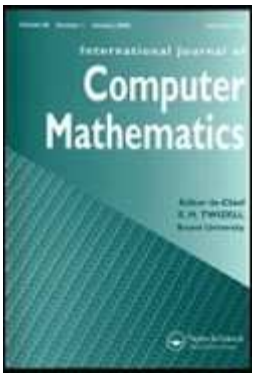
New advances in the computational exploration of semifields (CMMSE-09)

Ignacio Fernandez Rua, Elías Fernandez-Combarro, José Ranilla



New advances in the computational exploration of semifields (CMMSE-09)

Journal:	*International Journal of Computer Mathematics*
Manuscript ID:	GCOM-2009-0778-B.R3
Manuscript Type:	Review
Date Submitted by the Author:	21-Oct-2010
Complete List of Authors:	Rua, Ignacio; Universidad de Oviedo Fernandez-Combarro, Elías; Universidad de Oviedo Ranilla, José; Universidad de Oviedo
Keywords:	finite semifield, finite division ring, computational methods, classification, primitivity

New advances in the computational exploration of semifields

Elías F. Combarro* I.F. Rúa† J. Ranilla*

Abstract

Finite semifields (finite non necessarily associative division rings) have traditionally been considered in the context of finite geometries (they coordinatize projective semifield planes). New applications to coding theory, combinatorics and graph theory have broaden the potential interest in these rings.

We show recent progress in the study of these objects with the help of computational tools. In particular, we state results on the classification and primitivity of semifields obtained with the help of advanced and efficient implementations (both sequential and parallel) of different algorithms specially designed to manipulate these objects.

1 Introduction

A finite semifield (or finite division ring) D is a finite nonassociative ring with identity such that the set $D^* = D \setminus \{0\}$ is closed under the product, i.e., it is a loop [12, 4]. Finite semifields have been traditionally considered in the context of finite geometries since they coordinatize projective semifield planes [12]. Recent applications to coding theory [7, 9], combinatorics and graph theory [15], have broadened the potential interest in these rings.

Because of their diversity, the obtaining of general theoretical algebraic results seems to be a rather difficult (and challenging) task ([2, 16, 17]). On the other hand, because of their finiteness, computational methods can be naturally considered in the study of these objects. So, the classification of finite semifields of a given order is a rather natural problem to use computations. For instance, computers were used in the classification of semifields or orders 16 [11] and 32 [21, 12]. These results date back 40 years, when computers were being incorporated to scientific research. In [11], a complete account of the study of finite semifields in the first decades of the 20th century can be found.

In the last few years there is a renovated interest on the study of semifields with the help of computational methods. So, in [10] a quest for the study of semifields of order at most 256 is launched: *These computer-assisted results used very weak computers by modern standards;*

*Artificial Ingelligence Center, University of Oviedo, {elias,ranilla}@aic.uniovi.es. Partially supported by MICINN-TIN2010-14971, MEC-TIN2007-61273 and MEC-TIN2007-29664E

†Departamento de Matemáticas, Universidad de Oviedo, rua@uniovi.es . Partially supported by MEC-MTM2007-67884 C04-01 and IB08-147

it is surprising that there has not yet been an enumeration of all semifields of order at most 256 since the resulting data might be useful for finding new general constructions. This lead U. Dempwolff to describe in [5] all finite semifields of order 81 (independently this classification was also achieved by the first two authors [3]), and to the classification of semifields of order 64 which has been recently obtained by the three authors [19]. On the other hand, motivated by complete different reasons, in [18, 8], the primitivity of semifields of orders 32, 64 and 81 was considered.

In this paper we present the computational methods that we have implemented to deal with different problems in semifields, and the recent results we have obtained with these implementations. In particular, we will show the state of the art on the classification and primitivity problems.

The structure of the paper is as follows. In §2, basic properties of finite semifields are reviewed. Section §3 describes the algorithms specially designed to explore finite semifields. Finally, in §4, we present new advances on the classification and primitivity of semifields obtained with implementations of the previous algorithms.

2 Preliminaries

In this section we collect definitions and facts on finite semifields. Proofs can be found, for instance, in [12, 4].

