

Determination of division algebras with 243 elements

I.F. Rúa*

Elías F. Combarro†

J. Ranilla†

Abstract

Finite nonassociative division algebras (i.e., finite semifields) with 243 elements are completely classified.

1 Introduction

Finite division rings, also known as **finite semifields**, are nonassociative rings with identity such that the set of nonzero elements is closed under the product (i.e., a loop [11, 3]). In case it has no identity they are known as **presemifields**. These objects have been studied in different contexts: finite geometries (they coordinatize projective semifield planes [6]), coding theory [2, 8, 5], combinatorics and graph theory [13].

Computational methods have been considered in the study of these objects. Among others, the classification of finite semifields of orders 16 [10, 11], 32 [16, 11] and, more recently, orders 64 [14] and 81 [4] have been obtained with the help of computational tools. Presently, only the cases of orders 128, 243 and 256 remain to achieve the classification of semifield planes of order 256 or less suggested in [9].

In this paper we present a classification of semifields with **243 elements** up to isotopy. It is a computer-assited classification based on the algorithms introduced in [14].

2 Preliminaries

In this section we collect some definitions and facts on finite semifields, presemifields and planar functions (see, for instance [3, 11]). We restrict ourselves to the particular case of order $243 = 3^5$. The characteristic of a finite presemifield D with 3^5 elements is 3, and D is a 5–dimensional algebra over \mathbb{F}_3 . If D is a semifield, then \mathbb{F}_3 can be chosen to be contained in its associative-commutative center $Z(D)$. Other relevant subsets of a finite semifield are the left, right, and middle nuclei (N_l, N_r, N_m) , and the nucleus N which have to be field extensions \mathbb{F}_{3^e} ($e \leq 5$).

Classification of presemifields is usually considered up to *isotopy* (since this corresponds to classification of the corresponding projective planes up to isomorphism): If D_1, D_2 are two presemifields of order 3^5 , an isotopy between D_1 and D_2 is a triple (F, G, H) of bijective \mathbb{F}_3 –linear maps $D_1 \rightarrow D_2$ such that

$$H(ab) = F(a)G(b), \quad \forall a, b \in D_1.$$

Any presemifield is isotopic to a finite semifield.

*Departamento de Matemáticas, Universidad de Oviedo, rua@uniovi.es .

†Artificial Intelligence Center, University of Oviedo, {elias,ranilla}@aic.uniovi.es .

If $\mathcal{B} = [x_1, \dots, x_5]$ is a \mathbb{F}_3 -basis of a presemifield D , then there exists a unique set of constants $\mathbf{A}_{D,\mathcal{B}} = \{A_{i_1 i_2 i_3}\}_{i_1, i_2, i_3=1}^5 \subseteq \mathbb{F}_3$ such that

$$x_{i_1} x_{i_2} = \sum_{i_3=1}^5 A_{i_1 i_2 i_3} x_{i_3} \quad \forall i_1, i_2 \in \{1, \dots, 5\}$$

This set of constants is known as **cubical array** or **3-cube** corresponding to D with respect to the basis \mathcal{B} , and it completely determines the multiplication in D . If D is a presemifield, and $\sigma \in S_3$ (the symmetric group on the set $\{1, 2, 3\}$), then the set

$$\mathbf{A}_{D,\mathcal{B}}^\sigma = \{A_{i_{\sigma(1)} i_{\sigma(2)} i_{\sigma(3)}}\}_{i_1, i_2, i_3=1}^5 \subseteq \mathbb{F}_3$$

is the 3-cube of a presemifield. Different choices of bases lead to isotopic presemifields. Up to six projective planes can be constructed from a given finite semifield D using the transformations of the group S_3 . So, the classification of finite semifields can be reduced to the classification of the corresponding projective planes up to the action of the group S_3 .

Finite semifields of order 243 can be constructed from sets of matrices with certain properties [4][7, Proposition 3].

Proposition 1. *There exists a finite semifield D of order 3^5 if, and only if, there exists a set of 5 matrices (a **standard basis** of D) $S_D = \{A_1, \dots, A_5\} \subseteq GL(5, 3)$ (the set of invertible matrices of size 5 over \mathbb{F}_3) such that:*

1. A_1 is the identity matrix I ;
2. $\sum_{i=1}^5 \lambda_i A_i \in GL(5, 3)$, for all non-zero tuples $(\lambda_1, \dots, \lambda_5) \in \mathbb{F}_3^5$, that is, $(\lambda_1, \dots, \lambda_5) \neq \{\vec{0}\}$.
3. The first column of the matrix A_i is the column vector e_i^\downarrow with a 1 in the i -th position, and 0 everywhere else.

