can prove the following result.

Theorem 2.10. *Assume that q is even, and let $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ such that $u^3 = \sigma u + 1$ for some $\sigma \in \mathbb{F}_q^*$. Define $P(u)$ as in Theorem 2.6. Then nonzero elements in $\mathbb{F}_{q^3} \setminus P(u)$ do not exist.*

Proof. The proof proceeds exactly as it did for Theorem 2.6. Choose ξ to be an element of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $\xi^2 + \xi + \rho = 0$, where ρ is an element of $\mathbb{F}_q$ such that $Tr_{q/2}(\rho) = 1$. Then, taking $\{1, \xi\}$ as our basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, we write $\alpha = w + z\xi$ and $\beta = x + y\xi$ for uniquely determined elements $w, z, x, y \in \mathbb{F}_q$. Hence, system (14) in the proof of Proposition 2.6 becomes

$$\begin{cases} w^2 + wz + z^2\rho + y &= A' \\ wy + zx + \sigma y &= B' \\ z + x^2 + xy + y^2\rho &= C', \end{cases}$$

where $A' = A$, $B' = B + 1$ and $C' = C + \sigma$.

Thus the associated algebraic curve Γ_η now has affine equation

$$(x^2 + xy + y^2\rho)^3 + (B'y + \sigma y^2 + C'^2)(x^2 + xy + y^2\rho) + y^3$$
$$+(\sigma^2 + C'\sigma + A')y^2 + B'C'y + B'^2 = 0.$$

As in the proof of Theorem 2.6, if the element $\eta = A + Bu + Cu^2 \in \mathbb{F}_{q^3}$ does not belong to the set $P(u)$, the algebraic curve Γ_η has at most three affine $\mathbb{F}_q$–rational points (all on the line $y = 0$). From Lemma 2.9, this occurs if and only if $(A', B', C') = (0, 1, \sigma)$; that is, if and only if $(A, B, C) = (0, 0, 0)$. The result now follows. $\square$

At this stage it seems conceivable that some approach other than the one outlined in Theorem 2.7 and Theorem 2.8 might produce an even order semifield belonging to subclass $\mathcal{F}_4^{(a)}$ which is 3–dimensional over its right or middle nucleus. However, in the next section we will show that this cannot happen.

3 Isotopy and Uniqueness

From Theorem 2.2 we know that any semifield belonging to subclass $\mathcal{F}_4^{(a)}$ which is 3–dimensional over its right nucleus must have, up to isotopy, a spread set of linear maps of the form

$$S_{u,b} = \{x \mapsto (\alpha + \beta u + \gamma u^2)x + b\gamma x^{q^3} : \alpha, \beta, \gamma \in \mathbb{F}_{q^2}\},$$

for some $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and some $b \in \mathbb{F}_{q^6}^*$ such that $N(b) \notin P(u) = \{N(\alpha+\beta u+u^2)\colon \alpha, \beta, \in \mathbb{F}_{q^2}\}$. As always, N denotes the norm function from $\mathbb{F}_{q^6}$ to $\mathbb{F}_{q^3}$. We begin this section by showing that the number of isotopism classes of such semifields depends only upon $N(b)$.

Theorem 3.1. *Let $\mathbb{S}_{u,b}$ be the semifield defined by the spread set $S_{u,b}$ above. Then the following statements hold true:*

i) For each $u' \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$, there exists some $b' \in \mathbb{F}_{q^6}^*$ such that $\mathbb{S}_{u',b'}$ is isotopic to $\mathbb{S}_{u,b}$.

ii) If b' is an element of $\mathbb{F}_{q^6}^*$ such that $N(b') = N(b)$, then $\mathbb{S}_{u,b'}$ is isotopic to $\mathbb{S}_{u,b}$.

Proof. i) We first note that if $u = s + tu'$ with $s, t \in \mathbb{F}_q$ and $t \neq 0$, then $S_{u,b} = S_{u',b'}$, where $b' = \frac{b}{t^2}$. Indeed, since

$$\begin{aligned}\alpha + \beta u + \gamma u^2 &= \alpha + \beta(s + tu') + \gamma(s^2 + 2stu' + t^2u'^2)\\ &= \alpha + \beta s + \gamma s^2 + (\beta t + 2st\gamma)u' + t^2\gamma u'^2\\ &= \alpha' + \beta' u' + \gamma' u'^2,\end{aligned}$$

where $\alpha' = \alpha + \beta s + \gamma s^2$, $\beta' = \beta t + 2st\gamma$, and $\gamma' = t^2\gamma$, we see that $(\alpha', \beta', \gamma')$ vary over all of $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ as (α, β, γ) vary over $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$. Thus, setting $b' = \frac{b}{t^2}$, we have

