Received <day> <Month>, <year>; | Revised <day> <Month>, <year>; | Accepted <day> <Month>, <year>

DOI: xxx/xxxx

ARTICLE TYPE

On finite division rings with a designed automorphism group

Elías F. Combarro[1] | Alejandro P. Nicolás[2] | José Ranilla[1] | I.F. Rúa[2]

[1] Computer Science Department, University of Oviedo, Spain
[2] Mathematics Department, University of Oviedo, Spain

Abstract

Nonassociative algebras play a fundamental role in the description of physical systems. Symmetry is related to the transformations of these algebras, which are controlled by their automorphisms group. Starting from the known structure of finite division ring with 64 elements, we construct some nonassociative finite division algebras of orders 256 and 512 with a designed automorphism group.

KEYWORDS:
Finite Semifield; Projective planes; Automorphism Group

1 | INTRODUCTION

Nonassociative algebras play a fundamental role in Physics and Communications. For instance, Lie and Jordan algebras provide the mathematical structure of Quantum Mechanics, while finite nonassociative division rings have applications on coding theory[4,8,6], combinatorics and graph theory[13]. On the other hand, the symmetry of these objects can be related with several properties, as conservation laws and invariances in Physics. In this context, symmetries can be seen as transformation of the structure into itself and so, its group of automorphisms gives information about the behaviour of this kind of objects.

During the last few years, computational efforts in order to clasify some of these objects have been made. For instance, the classification of finite division rings, also called semifields, with 64 elements is completely known,[16], as well as those with 243 elements,[17]. However, many questions are open yet: there is not a classification of semifields with 128 or 256 elements, despite of the powerful computers available nowadays.

The knowledge of the structure of these concrete division rings can inspire new general constructions, as suggested in[9]. In this sense, the work of Lavrauw and Sheekey[11] gives examples of constructions of semifields which are neither twisted fields nor two-dimensional over a nucleus starting from the classification of semifields with 64 elements. In particular, these are the rings labelled as XIV, XXIV, XXVI and XXVII in[16]. On the other hand, the construction of finite division rings with a prescribed automorphism group has been carried out in references such as[3] and[14].

The present work is motivated by the behaviour of some division rings with 64 elements which also appear in the classification of[16]. In particular, semifields coordinatizing 18 planes in the Knuth classes XVII and XVIII and 27 in the Knuth class XXXIX (see Table 5 of[16]) have an automorphism group isomorphic to the group C_5. Notice that the order of this group, 5, and the dimension of the semifields over their center, 6, are relatively prime (a fact that differs completely from the situation of the finite field $\mathbb{F}_{64}$).

We will see in the next section that all these rings can be additively described as a direct sum of two Galois fields of orders 4 and 16. Moreover, some of them can be seen as a 3−dimensional vector spaces over a so called weak nucleus, see[10].

In the last part of the paper, we will use this concept in order to generalize the construction of such division rings. Exploring these ideas, we will be able to construct sporadic examples of semifields with 256 and 512 elements whose automorphism groups contain a subgroup of prescribed structure. These rings are new, since they do not fall in the Knuth orbit of any finite semifield either listed in[12] or contructed by[18].

2 | DIVISION RINGS OF ORDER 64 WITH A CYCLIC AUTOMORPHISM GROUP C_5

In this section we will study the structure of a division ring, i.e. a semifield, S with 64 elements with cyclic automorphism group C_5. First of all, observe that the center of any such a finite semifield contains $\mathbb{F}_2 = \{0, 1\}$, and S is naturally a 6-dimensional $\mathbb{F}_2-$algebra. We will prove that it is possible to find a set of 4 elements fixed by the action of the automorphism group, which yields an alternative additive decomposition of S.

Theorem 1. Let $(S, +, *)$ be a semifield with 64 elements and automorphism group $\mathrm{Aut}(S) = \langle\varphi\rangle$ isomorphic to C_5. Then, there exists an element $a \neq 0, 1$, such that $(\{0, 1, a, a + 1\}, +, *)$ is a semifield isomorphic to $\mathbb{F}_4$ which is fixed by the automorphism group. Moreover, there exists an element $b \in S \setminus \{0, 1, a, a + 1\}$ such that $(\{\varphi^i(b) \mid i \in \mathbb{N}\}, +, \cdot)$, with $\varphi^i(b) \cdot \varphi^j(b) = \varphi^{i+j}(b)$, is isomorphic to the finite field $\mathbb{F}_{16}$. So, S can be seen as a $\mathbb{F}_2$-vector space isomorphic to the direct sum $\mathbb{F}_4 \oplus \mathbb{F}_{16}$, with basis $\{1, a, b, \varphi(b), \varphi^2(b), \varphi^3(b)\}$.

Proof. Let us consider the set $\mathrm{Fix}(\varphi) = \{x \in S \mid \varphi(x) = x\}$ of fixed points under the action of $\mathrm{Aut}(S)$ over S. Since $|\mathrm{Aut}(S)| = 5$, we have $64 \neq |\mathrm{Fix}(\varphi)| \equiv 64 \pmod 5$. So, $|\mathrm{Fix}(\varphi)| = 4$ and, because there is a unique semifield with four elements, $(\mathrm{Fix}(\varphi), +, *) \cong \mathbb{F}_4$. Therefore, we can find an element $a \in S \setminus \{0, 1\}$ such that $\mathrm{Fix}(\varphi) = \{0, 1, a, a + 1\}$.

Since $\varphi \neq I = \varphi^5$ and $x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$, then the $\mathbb{F}_2$-irreducible polynomial $x^4 + x^3 + x^2 + x + 1$ divides the minimal polynomial of φ. So, there exist an element $b \in S \setminus \{0, 1, a, a + 1\}$ such that the $\mathbb{F}_2[x]-$cyclic submodule generated by b, $\langle b, \varphi(b), \varphi^2(b), \varphi^3(b)\rangle_{\mathbb{F}_2}$, is isomorphic to $\mathbb{F}_2[x]/\langle x^4 + x^3 + x^2 + x + 1\rangle \cong \mathbb{F}_{16}$.

Finally, notice that $\dim_{\mathbb{F}_2} S = 6$, so the set $\{1, a, b, \varphi(b), \varphi^2(b), \varphi^3(b)\}$, which is linearly independent over $\mathbb{F}_2$, is an $\mathbb{F}_2-$basis of S.

□

Remark 1. The decomposition of S as $\mathbb{F}_4 \oplus \mathbb{F}_{16}$ corresponds to the $\mathbb{F}_2-$module decomposition $\left(\mathbb{F}_2[x]/\langle x + 1\rangle\right)^2 \oplus \mathbb{F}_2[x]/\langle x^4 + x^3 + x^2 + x + 1\rangle$ and that φ preserves this decomposition. Notice that the restriction of the product $*$ of S to $\mathrm{Fix}(\varphi)$ is the product of the field $\mathbb{F}_4$, but this does not happen with $\mathbb{F}_{16}$. However, $\xi = \varphi(b) \in \mathbb{F}_{16}$ can be identified with a $5th-$primitive root of unity, and it can be assumed that the action of the automorphism φ over the elements of $\mathbb{F}_{16}$ is given by $\varphi(c) = \xi \cdot c$ for all $c \in \mathbb{F}_{16}$. From now on we shall simply write ξc instead of $\xi \cdot c$.

The next step in the description of semifields with 64 elements with cyclic automorphism group C_5 consists on the introduction of the definition of weak nucleus in the sense of[10].

Definition 1. Let $(S, +, *)$ be a semifield and let $\mathbb{F} \subseteq S$ be a field. Then, $\mathbb{F}$ is a weak nucleus for S if $(a * b) * c = a * (b * c)$ whenever any two of a, b, c are in $\mathbb{F}$.

Notice that if there exists a weak nucleus $\mathbb{F}$ of S, then S can be written as an $\mathbb{F}$-vector space. However, right and left multiplications ($R_a(x) = x * a$, $L_a(x) = a * x$, for all $a, x \in S$) will not be, in general, $\mathbb{F}$-linear transformations. Moreover, the weak nucleus is generally not preserved by isotopy.

In order to describe the structure of the semifields with weak nucleus presented in this section, we need the following result, which will be stated without proof.