In such a case, the set $\{B_{ijk}\}_{i,j,k=1}^d$, where $B_{ijk} = (A_j)_{ik}$, is the 3-cube corresponding to D with respect to the canonical basis of \mathbb{F}_3^5 .

If we identify the elements of \mathbb{F}_3 with the natural numbers $\{0, 1, 2\}$, then we can use the following convention to represent a semifield D of order 3^5 . Let $S_D = \{A_1, \dots, A_5\}$ be one of its standard bases. Since the first column of A_i has always a one in the i -th position and zeroes elsewhere, we can encode A_i as the natural number $\sum_{j=0}^{19} a_j 3^j$, where

$$\left(e_i^\downarrow \left| \begin{array}{cccc} a_{19} & a_{14} & a_9 & a_4 \\ a_{18} & a_{13} & a_8 & a_3 \\ a_{17} & a_{12} & a_7 & a_2 \\ a_{16} & a_{11} & a_6 & a_1 \\ a_{15} & a_{10} & a_5 & a_0 \end{array} \right. \right)$$

For a concrete representation of the semifield one can identify the semifield with \mathbb{F}_3^5 , and the multiplication with $x * y = \sum_{i=1}^5 x_i A_i y$, i.e., A_i is the matrix of left multiplication by the element e_i , where $\{e_1, \dots, e_5\}$ is the canonical basis of \mathbb{F}_3^5 . So, the elements of the standard basis are simply coordinate matrices of the linear maps $L_{e_i} : D \rightarrow D$, $L_{e_i}(y) = e_i * y$.

The following result shows that, in order to classify finite semifields of order 243, it is possible to impose for extra conditions on the standard bases.

Proposition 2. *Let D be a finite semifield of order 243. Then, there exists an isotope D' of D such that, if $S_{D'} = \{A_1, \dots, A_5\}$ is a standard basis of D' , then A_2 has one of the following forms:*

$$C(x^5 + x^3 + x + 1), C(x^5 + 2x + 1), C(x^5 + x^3 + x + 2), C(x^5 + 2x + 2) \quad (1)$$

or

$$\begin{pmatrix} C(x^3 + x^2 + x + 2) & 0 \\ 0 & C(x^2 + 2x + 2) \end{pmatrix}, \begin{pmatrix} C(x^3 + 2x^2 + x + 1) & 0 \\ 0 & C(x^2 + x + 2) \end{pmatrix} \quad (2)$$

where $C(p(x))$ is the companion matrix of the polynomial $p(x) \in \mathbb{F}_3[x]$.

Proof. We first show that there exists an element $b \in D \setminus \mathbb{F}_3$ (i.e., *non-scalar*) such that the characteristic polynomial of the linear transformation $L_b : D \rightarrow D$ ($L_b(x) = b * x$) is $x^5 + a_2x^3 + a_4x + a_5 \in \mathbb{F}_3[x]$. We fix $\{x_1, x_2, x_3, x_4, x_5\}$, a \mathbb{F}_3 -basis of D , and consider the characteristic polynomial of L_b for a generic element $b = \lambda_1x_1 + \lambda_2x_2 + \lambda_3x_3 + \lambda_4x_4 + \lambda_5x_5 \in D$:

$$x^5 + \rho_1(\bar{\lambda})x^4 + \rho_2(\bar{\lambda})x^3 + \rho_3(\bar{\lambda})x^2 + \rho_4(\bar{\lambda})x + \rho_5(\bar{\lambda})$$

where $\rho_i(\bar{\lambda})$ is a homogeneous polynomial in $\mathbb{F}_3[\bar{\lambda}] = \mathbb{F}_3[\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5]$, of degree i . Consider the system of equations $\rho_1(\bar{\lambda}) = \rho_3(\bar{\lambda}) = 0$. From the Chevalley-Waring theorem [12, Theorem 6.6] it has a nonzero solution, i.e., there exists a nonzero element $b \in D$ such that the characteristic polynomial of L_b is of the claimed form.