A finite nonassociative ring D is called **presemifield**, if the set of nonzero elements D^* is closed under the product. If D has an identity element, then it is called **(finite) semifield**. If D is a finite semifield, then D^* is a multiplicative loop. That is, there exists an element $e \in D^*$ (the identity of D) such that $ex = xe = x$, for all $x \in D$ and, for all $a, b \in D^*$, the equation $ax = b$ (resp. $xa = b$) has a unique solution.

Apart from finite fields (which are obviously finite semifields), *proper* finite semifields were first considered by L.E. Dickson [6] and were deeply studied by A.A. Albert [1]. The term *finite semifield* was introduced in 1965 by D.E. Knuth [12]. These rings play an important role in the study of certain projective planes, called *semifield planes* [12].

The characteristic of a finite presemifield D is a prime number p, and D is a finite-dimensional algebra over $GF(q)$ ($q = p^c$) of dimension d, for some $c, d \in \mathbb{N}$, so that $|D| = q^d$. If D is a finite semifield, then $GF(q)$ can be chosen to be 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 [4].

Isomorphism of presemifields is defined as usual for algebras, and the classification of finite semifields up to isomorphism can be naturally considered. Because of the connections to finite geometries, we must also consider the following notion. If D_1, D_2 are two presemifields over the same prime field $GF(p)$, then an **isotopy** between D_1 and D_2 is a triple (F, G, H) of bijective linear maps $D_1 \to D_2$ over $GF(p)$ such that

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

Clearly, any isomorphism between two presemifields is an isotopy, but the converse is not necessarily true. Any presemifield is isotopic to a finite semifield [12, Theorem 4.5.4]. From a

presemifield D, a projective plane $\mathcal{P}(D)$ can be constructed. We refer to [12] for the details. Theorem 6 in [1] shows that isotopy of finite semifields is the algebraic translation of the isomorphism between the corresponding projective planes. Two finite semifields D_1, D_2 are isotopic if, and only if, the projective planes $\mathcal{P}(D_1), \mathcal{P}(D_2)$ are isomorphic.

If $\mathcal{B} = [x_1, \ldots, x_d]$ is a $GF(q)$-basis of a presemifield D, then there exists a unique set of constants $\mathbf{A}_{D,\mathcal{B}} = \{A_{i_1 i_2 i_3}\}_{i_1,i_2,i_3=1}^{d} \subseteq GF(q)$ such that

$$x_{i_1} x_{i_2} = \sum_{i_3=1}^{d} A_{i_1 i_2 i_3} x_{i_3} \ \forall i_1, i_2 \in \{1, \ldots, d\}$$

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.

A remarkable fact is that permutation of the indexes of a 3-cube preserves the absence of nonzero divisors. Namely, if D is a presemifield, and $\sigma \in S_3$ (the symmetric group on the set $\{1, 2, 3\}$), then the set

$$\mathbf{A}^{\sigma}_{D,\mathcal{B}} = \{A_{i_{\sigma(1)} i_{\sigma(2)} i_{\sigma(3)}}\}_{i_1,i_2,i_3=1}^{d} \subseteq GF(q)$$

is the 3-cube of a $GF(q)$-algebra $D^{\sigma}_{\mathcal{B}}$ without zero divisors [12, Theorem 4.3.1]. Notice that, in general, different choices of bases $\mathcal{B}, \mathcal{B}'$ lead to nonisomorphic presemifields $D^{\sigma}_{\mathcal{B}}, D^{\sigma}_{\mathcal{B}'}$. However, these presemifields are always isotopic [12, Theorems 4.4.2 and 4.2.3].

By [12][Theorem 5.2.1], up to six projective planes can be constructed from a given finite semifield D using the transformations of the group S_3. Actually, S_3 acts on the set of semifield planes of a given order. 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.

With the help of 3-cubes the construction of finite semifields of a given order can be rephrased as a matrix problem [5][8, Proposition 3].