$$\begin{aligned}S_{u,b} &= \{x \mapsto (\alpha + \beta u + \gamma u^2)x + b\gamma x^{q^3} : \alpha, \beta, \gamma \in \mathbb{F}_{q^2}\}\\ &= \{x \mapsto (\alpha' + \beta' u' + \gamma' u'^2)x + b'\gamma' x^{q^3} : \alpha', \beta', \gamma' \in \mathbb{F}_{q^2}\} = S_{u,b'},\end{aligned}$$

where necessarily $N(b') \notin P(u')$ by Condition (1).

Now, suppose that $u' \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and $u \neq f + gu'$ with $f, g \in \mathbb{F}_q$. Then by [12, Lemma 2.3], there exist $\ell, m, s, t \in \mathbb{F}_q$ such that $u = \frac{s+tu'}{\ell+mu'}$. From our assumption on u', we know $m \neq 0$. Moreover, $sm - \ell t \neq 0$, since otherwise substituting $s = \frac{\ell t}{m}$ into the expression for u shows that $u = \frac{t}{m} \in \mathbb{F}_q$, a contradiction.

First, let $t = 0$. Since $\{1, u', u'^2\}$ is an $\mathbb{F}_q$–basis of $\mathbb{F}_{q^3}$, there exist $A, B, C \in \mathbb{F}_q$, with $C \neq 0$, such that $u = A + Bu' + Cu'^2$. Let $\lambda = \ell + mu' \in \mathbb{F}_{q^3}$. Then the spread set

$$\lambda S_{u,b} = \{x \mapsto (\alpha + \beta + \gamma u^2)\lambda x + b\lambda\gamma x^{q^3} : \alpha, \beta, \gamma \in \mathbb{F}_{q^2}\}$$

defines a semifield isotopic to $\mathbb{S}_{u,b}$. Now

$$(\alpha + \beta u + \gamma u^2)\lambda = \alpha' + \beta' u' + \gamma' u'^2,$$

where $\alpha' = \alpha\ell + \beta s + \gamma As$, $\beta' = \alpha m + \beta t + \gamma Bs$ and $\gamma' = \gamma Cs$.

Thus we may write $\gamma = \frac{\gamma'}{Cs}$ and

$$b\lambda\gamma = b\lambda\frac{\gamma'}{Cs} = b'\gamma',$$

where $b' = \frac{b\lambda}{Cs}$. That is,

$$\lambda S_{u,b} \subseteq \{x \mapsto (\alpha' + \beta' u' + \gamma' u'^2)x + b'\gamma' x^{q^3} \,:\, \alpha', \beta', \gamma' \in \mathbb{F}_{q^2}\} = S_{u',b'}.$$

Since the two sets contain the same number of maps, we obtain $\lambda S_{u,b} = S_{u',b'}$ and $\mathbb{S}_{u,b}$ is isotopic to $\mathbb{S}_{u',b'}$.

Finally, let $t \neq 0$ and note that $u = \frac{s+tu'}{l+mu'} = \frac{t}{m} + \frac{sm-lt}{m(l+mu')} = f + gu''$, where $f = \frac{t}{m}$, $g = \frac{sm-lt}{m} \neq 0$ and $u'' = \frac{1}{l+mu'}$. By the previous cases there exist $b', b'' \in \mathbb{F}_{q^6}^*$ such that $S_{u,b} = S_{u'',b''}$ and $\mathbb{S}_{u'',b''}$ is isotopic to $\mathbb{S}_{u',b'}$. Hence $\mathbb{S}_{u,b}$ is isotopic to $\mathbb{S}_{u',b'}$, completing the proof of this part.

ii) Let $b' \in \mathbb{F}_{q^6}^*$ such that $N(b') = N(b)$. Then $b' = b\mu^{q^3-1}$, for some $\mu \in \mathbb{F}_{q^6}^*$. Letting $\bar{\mu} : x \mapsto \mu x$, we see that

$$\bar{\mu}^{-1} S_{u,b} \bar{\mu} = \{x \mapsto (\alpha + \beta u + \gamma u^2)x + b\mu^{q^3-1} x^{q^3}\} = S_{u,b'},$$

and hence $\mathbb{S}_{u,b}$ and $\mathbb{S}_{u,b'}$ are also isotopic. This completes the proof. □

Corollary 3.2. *For every odd prime power q, there is a unique semifield, up to isotopism, of order q^6 in subclass $\mathcal{F}_4^{(a)}$ which is 3-dimensional over its right nucleus and hence 6-dimensional over its middle nucleus.*

Proof. By Theorem 2.7, we know there is a semifield $\mathbb{S}$ of order q^6 in class $\mathcal{F}_4^{(a)}$ which is 3-dimensional over its right nucleus and 6-dimensional over its middle nucleus. In fact, from the proof of Theorem 2.7 we know that $\mathbb{S} = \mathbb{S}_{u,b}$ for some $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and some $b \in \mathbb{F}_{q^6}^*$, using the notation established prior to the statement of Theorem 3.1.

