Symplectic 4-dimensional semifields of order $8^4$ and $9^4$

Michel Lavrauw$^{1,2,3}$ · John Sheekey$^4$

Received: 13 July 2022 / Revised: 23 December 2022 / Accepted: 5 January 2023 / Published online: 5 February 2023
© The Author(s) 2023

Abstract
We classify symplectic 4-dimensional semifields over $\mathbb{F}_q$, for $q \leq 9$, thereby extending (and confirming) the previously obtained classifications for $q \leq 7$. The classification is obtained by classifying all symplectic semifield subspaces in $\text{PG}(9, q)$ for $q \leq 9$ up to $K$-equivalence, where $K \leq \text{PGL}(10, q)$ is the lift of $\text{PGL}(4, q)$ under the Veronese embedding of $\text{PG}(3, q)$ in $\text{PG}(9, q)$ of degree two. Our results imply the non-existence of non-associative symplectic 4-dimensional semifields for $q$ even, $q \leq 8$. For $q$ odd, and $q \leq 9$, our results imply that the isotopism class of a symplectic non-associative 4-dimensional semifield over $\mathbb{F}_q$ is contained in the Knuth orbit of a Dickson commutative semifield.

Keywords
Semifield · Commutative · Symplectic · Veronese variety

Mathematics Subject Classification
12K10 · 51A35 · 51A50 · 51E23

1 Introduction

A finite semifield is a division algebra in which multiplication is not assumed to be associative. Finite semifields were introduced by Leonard Eugene Dickson at the beginning of the 20th century and are well studied objects in algebra, finite geometry and combinatorics, with applications in coding theory and cryptography, through their connections with projective
planes, MRD codes, PN functions and S-boxes. Commutative semifields are of special interest because the Knuth orbits of their isotopism classes contain the isotopism classes of symplectic semifields which in turn give rise to symplectic spreads, Dembowski–Ostrom polynomials, and Hadamard difference sets. There are many constructions of semifields known, most of which are non-commutative. We refer to [11, Sect. 6] for an overview of these constructions and the above mentioned links.

Computational classifications of semifields (n-dimensional over the finite field of order q) have been obtained for q = 2, n ≤ 6; q = 3, n ≤ 5; and q ≤ 5, n ≤ 4. These classifications have a (relatively) long history; the first of these results was obtained in the early days of computational results in mathematics. Kleinfeld [9] classified semifields (at that time called Veblen–Wedderburn systems) of order 16 with the help of a computer in 1960. Knuth used a computer to construct a new semifield of order 32, see [10]. A computational classification of all semifields of order 32 was obtained in 1962 (using a CDC 1604) by Walker [25], and confirmed by Knuth [10] soon after. More recently, computational classifications of semifields were obtained by Dempwolff [6] (\(q^n = 3^4\)), and by Combarro, Ranilla, and Rúa, see [20] (\(q^n = 2^6\)), [21] (\(q^n = 4^4, 5^4\)), [22] (\(q^n = 3^5\)), and [23] (\(q^n = 7^4\)).

Complete computational classifications are also known for certain special type of semifields, see for example [14], in which all 8-dimensional rank 2 commutative semifields are classified, relying on theoretical results from [3] and [12]. A partial classification of commutative semifields of order 35 and 55 can be found in [5], where the authors restrict the classification to commutative semifields whose corresponding Dembowski–Ostrom polynomials have their coefficients in the base field. Theoretical results on rank 3 commutative semifields of dimension at least 6 can be found in [4, 16, 19].

The contribution of this paper is the classification of symplectic semifields of order 84 and 94 with centre containing the fields of order 8 and 9 respectively. This advances the computational classification of symplectic semifields and of commutative semifields with the following theorems as our main results.

**Theorem 1** There exist no non-associative 4-dimensional symplectic semifields over \(\mathbb{F}_q\), q even, \(q \leq 8\).

**Theorem 2** A non-associative 4-dimensional symplectic semifield over \(\mathbb{F}_q\), q odd, \(q \leq 9\) is Knuth-equivalent to a Dickson commutative semifield.

As a corollary we have the following classifications in terms of commutative semifields.

**Corollary 1** There exist no non-associative 4-dimensional commutative semifields over \(\mathbb{F}_q\), q even, \(q \leq 8\).

**Corollary 2** A non-associative 4-dimensional commutative semifield over \(\mathbb{F}_q\), q odd, \(q \leq 9\) is isotopic to a Dickson commutative semifield.

The paper is organised as follows. In Sect. 2 we introduce the necessary notation and terminology. Section 3 contains the description of the algorithms and the proof of the main results. In Sects. 4 and 5 we list the representatives of the \(K\)-orbits of the symplectic semifield lines and of the \(K\)-orbits of two-dimensional symplectic semifield subspaces, under the action of \(K \cong \text{PGL}(4, q)\) in its action on the subspaces of \(\text{PG}(9, q)\), for \(q = 8\) and \(q = 9\).
2 Finite semifields and the associated algebraic varieties

In this section we set up some of the notation and terminology used in the paper. For reasons of brevity, we do not include all of the basic definitions in the theory of semifields; for those we refer the reader to [11].