Lemma 1. [Theorem 4.1 of[15]] Let $R = GR(q^d, p^d)$ be a Galois ring of order q^d and characteristic p^d (in particular a finite field). For any finite (R, R)-bimodule ${}_RM_R$ there exist a generator system $\{\mu_1, \dots, \mu_k\}$ (called distinguished basis) and a system of automorphism $\sigma_1, \dots, \sigma_k \in Aut(R)$ such that

$$\forall a \in R, l \in \{1, \dots, k\} \,:\; \mu_l a = \sigma_l(a)\mu_l \text{ and } M = R\mu_1 \oplus \cdots \oplus \mu_k$$

is a direct sum of cyclic (R, R)-bimodules.

Theorem 2. Let $(S, +, *)$ be a semifield with 64 elements, automorphism group $\mathrm{Aut}(S) = \langle\varphi\rangle \cong C_5$ and weak nucleus $\mathbb{F} = \mathrm{Fix}(\varphi) \cong \mathbb{F}_4$. Then, there exists an element $\lambda \in S$ such that $\{1, \lambda, \varphi(\lambda)\}$ is an $\mathbb{F}_4$-basis of S. Moreover, either $a * \lambda = \lambda * a$ for all $a \in \mathbb{F}$, and the basis is called of *type A*, or $a * \lambda = \lambda * a^2$ for all $a \in \mathbb{F}$, and it is called of *type B*.

Proof. From Definition 1, it follows that the semifield S is a bimodule over the weak nucleus $\mathbb{F}$. So, by Lemma 1, there exists a distinguished $\mathbb{F}$-basis of S, that is, it is possible to find an $\mathbb{F}$-basis $\{s_1, s_2, s_3\}$ of S such that, for $1 \leq i \leq 3$, $a * s_i = s_i * \sigma_i(a)$, with $\sigma_i \in \mathrm{Aut}(\mathbb{F})$, for all $a \in \mathbb{F}$. Notice that we can always take $s_1 = 1$ and $\sigma_1 = Id$. If $s_i = 1$ for some i, the claim is trivial. Otherwise, it suffices to see that $\{1, s_2, s_3\}$ is a generator system from S whith $a * 1 = 1 * a$ for all $a \in \mathbb{F}$.

Let us denote the element s_2 by λ. Suppose that $\sigma_2 = Id$ and so, $a * \lambda = \lambda * a$ for all $a \in \mathbb{F}$. Since S is isomorphic, as $\mathbb{F}_2-$vector space, to the direct sum $\mathbb{F} \oplus \mathbb{F}_{16}$, we can assume that $\lambda \in \mathbb{F}_{16}$. Otherwise, $\lambda = A + B$, with $A \in \mathbb{F}$ and $B \in \mathbb{F}_{16}$, and $\{1, \lambda - A, s_3\}$ is also a distinguished $\mathbb{F}$-basis of S. Under these assumptions, we claim that $\{1, \lambda, \varphi(\lambda)\}$ is an $\mathbb{F}-$distinguished basis of S. Since $\lambda \in \mathbb{F}_{16}$, the minimal polynomial $\varphi-$annihilating λ is $x^4 + x^3 + x^2 + x + 1$, i.e, $\sum_{k=0}^{4} \varphi^k(\lambda) = 0$. Let us suppose that the system $\{1, \lambda, \varphi(\lambda)\}$ is not $\mathbb{F}$-linearly independent. In such case, we can find $c_1, c_2 \in \mathbb{F}$ such that $\varphi(\lambda) = c_1 + c_2\lambda$. This implies that $\varphi^k(\lambda) = c_1 + c_2\varphi^{k-1}(\lambda)$ for all $k \in \mathbb{N}$ and so we have

$$0 = \sum_{k=1}^{5} \varphi^k(\lambda) = c_1 + c_2 \sum_{k=1}^{5} \varphi^{k-1}(\lambda) = c_1,$$

that is, $\varphi(\lambda) - c_2\lambda = 0$, and so $x^4 + x^3 + x^2 + x + 1$ divides $x - c_2$, a contradiction. Now, it is easy to check that $\{1, \lambda, \varphi(\lambda)\}$ is a distinguished basis and thus the claim is proved. The case $\sigma_3 = Id$ is handled similarly.

Finally, suppose that $\sigma_2(a) = \sigma_3(a) = a^2$ for all $a \in \mathbb{F}$. Consider $s_2 = A_2 + B_2$ and $s_3 = A_3 + B_3$ with $A_i \in \mathbb{F}$ and $B_i \in \mathbb{F}_{16}$, for $i = 2, 3$. If $A_2 = 0$ (resp. $A_3 = 0$), we can take $\lambda = s_2 \in \mathbb{F}_{16}$ (resp. $\lambda = s_3 \in \mathbb{F}_{16}$) and, repeating the argument used when $\sigma_2 = Id$, we can prove that $\{1, \lambda, \varphi(\lambda)\}$ is a distinguished $\mathbb{F}$-basis of S. Otherwise, $A_2 \neq 0$, $A_3 \neq 0$ and we can take $0 \neq \lambda = A_2^{-1} * s_2 + A_3^{-1} * s_3 = A_2^{-1} * B_2 + A_3^{-1} * B_3 \in \mathbb{F}_{16}$ (observe that $\mathbb{F}$ is a weak nucleus and $a * \lambda = \lambda * a^2$ for all $a \in \mathbb{F}$). Using the previous argument, $\{1, \lambda, \varphi(\lambda)\}$ can be shown to be a distinguished $\mathbb{F}$-basis of S.

□

We are able now to describe the product $*$ of the semifield S. First of all, from the previous result, we know that, if $\mathbb{F}$ is a weak nucleus of S, there exists a distinguished $\mathbb{F}$-basis $\{1, \lambda, \varphi(\lambda)\}$ of S. So, S can be seen as the direct sum of the weak nucleus $\mathbb{F}$, fixed by φ, and the $\mathbb{F}$-bimodule $L = \langle \lambda, \varphi(\lambda)\rangle_{\mathbb{F}}$, which is invariant under φ. Thus, any element $s \in S$ can be written as a sum $s = s_1 + s_2$ with $s_1 \in \mathbb{F}$ and $s_2 \in \langle \lambda, \varphi(\lambda)\rangle_{\mathbb{F}}$. It is straightforward to see that, if $a \in \mathbb{F}$, then $a * s = a * (s_1 + s_2) = s_1 * a + s_2 * \sigma(a)$, where σ is the automorphism of $\mathbb{F}$ associated with elements $\{\lambda, \varphi(\lambda)\}$ of the distinguished basis. Also, $\varphi(s_1 + s_2) = s_1 + \varphi(s_2)$. Taking these ideas into account, we can deduce the following result.

Theorem 3. Let $(S, +, *)$ be a semifield with 64 elements and automorphism group $\mathrm{Aut}(S) = \langle \varphi \rangle$ isomorphic to C_5. Let us suppose that $\mathbb{F} = \mathrm{Fix}(\varphi) \cong \mathbb{F}_4$ is a weak nucleus for S and that $\{1, \lambda, \varphi(\lambda)\}$ is a distinguished $\mathbb{F}$-basis of S with associated automorphism σ. If $S \cong \mathbb{F} \oplus L$, with $L \cong \mathbb{F}_{16}$, then there exist two $\mathbb{F}_2$-bilinear functions $F : \mathbb{F}_{16} \times \mathbb{F}_{16} \to \mathbb{F}_4$ and $G : \mathbb{F}_{16} \times \mathbb{F}_{16} \to \mathbb{F}_{16}$ satisfying $F(\varphi(b), \varphi(d)) = F(b, d)$ and $G(\varphi(b), \varphi(d)) = \varphi(G(b, d))$ for all $b, d \in L$, such that

$$(a + b) * (c + d) = (a * c + F(b, d)) \ + \ (a * d + \sigma(c) * b + G(b, d)).$$

Proof. Since the product $*$ is distributive, it is clear that

$$(a + b) * (c + d) = a * c + a * d + b * c + b * d = a * c + a * d + \sigma(c) * b + b * d.$$

Notice that the product $a * c \in \mathbb{F}$, and that $b * c = \sigma(c) * b$, since L has a distinguished basis associated with the automorphism σ. Let the product $b * d$ be $F(b, d) + G(b, d)$, where $F : L \times L \to F$ and $G : L \times L \to L$ must be $\mathbb{F}_2$-bilinear functions, since $*$ is distributive and the centre of S is $\mathbb{F}_2$. Thus, we arrive to

$$(a + b) * (c + d) = (a * c + F(b, d)) \ + \ (a * d + \sigma(c) * b + G(b, d)).$$

Since φ is an automorphism of S, the relation $\varphi(a + b) * \varphi(c + d) = \varphi((a + b) * (c + d))$ holds. Expanding this equation and using $a, c, \sigma(c) \in \mathrm{Fix}(\varphi)$, we arrive at

$$F(\varphi(b), \varphi(d)) + G(\varphi(b), \varphi(d)) = \varphi(F(b, d)) + \varphi(G(b, d)),$$

but $F(b, d) \in \mathbb{F}$, which is fixed by φ. So, we have

$$F(\varphi(b), \varphi(d)) + F(b, d) = G(\varphi(b), \varphi(d)) + \varphi(G(b, d)).$$

The sum $\mathbb{F} \oplus L$ is direct and L is invariant under φ, so $\mathbb{F} \cap L = 0$ and the result follows. □

As a consequence of this result, we can deduce the form of the functions F and G.