Proposition 1. *There exists a finite semifield D of dimension d over its center $Z(D) \supseteq GF(q)$ if, and only if, there exists a set of d matrices $\{A_1, \ldots, A_d\} \subseteq GL(d, q)$ (the set of invertible matrices of size d over the Galois field $GF(q)$) such that:*

1. *A_1 is the identity matrix I;*
2. *$\sum_{i=1}^{d} \lambda_i A_i \in GL(d, q)$, for all $(\lambda_1, \ldots, \lambda_d) \in GF(q)^d \setminus \{\underline{0}\}$.*
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 standard basis of $GF(q)^d$. In [5], $B_{\Sigma} = (A_1, A_2, ..., A_d)$, and the linear span $\Sigma =< A_1, A_2, ..., A_d >$ are called standard basis *and* semifield spread set (SSS)*, respectively.*

If we identify the elements of $GF(q)$ with the natural numbers 0 to $q-1$ (in a certain way), then we can use the following convention to represent a semifield D of dimension d over $GF(q)$ (this will be useful to shorten the tables containing our results in Section 4). Let

$B_\Sigma = (A_1, \ldots, A_d)$ be one of its standard bases . Recall that the first column of A_i has a one in the i-th position and zeroes elsewhere. If the remaining columns of A_i are

$$\begin{pmatrix} a_{(d-1)d-1} & \ldots & a_{2d-1} & a_{d-1} \\ \vdots & \vdots & \vdots & \vdots \\ a_{d(d-2)} & \ldots & a_d & a_0 \end{pmatrix}$$

then we will encode A_i as the natural number $\sum_{j=0}^{(d-1)d-1} a_j q^j$ (notice that q is the size of the center of D and so we can compute its powers q^j).

For a concrete representation of the semifield one can identify the semifield with $GF(q)^d$, and the multiplication with $x * y = \sum_{i=1}^{d} x_i A_i y$, i.e., A_i is the matrix of left multiplication by the element e_i, where $\{e_1, \ldots, e_d\}$ is the canonical basis of $GF(q)^d$. So, the elements of the standard basis are coordinate matrices of the linear maps $L_{e_i} : D \to D$, $L_{e_i}(y) = e_i * y$.

Finally, the following result relates the SSS of isotopic finite semifields (cf. [5, Section 2]).

Proposition 2. *If Σ is the SSS of a semifield D of dimension d over its center $GF(q)$, and Σ' is the SSS of an isotope of D, then there exists a matrix $Q \in GL(d, q)$, and $S \in \Sigma$, such that $\Sigma' = Q^{-1}\Sigma S^{-1} Q$.*

3 Algorithms for the computational exploration of semifields

The result stated in Proposition 1 is fundamental for the representation of finite semifields in a computer, since we can represent any finite semifield by one of its standard basis, i.e., by a set of ordered matrices of fixed size over a finite field. This was also the way semifields were represented in [21] or, more recently, in [8, 5, 19].

It is clear that a finite semifield can be represented by a big amount of different standard bases. Namely, any choice of basis of the corresponding vector space (such that the first element is the identity) induces one of those standard bases. So, in order to reduce the amount of different representations we deal only with *cyclic* representations.

Definition 1. A finite semifield D, of dimension d over its center $Z(D)$, is called

- **Left cyclic**, if there exists $a \in D$ (a left cyclic element) such that:

  $$\{e, a, a^{(2}, \ldots, a^{(d-1}\}$$

  is a $Z(D)$-basis of D.

- **Left primitive**, if there exists $a \in D$ (a left primitive element) such that:

  $$D^* = \{e, a, a^{(2}, a^{(3}, \ldots\}$$

  where $a^{(2} = aa, a^{(3} = aa^{(2}, \ldots$.

Any left primitive semifield is always left cyclic [8, Corollary 1]. First examples of left primitive semifields are associative finite semifields, i.e., finite fields, since the multiplicative group of a finite field is a cyclic group. It was conjectured in [22] that any finite semifield is always left (or right) primitive, but the two examples of 32 and 64 elements mentioned in [18, 8] show that this conjecture is not true. However, even these few nonprimitive semifields are cyclic. The use of cyclic representations has the advantage that computations are reduced significantly. So, if the representation is cyclic (i.e., $e_{i+1} = L^i_{e_2}(e_1)$, where e_1 is the identity of the semifield, and e_2 is a left cyclic element), then the matrix A_2 corresponding to this basis is a companion matrix. We shall show next that we can restrict our exploration to cyclic representations. Namely, we shall prove that all finite semifields of dimension 4 over its center (the cases of interest in this paper) are isotopic to a left cyclic semifield.