Throughout this paper, let $q$ be a power of a prime, and denote the finite field of order $q$ by $\mathbb{F}_q$. We consider semifields of dimension $n$ over $\mathbb{F}_q$; that is, division algebras in which multiplication is not assumed to be associative, whose centre contains $\mathbb{F}_q$, and which are $n$-dimensional over $\mathbb{F}_q$. Such semifields are in one-to-one correspondence with semifield spread sets: $n$-dimensional subspaces of $(n \times n)$-matrices over $\mathbb{F}_q$ in which every nonzero element is invertible. We note that we are not assuming a multiplicative identity in the definition of semifield; usually a division algebra without identity is called a presemifield, but we omit this distinction here for convenience and brevity. That we may do so without loss of generality follows from a well-known result which says that every presemifield is isotopic to a semifield, and the fact that we are interested in the classification of semifields up to isotopism.

It is also well-known that each isotopism class $[S]$ of a semifield $S$ gives rise to a total of six isotopism classes of semifields, called the Knuth orbit of $S$. Semifields whose isotopism class belongs to the same Knuth-orbit are called Knuth-equivalent. A semifield is said to be commutative if multiplication is commutative. A semifield is said to be symplectic if the spread it defines in $\text{PG}(2n-1, q)$ (the $(2n - 1)$-dimensional projective space over $\mathbb{F}_q$) consists of totally singular subspaces with respect to some symplectic polarity; i.e. it defines a spread of a symplectic polar space $W(2n-1, q)$. It is well known that a semifield is Knuth-equivalent to a commutative semifield if and only if it is Knuth-equivalent to a symplectic semifield.

In order to make the computational classification feasible we used a geometric approach. Isotopism classes of semifields can be seen as orbits (under a well-defined group action) of subspaces in the space of a Segre variety in a projective space [13]. Applying this connection to 4-dimensional semifields, we end up in a 15-dimensional projective space, which is unfortunately still too large for the parameters of the semifields that we are aiming to classify. However, since we are interested in commutative (or symplectic) semifields, we can reduce our search space to the space of a Veronese variety [13, 15], which in this case is a 9-dimensional projective space over $\mathbb{F}_q$. Below, we give some details of this connection between the algebraic approach and the geometric approach to the isotopism problem for symplectic semifields.

By an appropriate choice $a$ of non-degenerate symplectic bilinear form in $2n$ variables, it can be shown that symplectic semifields are in one-to-one correspondence with $n$-dimensional subspaces of symmetric $(n \times n)$-matrices over $\mathbb{F}_q$ in which every nonzero element is invertible [8]. Since the condition for a matrix to be invertible is invariant under multiplication by a non-zero scalar, it is natural to work in the projective setting, so we denote $N = \binom{n+1}{2}$ and consider $(n - 1)$-dimensional subspaces of $\text{PG}(N-1, q)$. In this projective setting, the points defined by rank one symmetric matrices over $\mathbb{F}_q$ correspond to the $\mathbb{F}_q$-rational points of a Veronese variety, the image of the Veronese map from $\text{PG}(n - 1, q)$ into $\text{PG}(N-1, q)$. We will denote points of a projective space by a letter followed by a tuple of field elements; for example, $p(1, 0, 0, 0)$ denotes a point of $\text{PG}(3, q)$, whose underlying coordinate vector is $(1, 0, 0, 0)$. We identify a point defined by an $(n \times n)$ symmetric matrix $A = (a_{ij})$ with the point $p$ of $\text{PG}(N - 1, q)$ given by $p(a_{11}, a_{12}, \ldots, a_{1n}, a_{22}, \ldots, a_{nn})$; that is, as coordinates we take the upper triangular part of the matrix and then read the entries row by row. We also define the rank of the point $p$ as the the rank of the corresponding matrix $A$. 

Springer
Given this setup, the Veronese variety $\mathcal{V}_{n-1,2}(q)$ is the image of the Veronese map $\nu_{n-1,2}$ defined by

$$\nu_{n-1,2} : \text{PG}(n-1, q) \mapsto \text{PG}(N-1, q)$$

$$: s(a_1, a_2, \ldots, a_n) \mapsto p(a_1^2, a_1a_2, \ldots, a_1a_n, a_2^2, \ldots, a_2a_n, \ldots, a_n^2).$$

That is, the point defined by the row vector $a$ is mapped to the point defined by the matrix $a^T a$. It is easy to see that $\mathbb{F}_q$-rational points on $\mathcal{V}_{n-1,2}(q)$ correspond precisely to points defined by symmetric matrices of rank one under the above mentioned correspondence.