Corollary 1. The $\mathbb{F}_2$-bilinear function $G : \mathbb{F}_{16} \times \mathbb{F}_{16} \to \mathbb{F}_{16}$ of Theorem 3 is of the form

$$G(b, d) = \sum_{i=0}^{3} \sum_{j=0}^{3} g_{ij}\, b^{2^i} d^{2^j},$$

with $g_{ij} \in \mathbb{F}_{16}$ for all $0 \leq i, j \leq 3$. Moreover, g_{ij} must be 0 for all $0 \leq i, j \leq 3$ such that $2^i + 2^j \not\equiv 1 \mod 5$.

Proof. For each $b \in \mathbb{F}_{16}$ consider the $\mathbb{F}_2$-linear application $G_b : \mathbb{F}_{16} \to \mathbb{F}_{16}$ defined by $G_b(d) = G(b, d)$ for all $d \in \mathbb{F}_{16}$. From Theorem 2.1 of[2], $G_b(d) = \sum_{j=0}^{3} g_j(b)\, d^{2^j}$. Now, notice that, for each $0 \leq j \leq 3$, $g_j : \mathbb{F}_{16} \to \mathbb{F}_{16}$ is $\mathbb{F}_2$-linear, so $g_j(b) = \sum_{i=0}^{3} g_{ij}\, b^{2^i}$. Thus, $G(b, d) = \sum_{i=0}^{3} \sum_{j=0}^{3} g_{ij}\, b^{2^i} d^{2^j}$.

From Theorem 3, we know that $\varphi(G(b, d)) = G(\varphi(b), \varphi(d))$ for all $b, d \in \mathbb{F}_{16}$. Using Remark 1, this condition can be rewrite as $\xi\, G(b, d) = G(\xi\, b, \xi\, d)$, with ξ a $5th-$primitive root of unity. That is,

$$\xi \left(\sum_{i=0}^{3} \sum_{j=0}^{3} g_{ij}\, b^{2^i} d^{2^j} \right) = \sum_{i=0}^{3} \sum_{j=0}^{3} g_{ij} \xi^{2^i + 2^j}\, b^{2^i} d^{2^j},$$

which implies $g_{ij} \xi^{2^i + 2^j - 1} = g_{ij}$ for all $1 \leq i, j \leq 3$. So, $g_{ij} = 0$ whenever $2^i + 2^j \not\equiv 1 \mod 5$. □

Corollary 2. The $\mathbb{F}_2$-bilinear function $F : \mathbb{F}_{16} \times \mathbb{F}_{16} \to \mathbb{F}_4$ of Theorem 3 is of the form

$$F(b, d) = \sum_{i=0}^{3} \sum_{j=0}^{1} \mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{16}}(f_{ij}\, b^{2^i} d^{2^j}),$$

with $f_{ij} \in \mathbb{F}_{16}$ for all $0 \leq i, j \leq 3$. Moreover, f_{ij} must be 0 for all $0 \leq i \leq 3$, $0 \leq j \leq 1$ such that $2^i + 2^j \not\equiv 0 \mod 5$.

Proof. Since $F : \mathbb{F}_{16} \times \mathbb{F}_{16} \to \mathbb{F}_4$ is $\mathbb{F}_2$-linear, $F(b, d) = \sum_{i=0}^{3} \sum_{j=0}^{3} f_{ij}\, b^{2^i} d^{2^j}$. For each $b, d \in \mathbb{F}_{16}$, $F(b, d) \in \mathbb{F}_4$ if and only if $F(b, d)^4 = F(b, d)$, that is, if and only if

$$\sum_{i=0}^{3} \sum_{j=0}^{3} f_{i-2\, j-2}^4\, b^{2^i} d^{2^j} = \sum_{i=0}^{3} \sum_{j=0}^{3} f_{ij}\, b^{2^i} d^{2^j},$$

where i, j are taken modulo 4. Thus, $f_{ij} = f_{i-2\, j-2}^4$ for all $0 \leq i \leq 3$, $0 \leq j \leq 3$ and so

$$F(b, d) = \sum_{i=0}^{3} \sum_{j=0}^{1} \left(f_{ij}\, b^{2^i} d^{2^j} + f_{i+2\, j+2}\, b^{2^{i+2}} d^{2^{j+2}} \right) =$$

$$= \sum_{i=0}^{3} \sum_{j=0}^{1} \left(f_{ij}\, b^{2^i} d^{2^j} + f_{ij}^4\, (b^{2^i})^4 (d^{2^j})^4 \right) = \sum_{i=0}^{3} \sum_{j=0}^{1} \mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{16}}(f_{ij}\, b^{2^i} d^{2^j}).$$

From Theorem 3, we know that $F(b, d) = F(\varphi(b), \varphi(d))$ for all $b, d \in \mathbb{F}_{16}$. Using Remark 1, this condition can be rewrite as $F(b, d) = F(\xi\, b, \xi\, d)$, with a ξ a $5th-$primitive root of unity. That is,

$$\sum_{i=0}^{3} \sum_{j=0}^{1} \left(f_{ij}\, b^{2^i} d^{2^j} + f_{ij}^4\, b^{2^{i+2}} d^{2^{j+2}} \right) = \sum_{i=0}^{3} \sum_{j=0}^{1} \left(f_{ij} \xi^{2^i + 2^j}\, b^{2^i} d^{2^j} + f_{ij}^4 \xi^{2^{i+2} + 2^{j+2}}\, b^{2^{i+2}} d^{2^{j+2}} \right),$$

which implies $f_{ij} \xi^{2^i + 2^j} = f_{ij}$ for all $1 \leq i \leq 3$, $0 \leq j \leq 1$. So, $f_{ij} = 0$ whenever $2^i + 2^j \not\equiv 0 \mod 5$.

□

From the computational classification of[16], it can be checked that there exist 33 non isomorphic semifields $(S, +, *)$ with 64 elements, automorphism group isomorphic to C_5 and weak nucleus $\mathbb{F}_4$. Twelve of them are of type A and 21 of type B. The semifields of type A are distributed in 4 different planes lying in the Knuth classes XVII and XVIII of[16], whereas the other ones coordinatize 5 planes in the Knuth classes XVIII and XXXIX of[16].

From Corollaries 1 and 2 we know that

$$F(b, d) = \mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{16}}(f_{02} b d^4 + f_{13} b^2 d^8),\ G(b, d) = g_{21} b^4 d^2 + g_{12} b^2 d^4 + g_{33} b^8 d^8.$$

The actual parameters for the different types and planes are shown in Table 1 . The element $\alpha \in \mathbb{F}_{16}$ is a primitive 15-th root of unity satisfying $\alpha^4 + \alpha + 1 = 0$.

Except for the plane 7, all these semifields have an isotopy (H, J, K) of order 3 which commutes with the automorphism of order 5. In such case, 15 must divide the order of the autotopism group. In agreement with[16], for the Knuth classes XVII and XVIII, this group has order 15 and so, it must be generated by the automorphism of order 5 and the isotopy (H, J, K). For the Knuth class XXXIX, the autotopism group has order 5 and so it must be generated only by the automorphism.

	Type A			Type B		
Knuth class	Plane	F	G	Plane	F	G
XVII	1	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{16}}(\alpha^8 bd^4 + \alpha^9 b^2 d^8)$	$\alpha b^8 d^8$			
	2	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{16}}(\alpha^7 bd^4 + \alpha b^2 d^8)$	$\alpha b^8 d^8$			
XVIII	3	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{16}}(\alpha^5 b^2 d^8)$	$b^4 d^2 + \alpha b^2 d^4$	5	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{16}}(\alpha^5 bd^4)$	$\alpha b^2 d^4 + b^8 d^8$
	4	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{16}}(\alpha^5 b^2 d^8)$	$\alpha b^4 d^2 + b^2 d^4$	6	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{16}}(\alpha^{10} b^2 d^8)$	$\alpha b^4 d^2 + b^8 d^8$
				7	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{16}}(\alpha^{10} b^2 d^8)$	$b^4 d^2 + \alpha^8 b^8 d^8$
				8	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{16}}(bd^4)$	$\alpha^5 b^2 d^4 + \alpha b^8 d^8$
XXXIX				9	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{16}}(\alpha^8 bd^4 + \alpha^2 b^2 d^8)$	$b^4 d^2 + b^2 d^4 + \alpha b^8 d^8$

TABLE 1 Functions F and G of semifields of order 64 with automorphism group isomorphic to C_5 and weak nucleus $\mathbb{F}_4$.