Remark 1. If Σ is the SSS of a semifield D with center $GF(q)$, then because of [1][Lemma 5], the characteristic polynomial of any matrix in $\Sigma \setminus \{\lambda I \mid \lambda \in GF(q)\}$ has no linear factors. We will say that a monic polynomial is *admissible* if it has no linear factors. On the other hand, if a D is left primitive, then it has a standard basis such that A_2 is a companion matrix whose characteristic polynomial is primitive (i.e. its multiplicative order is $\#D^*$) [8, Proposition 2, Corollary 1].

Proposition 3. *If D is a finite semifield, of dimension 4 over its center $Z(D) = GF(q)$, then there exists a left cyclic isotope D' of D.*

Proof. First of all, we shall show that there exists an element $b \in D \setminus GF(q)$ (i.e., *non-scalar*) such that the characteristic polynomial of L_b is either irreducible, or the product of two irreducible polynomials of degree two.

If $q = 2^c$, i.e., if the characteristic of D is 2, then from a similar argument to [1, Lemma 6] (there on the right, here on the left), there exists a non-scalar $b \in D \setminus GF(q)$ such that the characteristic polynomial of L_b has the form:

$$x^4 + c_1x^3 + c_3x + c_4$$

where $c_1, c_3, c_4 \in GF(q)$. From the previous remark, this polynomial does not have linear factors so we need only to show that it is not the square of an irreducible quadratic polynomial to prove our claim. If there exist $\alpha, \beta \in GF(q)$ such that

$$x^4 + c_1x^3 + c_3x + c_4 = (x^2 + \alpha x + \beta)^2 = x^4 + \alpha^2x^2 + \beta^2$$

then $c_1 = c_3 = 0, \alpha^2 = 0$ and $\beta^2 = c_4$. Since $q = 2^c$, all elements in $GF(q)$ are squares [14], so there exists $\gamma \in GF(q)$ such that

$$x^4 + c_4 = x^4 + \gamma^4 = (x + \gamma)^4$$

a contradiction, since this polynomial can not have linear factors.

If the characteristic of D is not 2, then we fix $\{x_1, x_2, x_3, x_4\}$ a $GF(q)$-basis of D, and consider the characteristic polynomial of L_b for a generic element $b = \lambda_1x_1 + \lambda_2x_2 + \lambda_3x_3 + \lambda_4x_4 \in D$:

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

where $\rho_i(\overline{\lambda})$ is a homogeneous polynomial in $GF(q)[\lambda_1, \lambda_2, \lambda_3, \lambda_4]$, of degree i. Consider the system of equations $\rho_1(\overline{\lambda}) = \rho_2(\overline{\lambda}) = 0$. From the Chevalley-Warning theorem [14, 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

$$x^4 + c_3x + c_4$$

where $c_3, c_4 \in GF(q)$. If this polynomial is a square

$$x^4 + c_3x + c_4 = (x^2 + \alpha x + \beta)^2 = x^4 + 2\alpha x^3 + (2\beta + \alpha^2)x^2 + 2\alpha\beta x + \beta^2$$

then $2\alpha = 0$, i.e. $\alpha = 0$, and $2\beta + \alpha^2 = 0$, i.e. $\beta = 0$, so that the polynoimial is x^4 and it has linear factors, which is not possible. Moreover, b can not be a scalar ($b \in GF(q)$), because in such a case the polynomial is $(x - b)^4$, and so it also has linear factors.