Now let $\mathbb{S}'$ denote any semifield of order q^6 in class $\mathcal{F}_4^{(a)}$ which is 3-dimensional over its right nucleus and 6-dimensional over its middle nucleus. By Theorem 2.2, there exists some $u' \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and some $b' \in \mathbb{F}_{q^6}^*$ such that $\mathbb{S}'$ is isotopic to the semifield $\mathbb{S}_{u',b'}$, whose multiplication is given by (4) subject to Condition (3). By part (i) of Theorem 3.1, there exists some $b'' \in \mathbb{F}_{q^6}^*$ such that $\mathbb{S}_{u',b''}$ is isotopic to $\mathbb{S}_{u,b}$. But there is a unique nonzero element in $\mathbb{F}_{q^3} \setminus P(u')$ by Theorem 2.6, and hence we must have $N(b') = N(b'')$. Therefore by part (ii) of Theorem 3.1, we know that $\mathbb{S}_{u',b'}$ is isotopic to $\mathbb{S}_{u',b''}$. Thus, by the transitivity of isotopism, we have that $\mathbb{S}'$ and $\mathbb{S}$ are isotopic, proving the result. □

Corollary 3.3. *For every odd prime power q, there is a unique semifield, up to isotopism, of order q^6 in subclass $\mathcal{F}_4^{(a)}$ which is 3-dimensional over its middle nucleus and hence 6-dimensional over its right nucleus.*

Proof. Recalling that Family $\mathcal{F}_4^{(a)}$ is closed under the transpose operation (see [14, Theorem 4.2]) and that the transpose operation interchanges the sizes of the right and middle nuclei (see [15, Prop. 4]), the result follows from Corollary 3.2. □

Corollary 3.4. *Let q be an odd prime power and let $\mathbb{S} = (\mathbb{F}_{q^6}, +, \circ)$ be a semifield of order q^6 with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$. Assume that either $\mathbb{N}_r \cong \mathbb{F}_{q^2}$ and $\mathbb{N}_m = \mathbb{F}_q$, or $\mathbb{N}_r = \mathbb{F}_q$ and $\mathbb{N}_m \cong \mathbb{F}_{q^2}$. If $\mathbb{S}$ does not not belong to class $\mathcal{F}_5$, then $\mathbb{S}$ is isotopic to either the unique semifield of Corollary 3.3 or the unique semifield of Corollary 3.2.*

Proof. Follows immediately from the above corollaries and [7, Thm. 3.5]. □

The situation for even q is quite different.

Theorem 3.5. *There is no even order semifield in subclass* $\mathcal{F}_4^{(a)}$ *which is either* 3-*dimensional over its middle nucleus or* 3-*dimensional over its right nucleus.*

Proof. Using an argument similar to that given in the proof of Corollary 3.2, the result follows from Theorem 2.2, Theorem 2.3, and Theorem 2.10. $\square$

Corollary 3.6. *Suppose that q is even and $\mathbb{S} = (\mathbb{F}_{q^6}, +, \circ)$ is a semifield of order q^6 with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$. Assume that either $\mathbb{N}_r \cong \mathbb{F}_{q^2}$ and $\mathbb{N}_m = \mathbb{F}_q$, or $\mathbb{N}_r = \mathbb{F}_q$ and $\mathbb{N}_m \cong \mathbb{F}_{q^2}$. Then $\mathbb{S}$ belongs to class $\mathcal{F}_5$.*

Proof. Follows immediately from Theorem 3.5 above and [7, Thm. 3.5]. $\square$

Remark 3.7. *It is still unknown if there exist semifields in class* $\mathcal{F}_4^{(a)}$ *that have both the right and middle nucleus equal to the center.*

The following table summarizes the state of the art on the classification project for semifields of order q^6 with $|\mathbb{N}_l| = q^3$ and $|\mathbb{K}| = q$.