The different values for the triplets (H, J, K) can be seen in Table 2 . The element $\beta \in \mathbb{F}_4$ is a primitive 3-th root of unity satisfying $\beta^2 + \beta + 1 = 0$.

Type A				Type B			
Plane	$H(a,b)$	$J(c,d)$	$K(e,f)$	Plane	$H(a,b)$	$J(c,d)$	$K(e,f)$
1	$(\beta a, \beta b)$	$(\beta^2 c, \beta^2 d)$	(e, f)	5	$(\beta a, \beta^2 b)$	$(\beta c, d)$	$(\beta^2 e, \beta f)$
2	$(\beta^2 a, \beta b)$	$(\beta^2 c, \beta d)$	$(\beta e, f)$	6	$(\beta a, b)$	$(\beta c, \beta d)$	$(\beta^2 e, \beta^2 f)$
3	$(\beta a, \beta b)$	$(\beta^2 c, \beta^2 d)$	(e, f)	8	$(\beta a, b)$	$(\beta c, \beta d)$	$(\beta^2 e, \beta^2 f)$
4	$(\beta^2 a, \beta b)$	$(\beta^2 c, \beta d)$	$(\beta e, f)$	9	$(\beta a, \beta^2 b)$	$(\beta c, d)$	$(\beta^2 e, \beta f)$

TABLE 2 Isotopy (H, J, K) of order 3 for semifields of order 64 with automorphism group isomorphic to C_5.

3 | EXTENDING THE CONSTRUCTION: SPORADIC FINITE SEMIFIELDS OF ORDERS 256 AND 512

In this section, we introduce some examples of sporadic semifields constructed from a weak nucleus and a cyclic automorphism group. The starting point are the semifields of 64 elements studied in the previous section.

Let $\mathbb{F} = \mathbb{F}_{2^n}$ with $n \in \{2, 3\}$. We want to construct semifields S from the direct product of the field $\mathbb{F}$, which will be a weak nucleus for S, and the field $\mathbb{K} = \mathbb{F}_{2^{nk}}$ for different values of k. Notice that $\mathbb{F}$ is a subfield of $\mathbb{K}$ and so $\mathbb{K}$ can be seen as a vector space over $\mathbb{F}$. Let us consider $\xi \in \mathbb{K}$ an $s-$th primitive root of unity for an appropriate $s \mid 2^{nk} - 1$. Let $(S, +)$ be the direct product of the additive groups $(\mathbb{F}, +)$ and $(\mathbb{K}, +)$, that is $S = \mathbb{F} \times \mathbb{K}$. Inspired by the behaviour of the semifields of 64 elements studied in the previous section, we define a product $*$ in $(S, +, \cdot)$ in the following way

$$(a, b) * (c, d) = (a \cdot c + F(b, d)\ ,\ a \cdot d + \sigma(c) \cdot b + G(b, d)), \tag{1}$$

where $\sigma \in \mathrm{Aut}(\mathbb{F})$ and $F : \mathbb{K} \times \mathbb{K} \to \mathbb{F}$ and $G : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ are $\mathbb{F}_2$-bilinear functions. It is easy to see that $*$ is a well-defined distributive product due to the $\mathbb{F}_2$-bilinearity of F and G. Moreover, the element $(1, 0)$ is an identity for $*$.

The ring $(S, +, *)$ will be a semifield if and only if there are no zero divisors for the product $*$. From now on, let us suppose that $(S, +, *)$ is a semifield. Then, we can prove some facts about the structure of S.

Proposition 1. Let $(S, +, *)$ be a semifield with multiplication defined by (1). Then, the field $\mathbb{F}$ is a weak nucleus for S.

Proof. Since $S = \mathbb{F}\times\mathbb{K}$, we identify the field $\mathbb{F}$ with the elements $(a, 0) \in S$, which clearly is a subfield of S. From the definition of the product $*$, and using the fact that F and G are $\mathbb{F}_2$ bilinear functions, we have that

$$\begin{aligned}\big((a_1,0) * (a_2,0)\big) * (c_1,c_2) &= \big((a_1 \cdot a_2) \cdot c_1, (a_1 \cdot a_2) \cdot c_2\big)\\ (a_1,0) * \big((a_2,0) * (c_1,c_2)\big) &= \big(a_1 \cdot (a_2 \cdot c_1), a_1 \cdot (a_2 \cdot c_2)\big)\end{aligned}$$

The equality $\big((a_1,0) * (a_2,0)\big) * (c_1,c_2) = (a_1,0) * \big((a_2,0) * (c_1,c_2)\big)$ comes from the associativity of the product of the field $\mathbb{K}$. Notice that, since $\mathbb{F}$ is a subfield of $\mathbb{K}$, we can see the product of $\mathbb{F}$ as the restriction of the product of $\mathbb{K}$.

In a similar way, since $\sigma \in \mathrm{Aut}(\mathbb{F})$, we can see that

$$\begin{aligned}\big((a_1,0) * (b_1,b_2)\big) * (a_2,0) &= (a_1,0) * \big((b_1,b_2) * (a_2,0)\big)\\ \big((b_1,b_2) * (a_1,0)\big) * (a_2,0) &= (b_1,b_2) * \big((a_1,0) * (a_2,0)\big)\end{aligned}$$

So, $\mathbb{F}$ is a weak nucleus for S. □

Using the same arguments presented in Corollaries 1 and 2, it is easy to see that the $\mathbb{F}_2$-bilinear functions F and G must have the following form

$$F(b,d) = \textstyle\sum_{i=0}^{nk-1} \sum_{j=0}^{n-1} \mathrm{Tr}_{\mathbb{F}}^{\mathbb{K}}(f_{ij}\, b^{2^i} d^{2^j}),\ G(b,d) = \sum_{i=0}^{nk-1} \sum_{j=0}^{nk-1} g_{ij}\, b^{2^i} d^{2^j}. \tag{2}$$

Let $\varphi : S \to S$ be the map defined by $\varphi(a,b) = (a, \xi \cdot b)$ for all $(a,b) \in S$. We can ensure that φ is an automorphism of the semifield $(S,+,*)$ provided that the functions F and G satisfy certain conditions.

Proposition 2. Let $(S,+,*)$ be the semifield with multiplication defined by (1). The map $\varphi : S \to S$ defined by $\varphi(a,b) = (a, \xi \cdot b)$ is an automorphism of $(S,+,*)$ if and only if $F(\xi \cdot b, \xi \cdot d) = F(b,d)$ and $G(\xi \cdot b, \xi \cdot d) = \xi \cdot G(b,d)$ for all $(b,d) \in S$.

Proof. First of all, we will prove that φ is bijective. Notice that if $\varphi(a,b) = \varphi(c,d)$ then $a = c$ and $\xi \cdot (b-d) = 0$, which implies $b = d$. Therefore, φ is injective and so bijective by finiteness.

Now, we will prove that φ is an homomorphism of $(S,+,*)$. Notice that

$$\varphi((a,b) + (c,d)) = \varphi(a+c, b+d) = (a+c\ ,\ \xi \cdot (b+d)) = \varphi(a,b) + \varphi(c,d).$$

From the definition of the product $*$, we have

$$\varphi((a,b) * (c,d)) = (a \cdot c + F(b,c)\ ,\ \xi \cdot (a \cdot d + \sigma(c) \cdot b + G(b,d))).$$

On the other hand,

$$\varphi(a,b) * \varphi(c,d) = (a \cdot c + F(\xi \cdot b, \xi \cdot d)\ ,\ a \cdot (\xi \cdot d) + \sigma(c) \cdot (\xi \cdot b) + G(\xi \cdot b, \xi \cdot d)).$$

Which leads to $F(\xi \cdot b, \xi \cdot d) = F(b,d)$ and $G(\xi \cdot b, \xi \cdot d) = \xi \cdot G(b,d)$ for all $(b,d) \in S$. The converse is trivial. □

Corollary 3. If φ is an isomorphism of $(S,+,*)$ with multiplication defined by (1), then f_{ij} must be 0 for all $0 \le i \le nk-1$ and $0 \le j \le n-1$ such that $2^i + 2^j \not\equiv 0 \bmod s$. Moreover, $g_{ij} = 0$ for all $0 \le i, j \le nk-1$ such that $2^i + 2^j \not\equiv 1 \bmod s$.