The element b can not be 1 or 2, since the trace of the polynomials $(x - 1)^5$ and $(x - 2)^5$ is not zero, and so b is non-scalar. Because of [1][Lemma 5], the characteristic polynomial of L_b has no linear factors, and so it has to be one of the following six polynomials:

$$x^5 + x^3 + x + 1, x^5 + 2x + 1, x^5 + x^3 + x + 2, x^5 + 2x + 2, x^5 + 2x^3 + 1, x^5 + 2x^3 + 2$$

The first four polynomials are irreducible, and so the set $\{1, b, b^2, b * b^2, b * (b * b^2)\}$ is a \mathbb{F}_3 -basis of D ([1, Section 3], there on the right, here on the left). This provides a standard basis $S_D = \{[L_1], [L_b], [L_{b^2}], [L_{b*b^2}], [L_{b*(b*b^2)}]\}$ where $[L_b]$ has one of the forms in equation (1) (notice that D is an isotope of itself).

On the other hand, the last two polynomials have the following factorizations:

$$(x^3 + x^2 + x + 2)(x^2 + 2x + 2), (x^3 + 2x^2 + x + 1)(x^2 + x + 2)$$

Because of [1, Lemma 5], there exists an isotope D' of D and an element $c \in D'$ such that its *minimal function* is the first factor. So, because both factors are coprime, we can choose a \mathbb{F}_3 -basis of D' of the form $\{1, c, c^2, d, c * d\}$. In the corresponding standard basis $S_{D'} = \{[L_1], [L_c], [L_{c^2}], [L_d], [L_{c*d}]\}$, the matrix $[L_c]$ has one of the forms in equation (2). □

3 The Semifield Planes of order 243: a classification

We obtained a complete classification of finite semifields of order 243 with the help of the algorithm introduced in [14]. This algorithm searches for standard bases of division algebras with 243 elements, and classify them according to equivalent S_3 -equivalent semifields. This is done either for partial or for complete standard bases.

Our algorithm was processed in parallel in Magerit, a cluster of 1204 nodes eServer BladeCenter (1036 JS20 and 168 JS21, both PowerPC 64 bits). Each JS20 node has two processors IBM PowerPC

single-core 970FX (two cores) with 2.2 GHz, 4 GB of RAM and 40 GB of local hard disk. On the other hand, each JS21 node has two processors IBM PowerPC dual-core 970FX (four cores) with 2.2 GHz, 8 GB of RAM and 80 GB of local hard disk. It was installed in 2006 and reached the 9th fastest in Europe and the 34th in the world (Top 500: List from November 2006). In May 2008 it was upgraded to reach 16 TFLOPS. This powerful cluster has allowed us to fill the gap between the commutative and the noncommutative case.

Next we present the results obtained from our classification (Table 1). Let us compare the number of S_3 -equivalence classes, semifield planes, and coordinatizing finite semifields which were found, with those previously known [15].

Number of classes	S_3 -action	Isotopy	Isomorphism
Previously known	7	19	27313
Actual number	9	23	85877

Table 1: Number of division algebras with 243 elements

As we can see two new S_3 -classes exist, that can not be constructed from commutative semifields. And four new semifield planes of such an order appear. Next we present standard bases of these classes (A_1 is always the identity matrix) (Table 2).

#	A_2	A_3	A_4	A_5	# Semifield
I	129317742	43151760	25524498	2715668620	\mathbb{F}_{3^5}
II	129317638	44994959	28587138	1226007534	Albert's twisted field
III	129317781	52757047	20739470	3274303432	Albert's twisted field
IV	129317742	43393513	26923067	2713804376	Coulter-Matthews'
V	129317742	43215002	26537147	2719346408	Ding-Yuan's
VI	129317742	43185096	19259172	2718371119	[15]
VII	129317742	43215002	26558192	2719382129	[15]
VIII	129317636	14673002	1139489406	3073918154	-
IX	129317636	18089998	3416237282	1030364558	-

Table 2: Standard bases of division algebras with 243 elements (VIII and IX are new semifields)

For these semifields, we have computed some information (see [14] for the notation and details). Namely, the order of their center and nuclei, $ZN = (Z, N, N_l, N_m, N_r)$, the list of all principal isotopes, and the order of their isomorphism groups. The length of the orbits in the fundamental triangle (L_x, L_∞, L_y) was also computed given in the form $\sum_{i=1}^r a_i[b_i]$, if a_i cycles of length b_i ($i = 1, \dots, r$) exist. Also, where possible, some information on the autotopism group has been include (Table 3).

Acknowledgments

This work has been partially supported by MEC - MTM - 2010 - 18370 - C04 - 01, IB08-147, MEC-TIN-2007-61273 and MICINN-TIN-2010-14971. The authors thankfully acknowledge the computer resources, technical expertise and assistance provided by the *Centro de Supercomputación y Visualización de Madrid (CeSViMa)* and the Spanish Supercomputing Network.