Semifields of order q^6 with $|\mathbb{N}_l| = q^3$ and $|\mathbb{K}| = q$

Family	$\lvert\mathbb{N}_m\rvert$	$\lvert\mathbb{N}_r\rvert$	Existence results
$\mathcal{F}_0$	q	q	**Generalized Dickson semifields, q odd**
$\mathcal{F}_1$	q	q	**Semifields from Payne–Thas ovoid of $Q(4, 3^3)$**
$\mathcal{F}_2$	q	q	**Semifields from Ganley flock of $PG(3, 3^3)$**
$\mathcal{F}_3$	q	q	HJ semifields [9] of type II, III, IV, V for $q = 2$
$\mathcal{F}_4^{(a)}$	q^2	q	$\exists$! **semifield for q odd,** $\nexists$ **semifields for q even**
	q	q^2	$\exists$! **semifield for q odd,** $\nexists$ **semifields for q even**
	q	q	?
$\mathcal{F}_4^{(b)}$	q	q	There exist semifields for $q = 3$ [7]
$\mathcal{F}_4^{(c)}$	q	q	There exist semifields for any q [6]
	q^2	q^2	**Cyclic semifields for any q**
$\mathcal{F}_5$	q^3	q^3	**Hughes Kleinfeld semifields**
	q^3	q	**Knuth semifields of type (17) for any q**
	q	q^3	**Knuth semifields of type (19) for any q**
	q^2	q	$\exists$ for any $q \neq 2$ (e.g. Generalized Twisted Fields)
	q	q^2	$\exists$ for any $q \neq 2$ (e.g. Generalized Twisted Fields)
	q	q	$\exists$ for any $q \neq 2$ (e.g. Generalized Twisted Fields)

Some explanatory comments on the above table are needed. All the possibilities for the sizes of the middle and right nuclei of a semifield belonging to one of the families $\mathcal{F}_0$, $\mathcal{F}_1$, $\mathcal{F}_2$, $\mathcal{F}_3$, $\mathcal{F}_4^{(a)}$, $\mathcal{F}_4^{(b)}$, $\mathcal{F}_4^{(c)}$ and $\mathcal{F}_5$ are listed (these are in the middle columns).

The last column contains the known examples of semifields with the given values for the parameters, i.e. with the given orders for the nuclei. Some of them appear written in bold face, this notation meaning that such examples, up to isotopy, are uniquely determined by the orders of the nuclei. In the other cases the examples appearing are not necessarily uniquely determined.

The following open problems remain.

- Are there semifields belonging to the Family $\mathcal{F}_3$ when $q > 2$?
- Are there semifields belonging to the Family $\mathcal{F}_4^{(a)}$ having $\mathbb{N}_r$ and $\mathbb{N}_m$ both of order q?
- Are there semifields belonging to the Family $\mathcal{F}_4^{(b)}$ when $q \neq 3$?
- Are there semifields belonging to the Family $\mathcal{F}_5$ having $\mathbb{N}_r$ and $\mathbb{N}_m$ of order either q or q^2 which are not isotopic to Generalized Twisted Fields?

References

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

[2] R.H. Bruck, R.C. Bose: The construction of translation planes from projective spaces, *J. Algebra*, **1** (1964), 85–102.

[3] J. Cannon, C. Playoust: *An Introduction to MAGMA*, University of Sydney Press, Sydney, 1993.

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

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

[6] G.L. Ebert, G. Marino, O. Polverino, R. Trombetti: Infinite families of new semifields, to appear in *Combinatorica*.

[7] G.L. Ebert, G. Marino, O. Polverino, R. Trombetti: On the multiplication of some semifields of order q^6, *Finite Fields and Their Applications*, **15** n.2 (2009), pp. 160–173.

[8] J.W.P. Hirschfeld: *Projective geometries over finite fields*, Clarendon Press, Oxford, 1979, 2nd Edition, 1998.

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

[10] J.W.P. Hirschfeld, G. Korchmáros, F. Torres: *Algebraic Curves over a Finite Field*, Princeton University Press, New Jersey, 2008.

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

[12] N. L. Johnson, G. Marino, O. Polverino, R. Trombetti: Semifields of order q^6 with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$, *Finite Fields and Their Applications*, **14** n.2 (2008), 456–469.

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

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

[15] D.M. Maduram: Transposed Translation Planes, *Proc. Amer. Math. Soc.*, **53** (1975), 265–270.

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

[17] M. Moisio: Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, *Acta Arith.*, **132** n.4 (2008), 329–350.

[18] O. Polverino: Linear sets in Finite Projective Spaces, submitted.

[19] A. Seidenberg: *Elements of the theory of Algebraic Curves*, Addison–Wesley Publishing Company, USA, 1968.