Proof. It suffices to apply the same argument of Corollaries 1 and 2, taking into account that the multiplicative order of ξ is s. □

Now, we will analyse which conditions must verify the $\mathbb{F}_2$-bilinear functions F and G in order to make $(S,+,*)$ a semifield. That is, in order to avoid zero divisors for the product $*$. In particular, we will apply the techniques presented in[10].

We start from the expression of the product $*$, that is

$$(a,b) * (c,d) = (a \cdot c + F(b,d)\ ,\ a \cdot d + \sigma(c) \cdot b + G(b,d)).$$

Recall that $a, c \in \mathbb{F}$ whereas $b, d \in \mathbb{K}$. We get a zero divisor when $(a,b) * (c,d) = (0,0)$ but neither $(a,b) = (0,0)$ nor $(c,d) = (0,0)$. In such case, we arrive at the following equations

$$\begin{aligned} a \cdot c + F(b,d) &= 0,\\ a \cdot d + \sigma(c) \cdot b + G(b,d) &= 0.\end{aligned}$$

Let us suppose that $a \cdot c \neq 0$. So, there exists an element $x \in \mathbb{F}$ such that $a = x \neq 0$ and $c = x^{-1} \cdot F(b,d)$. Substitution in the other equation leads us to

$$x \cdot d + \sigma(x)^{-1} \cdot \sigma(F(b,d)) \cdot b + G(b,d) = 0.$$

This expression can be transformed into the following one

$$d \cdot \sigma(x) \cdot x + G(b, d) \cdot \sigma(x) + \sigma(F(b, d)) = 0, \tag{3}$$

which can be seen as a set of polynomials in $\mathbb{K}[x]$. Thus, if any of these polynomials has a root in $\mathbb{F}$, then we can ensure that there exists a zero divisor in S. The converse is also true. That is, if there exist elements (a, b) and (c, d) such that $(a, b) * (c, d) = (0, 0)$ with $a \cdot c \neq 0$, then it is easy to see that $x = a \in \mathbb{F}$ is a root of the polynomial

$$d \cdot \sigma(x) \cdot x + G(b, d) \cdot \sigma(x) + \sigma(F(b, d))$$

for certain values of b and d.

If $a \cdot c = 0$, then we have $F(b, d) = 0$ and either $a = 0$ or $c = 0$. In such case, there exists a zero divisor if the equation $\sigma(c) \cdot b + G(b, d) = 0$ has a solution with $b \neq 0$, or if $a \cdot d + G(b, d) = 0$ for some $d \neq 0$.

We have constructed some examples of new semifields starting from a weak nucleus $\mathbb{F}$ with a designed automorphism φ. In particular, we have chosen $\mathbb{F}$ to be the field $\mathbb{F}_4$ or $\mathbb{F}_8$ whereas the field $\mathbb{K}$ is given by an extension of $\mathbb{F}$. The most difficult step consists on the verification of the absence of zero divisors. For doing that, the previous techniques were applied with the help of Magma,[1]. Our results are summarized in Table 3 .

$\mathbb{F} \setminus \mathbb{K}$	$\mathbb{F}_4$	$\mathbb{F}_8$	$\mathbb{F}_{16}$	$\mathbb{F}_{64}$	$\mathbb{F}_{256}$
$\mathbb{F}_4$	$\varphi^3 = 1$ $\sigma(a) = a^2$	n/a	$\varphi^5 = 1$ $\sigma(a) = a$ $\sigma(a) = a^2$	$\varphi^9 = 1$ $\sigma(a) = a^2$	$\varphi^{17} = 1$ $\varphi^{51} = 1$ $\varphi^{85} = 1$ $\varphi^{255} = 1$
#Planes	2		9	6	0
$\mathbb{F}_8$	n/a	$\varphi^7 = 1$	n/a	$\varphi^9 = 1$ $\sigma(a) = a$ $\sigma(a) = a^2$ $\sigma(a) = a^4$	n/a
#Planes		0		18	

TABLE 3 Possible choices for automorphisms in semifields with weak nucleus.

The weak nucleus $\mathbb{F}$ appears in the rows of the table, while the columns represent the field $\mathbb{K}$. Since $\mathbb{F}$ must be a subfield of $\mathbb{K}$ there are some forbidden combinations. Such is the case of $\mathbb{F} = \mathbb{F}_4$, $\mathbb{K} = \mathbb{F}_8$ and, for $\mathbb{F} = \mathbb{F}_8$, $\mathbb{K} = \mathbb{F}_4$, $\mathbb{F}_{16}$ and $\mathbb{F}_{256}$. The new semifields are characterized by the order of the automorphism φ and $\sigma \in \mathrm{Aut}(\mathbb{F})$. For $\mathbb{F} = \mathbb{K} = \mathbb{F}_8$ there are no semifields with an automorphim of order 7, as can be seen in the classification of[16], whereas for $\mathbb{F} = \mathbb{F}_4$ and $\mathbb{K} = \mathbb{F}_{256}$ no semifields with an automorphism of order 17 have been found.

The semifields $S = (\mathbb{F}_4 \times \mathbb{F}_4, +, *)$ are already known. This construction provides semifields with 3 and 6 automorphisms which are isotopic to the systems V and W of Section 2.2 of[10]. The same happens with $S = (\mathbb{F}_4 \times \mathbb{F}_{16}, +, *)$ for the two possible choices of σ: these semifields are exactly those considered in the previous section.

The computational process for finding the new semifields is the following one. First of all, we choose the field $\mathbb{F} = \mathbb{F}_{2^n}$, which will be the weak nucleus for S, and an extension $\mathbb{K} = \mathbb{F}_{2^{nk}}$ of $\mathbb{F}$. Now, we fix a $\mathbb{F}_2$-basis $\{1, \xi, \dots, \xi^{nk-1}\}$ for $\mathbb{K}$ and choose an automorphism σ of $\mathbb{F}$. Recall that the multiplicative order, s, of ξ will be the order of the automorphism φ of S. With Magma,[1], we construct the functions F and G for all possible choices of the coefficients f_{ij} and g_{ij} (notice that some of these coefficients are known to be 0), and then we find the roots of polynomial (3) for all possible choices of $b, d \in \mathbb{K}$. If there exists a root in $\mathbb{F}$, then we have found a zero divisor and $(S, +, *)$ can not be a semifield. Otherwise, we calculate $(a, b) * (c, d)$ for all $a, c \in \mathbb{F}$ and $b, d \in \mathbb{K}$ and verify the absence of zero divisors. If there are none of them, we have found a new semifield $(S, +, *)$ with an automorphism φ of order s and weak nucleus $\mathbb{F}$.

Some semifields have been found with weak nucleus $\mathbb{F} = \mathbb{F}_4$ and $\mathbb{K} = \mathbb{F}_{64}$. They all have order 256 and automorphism group isomorphic to C_9. From Corollary 3, we know that the functions F and G must have the following form

$$F(b, d) = \mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(f_{30} b^8 d + f_{41} b^{16} d^2), \; G(b, d) = g_{31} b^8 d^2 + g_{13} b^2 d^8 + g_{55} b^{32} d^{32}.$$