Plane	S_3 - class	$ \text{At} $	(L_x, L_∞, L_y)	S/A sum	ZN
I		292820	$2[1] + 1[242]$ $2[1] + 1[242]$ $2[1] + 1[242]$	$\frac{1}{5}$	(243, 243, 243, 243, 243)
II		2420 Solvable	$2[1] + 1[242]$ $2[1] + 1[242]$ $2[1] + 1[242]$	$\frac{24}{1} + \frac{1}{5}$	(3, 3, 3, 3, 3)
III		2420 Solvable	$2[1] + 1[242]$ $2[1] + 1[242]$ $2[1] + 1[242]$	$\frac{24}{1} + \frac{1}{5}$	(3, 3, 3, 3, 3)
IV		20 $\mathbb{Z}_2 \times \mathbb{Z}_{10}$	$2[1] + 1[2] + 24[10]$ $2[1] + 1[2] + 24[10]$ $2[1] + 1[2] + 24[10]$	$\frac{2928}{1} + \frac{1}{5}$	(3, 3, 3, 3, 3)
V		20 $\mathbb{Z}_2 \times \mathbb{Z}_{10}$	$2[1] + 1[2] + 24[10]$ $2[1] + 1[2] + 24[10]$ $2[1] + 1[2] + 24[10]$	$\frac{2928}{1} + \frac{1}{5}$	(3, 3, 3, 3, 3)
VI		20 $\mathbb{Z}_2 \times \mathbb{Z}_{10}$	$2[1] + 1[2] + 24[10]$ $2[1] + 1[2] + 24[10]$ $2[1] + 1[2] + 24[10]$	$\frac{2928}{1} + \frac{1}{5}$	(3, 3, 3, 3, 3)
VII		220 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times (\mathbb{Z}_5 \times \mathbb{Z}_{11})$	$2[1] + 1[22] + 2[110]$ $2[1] + 1[22] + 2[110]$ $2[1] + 1[22] + 2[110]$	$\frac{266}{1} + \frac{1}{5}$	(3, 3, 3, 3, 3)
VIII		4 $\mathbb{Z}_2 \times \mathbb{Z}_2$	$2[1] + 121[2]$ $2[1] + 121[2]$ $2[1] + 121[2]$	$\frac{14641}{1}$	(3, 3, 3, 3, 3)
IX		4 $\mathbb{Z}_2 \times \mathbb{Z}_2$	$2[1] + 121[2]$ $2[1] + 121[2]$ $2[1] + 121[2]$	$\frac{14641}{1}$	(3, 3, 3, 3, 3)

Table 3: Division algebras with 243 elements and their properties

References

- [1] A. A. Albert, *Finite division algebras and finite planes*, Proceedings of Symposia in Applied Mathematics **10** (1960), 53-70.
- [2] 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.
- [3] M. Cordero, G. P. Wene, *A survey of finite semifields*, Discrete Mathematics **208/209** (1999), 125-137.
- [4] U. Dempwolff, *Semifield Planes of Order 81*, J. of Geometry **89** (2008), 1-16.
- [5] S. González, C. Martínez, I.F. Rúa, *Symplectic Spread based Generalized Kerdock Codes*, Designs, Codes and Cryptography **42 (2)** (2007), 213–226.
- [6] M. Hall(Jr.), *The theory of groups*, Macmillan, (1959).
- [7] I.R. Hentzel, I. F. Rúa, *Primitivity of Finite Semifields with 64 and 81 elements*, International Journal of Algebra and Computation **17 (7)** (2007), 1411-1429.
- [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] Kleinfeld, E. Techniques for enumerating Veblen-Wedderburn systems. J. Assoc. Comp. Mach. **1960**, 7, 330-337.
- [11] D.E. Knuth, *Finite semifields and projective planes*, Journal of Algebra **2** (1965), 182-217.
- [12] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of mathematics and its applications 20, Addison-Wesley (1983).
- [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] I. F. Rúa, Elías F. Combarro, J. Ranilla, *Classification of Semifields of Order 64*, J. of Algebra, **322 (11)** (2009), 941-961.
- [15] I. F. Rúa, Elías F. Combarro, *Commutative semifields of order 3^5* , (submitted, 2009).
- [16] R. J. Walker, *Determination of division algebras with 32 elements*, Proceedings in Symposia of Applied Mathematics **75** (1962), 83-85.