Let us finally show that this element guarantees the existence of an isotope in the conditions of the proposition. Since the characteristic polynomial $p(x)$ of L_b is either irreducible, or the product of two irreducible polynomials of degree two, we have that the minimal polynomial of L_b is exactly $p(x)$ [13, Chapter III, Theorem 13]. Moreover, there exists an element $f \in D$ such that the minimal polynomial of $L_b|_{<f>}$ is $p(x)$ [13, Chapter III, Theorem 1] ($L_b|_{<f>}$ denotes the restriction of the linear map L_b to the vector subspace generated by the element f). Consider the following multiplication in D:

$$x * y = R_f^{-1}(x)y$$

where $R_f : D \to D, R_f(x) = xf$. Then, $(D, +, *) = D'$ is an isotope of D with unit f and the multiplication by the element bf has the following property:

$$L^*_{bf}(y) = (bf) * y = R_f^{-1}(bf)y = by = L_b(y)$$

Hence, bf is a left cyclic element in D'. □

Next, we describe the algorithms that we have implemented to explore finite semifields. In particular, we present those who have been used to generate all finite semifields of dimension 4 over $GF(5)$ and $GF(4)$. As we have previously proved, any semifield of this type is isotopic to another one that can be described by a standard basis (a tuple of 4 matrices satisfying certain conditions, in particular $A_1 = I$ and A_2 a companion matrix). So, the output of the algorithm will be tuples of matrices which correspond to finite semifields. Not all possible tuples satisfying the conditions of Proposition 1 will be listed. It is only necessary to obtain representatives of all S_3-equivalence classes.

The first algorithm, a backtracking method (cf. [21]) for searching standard bases, is written below with the help of two auxiliary functions. The first one (*Complete*) enumerates all valid semifields with given initial *partial* standard basis, i.e., a tuples $(A_1, \ldots, A_i)$ that can be potentially extended to a standard basis. The second one (*Complete2*) enumerates all valid semifield with given partial standard basis and some columns of the next matrix in the standard basis. The function *Complete* uses the already known partial standard basis to create the initial columns of the next matrix and then calls *Complete2*. This second function, in turn, recursively adds columns to the incomplete matrix (backtracking if necessary) and then calls *Complete* with a new partial standard basis.

Algorithm 1: Search algorithm for standard bases of finite semifields of dimension 4

- **Input:** Size of the center $p = 4, 5$, and a fixed companion matrix A_2
- **Output:** List of standard bases with second matrix A_2 representing semifields with given center
- **Procedure:**

Create an empty list of matrices L
Insert the identity I in L
Insert A_2 in L
Call $Complete(L, p)$

Algorithm 2: Function $Complete$

- **Input:** A list of partial standard bases L, and the size of the center $p = 4, 5$
- **Output:** List of matrices representing all the semifields with partial standard basis in the list L, of the given center
- **Procedure:**

$m \leftarrow$ size of L
if m is equal to 4 **then**
  return $\{L\}$
end
else
  Create a matrix M of 1 column
  Set the first column of M equal to the $(m+1)$-th column of the identity
  Return $Complete2(L, M, p)$
end

Algorithm 3: Function $Complete2$

- **Input:** A list of partial standard bases L, a truncated matrix M, and the size of the center $p = 4, 5$
- **Output:** List of standard bases representing all the semifields with partial standard bases L (containing M), of the given center
- **Procedure:**

$k \leftarrow$ number of columns of M
if k is equal to 4 **then**
  Insert M in L
  Return $Complete(L, p)$
end
else
  Create an empty list W
  Compute C, the list of columns c such that the join of M and c is

linearly independent of the matrices of L (truncated at the $k+1$ first columns)
for each c in C **do**
Join c to M, as its $k+1$-th column
$W := W \cup Complete2(L, M, p)$
Remove c from M
end
Return W
end

As we can see, a partial standard basis of size 2 is needed to initialize the former algorithm. The next procedure generates the list of such partial standard bases. We generate only *nonequivalent* partial standard basis, i.e., so that none of them can be obtain from any other by means of a transformation of the form of Proposition 2. Also, since S_3-equivalence is considered, we can consider the transpose of the matrices in the list (see [19]).