Plane	$F(b,d)$	$G(b,d)$	Atm(S)	Atp(S)
1	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{57}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{44}b^2d^8+\alpha^{12}b^{32}d^{32}$	C_9	$C_9 \times C_3$
	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{12}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{47}b^2d^8+\alpha^{27}b^{32}d^{32}$		
	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{21}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{59}b^2d^8+\alpha^{24}b^{32}d^{32}$		
2	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{60}b^{16}d^2)$	$b^8d^2+\alpha^{29}b^2d^8+\alpha^{22}b^{32}d^{32}$		
	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{42}b^{16}d^2)$	$\alpha^3b^8d^2+\alpha^{26}b^2d^8+\alpha^{58}b^{32}d^{32}$		
	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{3}b^{16}d^2)$	$\alpha^3b^8d^2+\alpha^{46}b^2d^8+\alpha^{8}b^{32}d^{32}$		
3	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{42}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{6}b^2d^8+\alpha^{47}b^{32}d^{32}$		
	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{33}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{18}b^2d^8+\alpha^{17}b^{32}d^{32}$		
	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{15}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{21}b^2d^8+\alpha^{41}b^{32}d^{32}$		
4	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{39}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{11}b^2d^8+\alpha^{48}b^{32}d^{32}$		
	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{48}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{35}b^2d^8+\alpha^{33}b^{32}d^{32}$		
	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{3}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{41}b^2d^8+\alpha^{45}b^{32}d^{32}$		
5	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{24}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{18}b^2d^8+\alpha^{11}b^{32}d^{32}$		
	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{21}b^{16}d^2)$	$\alpha^3b^8d^2+\alpha^{46}b^2d^8+\alpha^{41}b^{32}d^{32}$		
	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{15}b^{16}d^2)$	$\alpha^3b^8d^2+\alpha^{26}b^2d^8+\alpha^{61}b^{32}d^{32}$		
6	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{6}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{6}b^2d^8+\alpha^{23}b^{32}d^{32}$		
	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{24}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{18}b^2d^8+\alpha^{11}b^{32}d^{32}$		
	$\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{64}}(\alpha^{60}b^{16}d^2)$	$\alpha b^8d^2+\alpha^{21}b^2d^8+\alpha^{8}b^{32}d^{32}$		

TABLE 4 Functions F and G of new semifields of order 256 with a weak nucleus $\mathbb{F}_4$, and their automorphism (Atm(S)) and autotopy (Atp(S)) groups (all of them lie in the same Knuth class).

We have only found semifields when the automorphism σ is of the form $\sigma(a) = a^2$ for all $a \in \mathbb{F}$. Thus, the product $*$ of S is given by

$$(a,b) * (c,d) = (a \cdot c + F(b,d)\ ,\ a \cdot d + c^2 \cdot b + G(b,d)),$$

where the explicit form of $F(b,d)$ and $G(b,d)$ is given in Table 4 . The element $\alpha \in \mathbb{K}$ is a primitive 63-th root of unity satisfying $\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$. As can be seen in that table, we have found a total of 18 non isomorphic semifields, lying in six different planes. All these planes are in the same Knuth orbit.

By construction, for all these semifields the map $\varphi(a,b) = (a, \xi \cdot b)$, is an automorphism of order 9. Thus, the order of their automorphism group, $|\mathrm{Atm}(S)|$, must be a multiple of 9. After computational verification we found that, in fact, $|\mathrm{Atm}(S)| = 9$ and so, the automorphism group of any of these semifields is isomorphic to the cyclic group C_9. On the other hand, if $\beta \in \mathbb{F}_{64}$ is a 3-rd root of unity, it is easy to see that the triple (H, J, K), defined by $H(a,b) = (\beta^2 \cdot a, \beta^2 \cdot b)$, $J(c,d) = (\beta^2 \cdot c, \beta \cdot d)$ and $K(e,f) = (\beta \cdot e, f)$, satisfies the relation $H(a,b) * J(c,d) = K((a,b) * (c,d))$ and so, it is an isotopy of S of order 3 which commutes with the automorphism φ. Then, the autotopism group, Atp(S), must contain the group $C_9 \times C_3$ as subgroup. Using the computational methods of[5], we verified that $\mathrm{Atp}(S) \cong C_9 \times C_3$.

In the case $\mathbb{F} = \mathbb{F}_4$ and $\mathbb{K} = \mathbb{F}_{256}$ with an automorphism φ of order 17, we obtain from Corollary 3 that $F(b,d) = \mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_{256}}(f_{14}bd^{16} + f_{15}b^2d^{32})$ and $G(b,d) = g_{41}b^{16}d^2 + g_{14}b^2d^{16} + g_{77}b^{128}d^{128}$. After a systematic computational search for these semifields, we have not found any of them. For the automorphisms of order 51, 85 and 255, the function $F(b,d)$ must be identically zero and $G(b,d) = g_{77}b^{128}d^{128}$. As in the previous case, there are no semifields of this kind. A proof of the non existence of these semifields is provided in Theorem 5.

The results obtained for semifields with weak nucleus $\mathbb{F} = \mathbb{F}_8$ and $\mathbb{K} = \mathbb{F}_{64}$ are summarized in Table 5 . The element $\alpha \in \mathbb{K}$ is a primitive 63-th root of unity such that $\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$. We have found a total of 94 non-isomorphic such semifields

Knuth Class	Plane	$F(b,d)$	$G(b,d)$	Atm(S)	Atp(S)
I	1	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{12}b^8d+\alpha^6b^{32}d^4)$	$\alpha^{42}b^{32}d^{32}$	$C_9 \rtimes C_3$	$C_{63} \rtimes C_3$
	13	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{12}b^8d+\alpha^6b^{32}d^4)$	$\alpha^{21}b^{32}d^{32}$		
II	2	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{13}b^8d+\alpha^{58}b^{16}d^2+\alpha^2b^{32}d^4)$	$\alpha^5b^{32}d^{32}$	C_9	C_{63}
	3	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{31}b^8d+\alpha^{49}b^{16}d^2+\alpha^2b^{32}d^4)$	$\alpha^{31}b^{32}d^{32}$		
III	4	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{46}b^8d+\alpha^6b^{16}d^2+\alpha^6b^{32}d^4)$	$\alpha^{19}b^{32}d^{32}$	C_9	C_{63}
	7	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^4b^8d+\alpha^{24}b^{16}d^2+\alpha^6b^{32}d^4)$	$\alpha^{50}b^{32}d^{32}$		
IV	6	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{38}b^8d+\alpha^{12}b^{16}d^2+\alpha^2b^{32}d^4)$	$\alpha^4b^{32}d^{32}$	C_9	C_{63}
	12	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{11}b^8d+\alpha^{57}b^{16}d^2+\alpha^2b^{32}d^4)$	$\alpha^{14}b^{32}d^{32}$		
V	9	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{29}b^8d+\alpha^5b^{16}d^2+\alpha^6b^{32}d^4)$	$\alpha^{14}b^{32}d^{32}$	C_9	C_{63}
	10	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{29}b^8d+\alpha^5b^{16}d^2+\alpha^6b^{32}d^4)$	$\alpha^{49}b^{32}d^{32}$		
VI	5	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{34}b^8d+\alpha^{18}b^{16}d^2+\alpha^2b^{32}d^4)$	$\alpha^{42}b^{32}d^{32}$	C_9	C_{63}
	8	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{52}b^8d+\alpha^9b^{16}d^2+\alpha^2b^{32}d^4)$	$\alpha^{12}b^{32}d^{32}$		
VII	11	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{27}b^{16}d^2)$	$\alpha^3b^8d^2+\alpha^{45}b^2d^8$	$C_9 \rtimes C_3$	$C_{63} \rtimes C_3$
	14	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(b^{16}d^2)$	$b^8d^2+\alpha^{42}b^2d^8$		
	15	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(b^{32}d^{32})$	$b^8d^2+\alpha^{21}b^{32}d^{32}$		
	16	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(\alpha^{54}b^{32}d^{32})$	$\alpha^3b^8d^2+b^{32}d^{32}$		
	17	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(b^8d)$	$\alpha^{42}b^2d^8+b^{32}d^{32}$		
	18	$\mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(b^8d)$	$b^2d^8+\alpha^{42}b^{32}d^{32}$		

TABLE 5 Functions F and G of new semifields of order 512 with a weak nucleus $\mathbb{F}_4$, and their automorphism (Atm(S)) and autotopy (Atp(S)) groups.

of order 512 distributed in 18 planes. The product $*$ is of the form

$$(a,b)*(c,d) = (a\cdot c + F(b,d)\ ,\ a\cdot d + \sigma(c)\cdot b + G(b,d)),$$

with $F(b,d) = \mathrm{Tr}_{\mathbb{F}_8}^{\mathbb{F}_{64}}(f_{30}\,b^8d + f_{41}\,b^{16}d^2 + f_{52}\,b^{32}d^4)$ and $G(b,d) = g_{31}\,b^8d^2 + g_{13}\,b^2d^8 + g_{55}\,b^{32}d^{32}$, as is established in Corollary 3. The automorphism σ is the identity for planes 1–14, $\sigma(a) = a^2$ for planes 15 and 16, and finally, $\sigma(a) = a^4$ for planes 17 and 18.

By construction, the map $\varphi(a,b) = (a, \xi\cdot b)$, with $\xi \in \mathbb{F}_{64}$ a primitive 9-th root of unity satisfying $\xi^6+\xi^3+1 = 0$, is an isomorphism of S. So, the group Atm(S) must have a cyclic subgroup of order 9. The planes $1, 11, 13, 14, 15, 16, 17$ and 18 have another automorphism τ of order 3, that can be found in Table 6 . It is straightforward to see that $\tau\varphi\tau^{-1} = \varphi^7$ and so, the group Atm(S) must contain the group $G = \langle g_1, g_2 \mid g_1^9 = 1\ ,\ g_2^3 = 1\ ,\ g_2g_1g_2^{-1} = g_1^7\rangle$ as a subgroup. This group has order 27 and is isomorphic to a semidirect product $C_9 \rtimes C_3$. Using computational methods, we verified that the group Atm(S) has order 27 and so it is equal to G. The remaining 10 planes have no other automorphism apart from φ and its powers and so, Atm(S) $\cong C_9$ for all of them.

Planes $1, 2, 4, 5, 6$ and 9 lie on the Knuth classes I to VI. Each class also contains the dual plane of the chosen representative (i.e., planes $13, 3, 7, 12, 10$ and 8) see Table 5 . The other six planes constitute a single Knuth class: VII. For semifields in classes I and VII, we can find an isotopy (H, J, K) of order 7, see Table 6 , which commutes with the automorphism φ. Thus, we have an isotopy $(\widetilde{H}, \widetilde{J}, \widetilde{K}) = (H\cdot\varphi, J\cdot\varphi, K\cdot\varphi)$ of order 63 which verifies that $\tau\cdot(\widetilde{H}, \widetilde{J}, \widetilde{K})\cdot\tau^{-1} = (\widetilde{H}, \widetilde{J}, \widetilde{K})^{16}$ for all τ in Table 6 . So, the autotopy group, Atp(S), for semifields in classes I and VII must contain the subgroup $G = \langle g_1, g_2 \mid g_1^{63} = 1\ ,\ g_2^3 = 1\ ,\ g_2g_1g_2^{-1} = g_1^{16}\rangle$ which is isomorphic to a semidirect product $C_{63} \rtimes C_3$.After a computational verification, we found that Atp(S) has order 189 and so, Atp(S) $= G$. For classes II to VI, there exist the automorphism φ and the isotopy (H, J, K) of order 7 given by $H(a,b) = (\eta^6a, \eta^6b)$, $J(c,d) = (\eta c, \eta d)$ and $K(e,f) = (e,f)$, where η is a 7-th root of unity. The automorphism and the isotopy commute, so, in this case, the autotopy group Atp(S) contains the direct product $C_9 \times C_7 \cong C_{63}$. Using computational methods, we found that, in fact, Atp $\cong C_{63}$.

Knuth Class	Plane	$\tau(a,b)$	$H(a,b)$	$J(c,d)$	$K(e,f)$
I	1	$(a^2,\alpha^6 b^{16})$	$(\eta^6 a,\eta^6 b)$	$(\eta c,\eta d)$	(e,f)
	13	$(a^2,\alpha^6 b^{16})$	$(\eta^6 a,\eta^6 b)$	$(\eta c,\eta d)$	(e,f)
VII	11	$(a^2,\alpha^{12} b^{16})$	$(\eta a,\eta^4 b)$	$(\eta c,\eta^4 d)$	$(\eta^2 e,\eta^5 f)$
	14	(a^2,b^{16})	$(\eta a,\eta^4 b)$	$(\eta c,\eta^4 d)$	$(\eta^2 e,\eta^5 f)$
	15	(a^2,b^{16})	$(\eta^2 a,\eta^3 b)$	$(\eta^6 c,\eta^6 d)$	$(\eta e,\eta f)$
	16	$(a^2,\alpha^{54} b^{16})$	$(\eta^2 a,\eta^3 b)$	$(\eta^6 c,\eta^6 d)$	$(\eta e,\eta f)$
	17	(a^2,b^{16})	$(\eta^5 a,\eta^6 b)$	$(\eta^4 c,\eta^3 d)$	$(\eta^2 e,\eta f)$
	18	(a^2,b^{16})	$(\eta^5 a,\eta^6 b)$	$(\eta^4 c,\eta^3 d)$	$(\eta^2 e,\eta f)$

TABLE 6 Automorphism τ of order 3 and Isotopy (H, J, K) of order 7 for semifields of order 512 in Knuth classes I and VII. The element η is a 7-th root of unity.

3.1 | Proof that the sporadic semifields are new

In this subsection we provide some facts which show that the sporadic semifields described in this work are new. Since the size of the nuclei N_l, N_r and N_m, is invariant under isotopy transformations, we will use this information in order to prove that the constructed semifields are actually new.

The sporadic semifields with 256 elements lie in a unique Knuth orbit, and the size of their nuclei is $|N_l| = |N_r| = |N_m| = 2$. In agreement with[12], these semifields could be in the Knuth orbit of:

1. Hughes-Kleinfeld semifields of order $2^{2\cdot 4}$ and Sandler semifields of order $2^{4\cdot 2}$ with center of order 2. All these semifields have at least two of their nuclei of size 4. So, they can not be isotopic to any of the semifields constructed in this section.

2. Knuth semifields of type I, II, III or IV and binary Knuth semifields. Knuth semifields of type II, III and IV must have two nuclei of size 2^4. So, the only ones that can be isotopic to the semifields found in this section are those of type I. Using computational methods, we found that the our semifields are neither Knuth semifields of type I nor binary Knuth semifields, since they are not commutative.

In addition, we have taken into account the constructions of semifields presented in[18]. They generalize some known structures like generalized twisted fields and cyclic semifields, but some of them are completely new. As can be seen in Corollary 2 of[18], there are two different families of these semifields. The first one is denoted by $S_{n,s,1}(\eta,\rho,F) \leq M_n(\mathbb{F}_{q^s}) \leq M_{ns}(\mathbb{F}_q)$, with $q = p^e$, $\eta \in \mathbb{F}_{q^n}$, $\rho \in \mathrm{Aut}(\mathbb{F}_{q^n})$ and F an irreducible polynomial over $K[x]$, with K a subfield of $\mathbb{F}_{q^n}$. The second family is denoted by $S_{n,s,k}(0,0,F)$, with F an irreducible polynomial over $K[x]$. In any case, for semifields of order 256, the size of their nuclei can never be equal to $|N_l| = |N_r| = |N_m| = 2$. Thus, the semifields described in this section can never be isotopic nor fall in the Knuth orbit of those presented in[18].

There exist seven different Knuth classes for the sporadic semifields with 512 elements. The size of the nuclei for semifield III in Table 5 are $|N_l| = |N_r| = |N_m| = 2$, whereas for the other ones we have $|N_l| = |N_r| = 2, |N_m| = 8$. From[12], these semifields could be isotopic to some of the following ones:

1. Albert generalized twisted fields of order 2^9. These semifields have center of order 2^3. So, they can not be isotopic to semifields in Table 5 since the formers have center isomorphic to $\mathbb{F}_2$.

2. Knuth binary semifields. These semifields are commutative and so their Knuth orbits have 3 semifields at most. However, it has been computationally checked that the Knuth orbit of semifields in Table 5 always has 6 semifields.

3. Jha-Johnson cyclic semifields. They are a special case of the construction in[18], and they will be analysed latter on.

4. Kantor-Williams symplectic pre-semifields of order 2^9 or 8^3 and their commutatives Knuth derivatives. Again, the Knuth orbit of these semifields has 3 semifields at most, so those in Table 5 can not be isotopic to any of them.

Finally, we have to consider the semifields $S_{n,s,1}(\eta,\rho,F)$ and $S_{n,s,1}(0,0,F)$ of[18]. There are only two possible choices for the parameters n and s in order to construct semifields with nuclei of sizes $|N_l| = |N_r| = |N_m| = 2$ or $|N_l| = |N_r| = 2$ and

$|N_m| = 8$. For the first case, $n = 3$, $s = 1$ and $q = 2^3$. By Remark 8 of[18], these semifields must be Albert generalized twisted fields. But, in that case, the nuclei and the center must have 8 elements, which leads to a contradiction. So, $n = 3$, $s = 3$, $q = 2$ and the semifield must be of type $S_{3,3,1}(\eta, \rho, F)$. From Theorem 6 of[18], this election of parameters implies $\eta = 0$ and so, as a consequence of Theorem 8 of[18], the semifield must be of type $S_{3,3,1}(0, 0, F)$. In such a case, the sizes of the nuclei must be $|N_l| = |N_m| = 2^3$, $|N_r| = 2^9$, which is impossible.