Algorithm 4: $PartialStandardBasesOfSize2$

- **Input:** None
- **Output:** A set of nonequivalent partial bases (of size 2) of semifields of dimension 4 over the center $GF(p), p = 4, 5$
- **Procedure:**

$T := \emptyset$ // `Set of nonequivalent partial standard bases`
$C := \{Companion\ matrices\ with\ admissible\ characteristic\ polynomial\}$
for A_2 in C **do**
$T := T \cup \{(I, A_2)\}$
end
for A in T **do** // `Removal of partial standard bases equivalent to A`
for Σ in $\{< I, A_2 >, < I, A_2^t >\}$ **do**
for S in Σ **do** // `Generation of partial standard bases equivalent to A`
for $E \in \Sigma, Q \in GL(4, p)$ such that $Q^{-1}ES^{-1}Q$ is in C **do** // `New matrix` A_2
if $(I, Q^{-1}ES^{-1}Q) \neq A$ **then**
Remove $(I, Q^{-1}ES^{-1}Q)$ from T
end
end
end
end
end
return T

4 New advances in the exploration of semifields

Next we show our recent advances in the exploration of finite semifields obtained with the implementation of the algorithms presented in the previous section. In order to reduce computation times we have used adequate implementations in language C using Streaming SIMD Extensions. Moreover, shared and distributed parallel programming techniques have been used when the computational intensity is very high. This approach proved to be specially suitable in the manipulation of semifields in [8] and was later confirmed with the experiments which lead to the classification of semifields or order 81. These rings were classified in [5] *in a few days on a PC*, using implementations in `GAP` [20]. Independently, this classification was achieved in a few minutes using our implementations in C language [3]. Of course, GAP provides powerful routines to deal with known structures, such as finite fields. However, C provides astonishingly fast procedures. Also, parallel processing has been considered just like in the case of exploration of finite semifields of order 64 [19]. Our new results include the classification of finite semifields of orders 5^4 and 4^4 (in this case with center $Z \supseteq GF(4)$), and the study of primitivity of commutative semifields of order 128.

4.1 Semifields of order 5^4

A total amount of 42 S_3-classes of semifields of order 5^4 exist. The concrete description of representatives of these classes is contained in the Table 1. $GF(5)$ is identified with the natural numbers 0 to 4. Notice that I is the finite field $GF(625)$.

4.2 Semifields of order 4^4 and center $Z \supseteq GF(4)$

A total amount of 28 S_3-classes of semifields of order 4^4 (with center $Z \supseteq GF(4)$) exist. The concrete description of representatives of these classes is contained in the Table 2. Here $GF(4) = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$ is identified with the set $\{0, 1, 2, 3\}$. Notice that I is the finite field $GF(256)$.

4.3 Primitivity of commutative semifields of order 128

A complete study of primitivity of commutative semifields of order 128 was carried out with our implementations. The only modification in the algorithm presented in the previous section consists in checking, while generating a partial standard basis, whether the conditions on the characteristic polynomials of the SSS are satisfied or not (Remark 1). Unfortunatedly, no new nonprimitive semifield was found. This is the last step in the quest of these semifields, which we summarize in the Table 3.

5 Conclusions

We have considered a series of algorithms and methods to explore finite semifields. The implementation of these methods have been used to study the primitivity of commutative semifields of order 128 and the classification of semifields of orders 5^4 and 4^4 (in this case with center