4 | CONCLUSIONS

In this work we have studied the structure of some division rings with 64 elements and automorphism group isomorphic to the cyclic group C_5. Using the techniques presented in[10], we have been able to extend this behaviour to other finite division rings with 256 and 512 elements and with a designed automorphism group. Notice that all these rings are 3-dimensional vector spaces over the weak nucleus instead of 2-dimensional, as in[10]. These rings have been classified into Knuth orbits and their autotopism group has been calculated. Finally, we have proved that these rings do not belong to the large class of semifields presented in[18]. The work finishes with some results about the non existence of division rings with 256 and 1024 and certain automorphisms groups.

4.1 | Acknowledgments

This work has been partially supported by the Ministry of Economy and Competitiveness (Ministerio de Economía y Competitividad) from Spain/FEDER under grant TEC2015-67387-C4-3-R, by the Ministry of Economy, Industry and Competitiveness (Ministerio de Economía, Industria y Competitividad) from Spain/FEDER under grant MTM2017-83506-C2-2-P and by Principado de Asturias under grant GRUPIN14-142.

4.2 | Bibliography

References

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

2. J. V. Brawlwy, L. Carlitz, T. Vaughan *Linear permutation polynomials with coefficients in a sufield*, Acta Arithmetica **24** (1973), 193-199.

3. Mashhour Bani-Ata, Shuaa Aldhafeeri, Fethi Belgacem, Mahmoud Laila, *On Four-Dimensional Unital Division Algebras over Finite Fields*, Algebras and Representation Theory **18** (2015), 215–220.

4. A. R. Calderbank, P. J. Cameron, W. M. Kantor, J. J. Seidel, *$\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets*, Proc. London Math. Soc **75** (1997), 436–480.

5. E.F. Combarro, I. F. Rúa, J. Ranilla, *New advances in the computational exploration of semifields*, International Journal of Computer Mathematics **88 (9)** (2011), 1990-2000.

6. S. González, C. Martínez, I.F. Rúa, *Symplectic Spread based Generalized Kerdock Codes*, Designs, Codes and Cryptography **42 (2)** (2007), 213–226.

7. M. Hall(Jr.), *The theory of groups*, Macmillan, (1959).

8. W. M. Kantor, M. E. Williams, *Symplectic semifield planes and $\mathbb{Z}_4$-linear codes*, Transactions of the American Mathematical Society **356** (2004), 895–938.

9. W. M. Kantor, *Finite semifields*, Finite Geometries, Groups, and Computation (Proc. of Conf. at Pingree Park, CO Sept. 2005), de Gruyter, Berlin-New York (2006).

10. D.E. Knuth, *Finite semifields and projective planes*, Journal of Algebra **2** (1965), 182-217.

11. M. Lavrauw, J, Sheekey, *The BEL-rank of finite semifields*, Des. Codes Cryptogr. **84** (2017), 345–358.

12. M. Lavrauw, O. Polverino, *Finite Semifields*, in Current Research in Galois Geometry, L. Storme and J. de Beule (Eds.) (2011) 131–160.

13. J. P. May, D. Saunders, Z. Wan, *Efficient Matrix Rank Computation with Applications to the Study of Strongly Regular Graphs*, Proceedings of ISSAC 2007, 277-284, ACM, New-York, 2007.

14. Mashhour I. M. Al-Ali, *The Automorphism Group of a Semifield of Order q^4*, Communications in Algebra **36** (2008), 3347–3352.

15. A. A. Nechaev, *Finite principal ideal rings*. Math. USSR Sb. **2** (1973), 364-382.

16. I. F. Rúa, Elías F. Combarro, J. Ranilla, *Classification of Semifields of Order 64*, J. of Algebra, **322 (11)** (2009), 941-961.

17. I. F. Rúa, Elías F. Combarro, J. Ranilla, *Determination of division algebras with 243 elements*, Finite Fields and their Applications, **18** (2012), 1148-1155.

18. J. Sheekey, *New Semifields and new MRD Codes from Skew Polynomial Rings*, arXiv:1806.00251.

□

APPENDIX

A NON EXISTENCE RESULTS

In this last section, we collect some results on the nonexistence of semifields with weak nucleus and designed automorphism group.

In the case of semifields with 256 elements with weak nucleus $\mathbb{F} = \mathbb{F}_4$ and $\mathbb{K} = \mathbb{F}_{64}$ there exist two more possible choices for the automorphism group. However, it is not possible to construct such semifield, as it is proved in the following result.

Theorem 4. There are no semifields $S = (\mathbb{F}_4 \times \mathbb{F}_{64}, +, *)$ with multiplication defined by (1) with an automorphism φ of order 21 or 63.

Proof. From Corollary 3, the order of the automorphism φ implies that, from (2), $F(b,d) = 0$ and $G(b,d) = g_{55}b^{32}d^{32}$ for all $b, d \in \mathbb{F}_{64}$. So, $(a,b) * (c,d) = (0,0)$ is equivalent to the conditions $a \cdot c = 0$ and $a \cdot d + \sigma(c) \cdot b + g_{55}b^{32}d^{32} = 0$. If $g_{55} = 0$, then $(a,b) = (c,d) = (0,1)$ are zero divisors. So let us assume that $g_{55} \neq 0$. Let $\alpha \in \mathbb{F}_{64}$ be a primitive 63-th root of unity, so that $g_{55} = \alpha^k$, for some integer k. Let us suppose that $a = 0$ and that $b, c, d \neq 0$. Then, $\sigma(c) \cdot b = g_{55}b^{32}d^{32}$ and so, $\sigma(c) = g_{55}(db^{-1})^{32}$ because $b^{63} = 1$ gives $b^{-32} = b^{31}$. Since $\sigma \in \mathrm{Aut}(\mathbb{F}_4)$, the latter equation has a valid solution if and only if $(g_{55}d^{32}b^{-32})^4 = g_{55}d^{32}b^{-32}$, that is, if and only if $(db^{-1})^{30} = g_{55}^3$ because $(db^{-1})^{63\cdot 2} = 1$ gives $(db^{-1})^{-32\cdot 3} = (db^{-1})^{30}$. The previous equation can be written as $\alpha^{30i} = \alpha^{3k}$, and it has solutions if and only if the congruence $30i \equiv 3k \pmod{63}$ has any solutions in $\mathbb{Z}$, which is true because $\gcd(30, 63) = 3$ trivially divides $3k$ for any k. Let i be any one of these solutions, and let $z = \alpha^i$. For any $b \neq 0$, let $R_{b^{-1}}$ be the right multiplication by b^{-1} in $\mathbb{F}_{64}$. This operator is surjective, so there exists an element d such that $R_{b^{-1}}(d) = z$. Then, $(db^{-1})^{30} = \alpha^{30i} = \alpha^{3k} = g_{55}^3$ and so, we have found an element $d \neq 0$ such that $(0,b) * (c,d) = 0$ and S cannot be a semifield.

□

For semifields with 1024 elements and weak nucleus $\mathbb{F} = \mathbb{F}_4$, notice that it is also possible to take automorphisms of order 51, 85 and 255. In such case, the functions F and G given in (2) must be $F(b,d) = 0$ and $G(b,d) = g_{77}b^{128}d^{128}$. It is easy to see that there are no semifields of this kind.

Theorem 5. There are no semifields $S = (\mathbb{F}_4 \times \mathbb{F}_{256}, +, *)$ with multiplication defined by (1) with an automorphism φ of order 51, 85 or 255.

Proof. As in the proof of the previous theorem, it suffices to find $b, d \in \mathbb{F}_{256}^*$ such that $(db^{-1})^{126} = g_{77}^3$. If $\zeta \in \mathbb{F}_{256}$ is a primitive 255-th root of unity, this condition is equivalent to solve the congruence $126i \equiv 3k \pmod{255}$ for a certain k such that $g_{77} = \zeta^k$. But this congruence can always be solved, because $\gcd(126, 255) = 3$ divides $3k$ for any k. The rest of the proof is as in the previous theorem and will be omitted. □

Finally, we state the following result about the non existence of semifields of order 1024 with weak nucleus $\mathbb{F} = \mathbb{F}_8$ and automorphism group of order 21 or 63. The proof is similar to those of Theorems 4 and 5 and will be omitted.

Theorem 6. There are no semifields $S = (\mathbb{F}_8 \times \mathbb{F}_{64}, +, *)$ with multiplication defined by (1) with an automorphism φ of order 21 or 63.