#	A_2	A_3	A_4	(Z, N, N_l, N_m, N_r)
I	1954030	565681	109410291	$(625, 625, 625, 625, 625)$
II	1954030	469480	70893499	$(5, 5, 5, 5, 5)$
III	1954030	469480	81926092	$(5, 5, 5, 5, 5)$
IV	1954030	469480	109706214	$(5, 5, 5, 5, 5)$
V	1954030	469480	115187757	$(5, 5, 5, 5, 5)$
VI	1954030	469480	219662859	$(5, 5, 5, 5, 5)$
VII	1954030	469480	224156783	$(5, 5, 5, 5, 5)$
VIII	1954030	469831	49975531	$(5, 5, 5, 5, 5)$
IX	1954030	469831	51050463	$(5, 5, 5, 5, 5)$
X	1954030	469831	162916061	$(5, 5, 5, 5, 5)$
XI	1954030	469831	209752465	$(5, 5, 5, 5, 5)$
XII	1954030	470801	56951034	$(5, 5, 5, 5, 5)$
XIII	1954030	470801	97596661	$(5, 5, 5, 5, 5)$
XIV	1954030	484619	231520988	$(5, 5, 5, 5, 5)$
XV	1954030	488868	76607761	$(5, 5, 5, 5, 5)$
XVI	1954030	489303	92517950	$(5, 5, 5, 5, 5)$
XVII	1954030	489303	135078936	$(5, 5, 5, 5, 5)$
XVIII	1954030	489303	178662102	$(5, 5, 5, 5, 5)$
XIX	1954030	492721	78475264	$(5, 5, 5, 5, 5)$
XX	1954030	492721	88167145	$(5, 5, 5, 5, 5)$
XXI	1954030	493317	183329012	$(5, 5, 5, 5, 5)$
XXII	1954030	500445	221902310	$(5, 5, 5, 5, 5)$
XXIII	1954030	500933	118596969	$(5, 5, 5, 5, 5)$
XXIV	1954030	512497	97541900	$(5, 5, 5, 5, 5)$
XXV	1954030	512497	204964393	$(5, 5, 5, 5, 5)$
XXVI	1954030	513265	151861995	$(5, 5, 5, 5, 5)$
XXVII	1954030	520378	81047410	$(5, 5, 5, 5, 25)$
XXVIII	1954030	524367	81105195	$(5, 5, 5, 5, 5)$
XXIX	1954030	864819	65692963	$(5, 5, 5, 25, 5)$
XXX	1954030	866032	91203403	$(5, 5, 5, 5, 5)$
XXXI	1954030	875046	223896265	$(5, 5, 5, 5, 5)$
XXXII	1954030	882554	128424368	$(5, 5, 5, 5, 5)$
XXXIII	1954030	955963	86412805	$(5, 5, 5, 5, 5)$
XXXIV	1954030	992164	91135073	$(5, 5, 5, 5, 25)$
XXXV	1954030	995510	73227955	$(5, 5, 5, 5, 25)$
XXXVI	1954030	1020155	129680821	$(5, 5, 25, 5, 5)$
XXXVII	1954030	1020155	137293666	$(5, 5, 25, 5, 5)$
XXXVIII	1954030	1167110	126378035	$(5, 5, 5, 5, 25)$
XXXIX	1954030	1259745	165287727	$(5, 5, 5, 25, 5)$
XL	1954030	7195668	86845792	$(5, 5, 25, 25, 25)$
XLI	1954030	12300642	137293666	$(5, 5, 25, 25, 25)$
XLII	1954030	23419082	74656357	$(5, 5, 25, 25, 25)$

Table 1: Semifields of order 5^4 (A_1 is always the identity)

#	A_2	A_3	A_4	(Z, N, N_l, N_m, N_r)
I	262580	111661	11808191	$(256, 256, 256, 256, 256)$
II	262580	83501	4780498	$(4, 4, 4, 4, 4)$
III	262580	83697	5132708	$(4, 4, 4, 4, 4)$
IV	262580	83697	8282791	$(4, 4, 4, 4, 4)$
V	262580	83697	9838330	$(4, 4, 4, 4, 4)$
VI	262580	83697	13430083	$(4, 4, 4, 4, 4)$
VII	262580	83697	15276284	$(4, 4, 4, 4, 4)$
VIII	262580	83733	9867916	$(4, 4, 4, 4, 4)$
IX	262580	83739	5449621	$(4, 4, 4, 4, 4)$
X	262580	83739	9544454	$(4, 4, 4, 4, 4)$
XI	262580	84816	5026619	$(4, 4, 4, 4, 4)$
XII	262580	84816	10383745	$(4, 4, 4, 4, 4)$
XIII	262580	84986	5462727	$(4, 4, 4, 4, 4)$
XIV	262580	84986	14115647	$(4, 4, 4, 4, 4)$
XV	262580	85585	7287796	$(4, 4, 4, 4, 4)$
XVI	262580	86757	4757187	$(4, 4, 4, 4, 4)$
XVII	262580	89416	4751452	$(4, 4, 4, 4, 4)$
XVIII	262580	91787	14663856	$(4, 4, 4, 4, 4)$
XIX	262580	93086	5121786	$(4, 4, 4, 4, 4)$
XX	262580	94652	14400687	$(4, 4, 4, 4, 4)$
XXI	262580	148118	10055074	$(4, 4, 4, 4, 4)$
XXII	262580	149049	11399190	$(4, 4, 4, 4, 4)$
XXIII	262580	154590	13245222	$(4, 4, 4, 4, 4)$
XXIV	262580	177536	4815767	$(4, 4, 16, 4, 4)$
XXV	262580	177536	6834559	$(4, 4, 16, 4, 4)$
XXVI	262580	177536	14130408	$(4, 4, 16, 4, 4)$
XXVII	262580	637170	11675230	$(4, 4, 16, 16, 16)$
XXVIII	262580	897096	5396188	$(4, 4, 16, 16, 16)$

Table 2: Semifields of order 256 with center $Z \supseteq GF(4)$ (A_1 is always the identity)

Order	**8**	**16**	**32**	**64**	**81**	**128**
Number of nonprimitive semifields	0	0	1	1	0	**0 (commutative)**

Table 3: Number of nonprimitive semifields

$Z \supseteq GF(4)$). Our approach has proved to be quite useful, since we have classified semifields which were not previously reachable (because of the computation complexity, which increases exponentially on the dimension of the semifield). We summarize the known results on the classification of semifields in Table 4. Results obtained by our methods are included in boldface.

Number of S_3-classes	**d = 3**	**d = 4**	**d = 5**	**d = 6**
q = 2	1	3	3	**80**
q = 3	2	**12**	?	?
q = 4	2	**28**	?	?
q = 5	3	**42**	?	?

Table 4: Finite semifields of dimension d over $Z \supseteq GF(q)$

6 Acknowledgment

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.

References

[1] A. A. Albert, *Finite division algebras and finite planes*, Proceedings of Symposia in Applied Mathematics **10** (1960), 53-70.

[2] I. Cardinali, O. Polverino, R. Trombetti, *Semifield planes of order q^4 with kernel F_{q^2} and center F_q*, European J. Combin. **27** (2006), 940-961.

[3] E. F. Combarro, I. F. Rúa, *New Semifield Planes of order 81*, (2008) (unpublished).

[4] M. Cordero, G. P. Wene, *A survey of finite semifields*, Discrete Mathematics **208/209** (1999), 125-137.

[5] U. Dempwolff, *Semifield Planes of Order 81*, J. of Geometry **89** (2008), 1-16.

[6] L. E. Dickson, *Linear algebras in which division is always uniquely possible*, Transactions of the American Mathematical Society **7** (1906), 370-390.

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

[8] 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.

[9] 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.

[10] 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).

[11] E. Kleinfeld, *A history of finite semifields*, Lecture Notes in Pure and Appl. Math. **82**, Dekker, New York, 1983.

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

[13] N. Jacobson, *Lectures in Abstract Algebra. II. Linear Algebra*, Springer-Verlag (1953).

[14] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of mathematics and its applications 20, Addison-Wesley (1983).

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

[16] G. Menichetti, *On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field*, Journal of Algebra **47** (1977), 400-410.

[17] G. Menichetti, *$n-$dimensional algebras over a field with a cyclic extension of degree n*, Geom. Dedicata **63(1)** (1996), 69-94.

[18] I. F. Rúa, *Primitive and non primitive finite semifields*, Communications in Algebra, **32 (2)** (2004), 793-803

[19] I. F. Rúa, Elías F. Combarro, J. Ranilla, *Classification of Semifields of Order 64*, J. of Algebra **3 22** (11) (2009), 4011-4029.

[20] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, (2008)

[21] R. J. Walker, *Determination of division algebras with 32 elements*, Proceedings in Symposia of Applied Mathematics **75** (1962), 83-85.

[22] G. P. Wene, *On the multiplicative structure of finite division rings*, Aequations Mathematicae **41** (1991), 222-233.