Points of rank two in $\text{PG}(N, q)$, where $N = \binom{n+2}{2} - 1$, are points which belong to the secant variety $\mathcal{V}_{n,2}(q)$ of the Veronese variety $\mathcal{V}_{n,2}(q)$ but do not belong to $\mathcal{V}_{n,2}(q)$. Similarly, one has the $i$-th secant variety $\mathcal{V}_{n,2}(q)^{(i)}$ of $\mathcal{V}_{n,2}(q)$. It follows that symplectic semifield spread sets correspond to $(n - 1)$-dimensional subspaces of $\text{PG}(N - 1, q)$ disjoint from the $(n - 2)$-nd secant variety $\mathcal{V}_{n-1,2}(q)^{(n-1)}$ of the Veronese variety $\mathcal{V}_{n-1,2}(q)$. Since we will search for symplectic semifield spread sets by classifying all subspaces (of any dimension) disjoint from $\mathcal{V}_{n-1,2}(q)^{(n-1)}$, we introduce the following terminology for convenience.

**Definition 1** A symplectic semifield subspace of $\text{PG}(N - 1, q)$ is a subspace which is disjoint from the $(n - 2)$-nd secant variety $\mathcal{V}_{n-1,2}(q)^{(n-1)}$ of the Veronese variety $\mathcal{V}_{n-1,2}(q)$. If a symplectic semifield subspace is not properly contained in another symplectic semifield subspace, we say that it is maximal. An $(n - 1)$-dimensional symplectic semifield subspace $\text{PG}(N - 1, q)$ is called a maximum symplectic semifield subspace.

The natural definition of equivalence in this setting is equivalence under the group $K \cong \text{PGL}(n, q)$ as a subgroup of $\text{PGL}(N, q)$ stabilising the Veronese variety. The action of $K$ on $\text{PG}(N - 1, q)$ is induced by the action of $\text{GL}(n, q)$ on symmetric matrices given by $A \mapsto XAX^T$. In terms of semifields, this corresponds to the notion of strong isotopy.

We note that the more general definition of equivalence of semifields is using isotopy; this corresponds to equivalence under the action of a subgroup of $\text{PGL}(n^2, q)$ stabilising a Segre variety in $\text{PG}(n^2 - 1, q)$ [13]. It can occur that symplectic semifields are isotopic but not strongly isotopic; see for example [17, 26], but in the cases considered in this paper, these two notions coincide.

### 3 Description of the algorithms and proofs of the main results

The computational classification of symplectic 4-dimensional semifields order $q^4$ for $q \leq 9$ was obtained using GAP [24] and the package FinInG [1] for computations in Finite Incidence Geometry.

Let $K \cong \text{PGL}(4, q)$ denote the subgroup of $\text{PGL}(10, q)$ obtained as the image of the lifting homomorphism of the action of $\text{PGL}(4, q)$ from $\text{PG}(3, q)$ to $\text{PG}(9, q)$ through the quadratic Veronese map as described above. As explained in the previous sections, in order to classify the 4-dimensional symplectic semifields up to isotopism, it suffices to classify their Knuth orbits, and this amounts to classifying the $K$-orbits of solids in $\text{PG}(9, q)$, which are disjoint from the secant variety $\mathcal{V}_{n,2}(q)^{(3)}$. Such solids are called symplectic semifield solids.

Since the problem is equivalent to classifying the $K$-orbits of symplectic semifield solids in $\text{PG}(9, q)$ and there are about $10^{22}/2$ solids in $\text{PG}(9, 8)$, and close to $10^{23}$ solids in $\text{PG}(9, 9)$, a brute force approach is not feasible. The main structure of the algorithm is a breadth first type algorithm with isomorphism rejection under $K$ at every step, based on ideas from the algorithm snakes and ladders as described in [2, Sect. 9.6]. We also used ideas from the orbit
computation functionality provided by the FinInG package [1] and the Orb package [18], whose methods we adjusted and reimplemented, tailored for the specific problem at hand, in order to make the computations feasible.

In order to compute the $K$-orbits on symplectic semifield solids our algorithm computes the $K$-orbits of all symplectic semifield subspaces of projective dimension at most three. Moreover, the algorithm collects interesting data along the way, allowing us to recover the stabiliser groups and maximality of the symplectic semifield subspaces.

We first computed the orbits of $K$ on points of $\text{PG}(9, q)$, and for each point in each orbit an element of $K$ mapping that point to the representative of its orbit. There are two orbits of points of rank four in $\text{PG}(9, q)$ with representatives $p_1(1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$ and $p_2(1, 0, 0, 0, 1, 0, 0, 1, 0, \omega)$, where $\omega$ is a primitive element in $\mathbb{F}_q$.

For each of the representatives $p_i$ and $i = 1, 2$ of the $K$-orbits on points of $\text{PG}(9, q)$, we compute its stabiliser $K_{p_i}$ in $K$ and the orbits of that stabiliser on the symplectic semifield lines through $p_i$.

For each dimension $d \leq 2$, the algorithm stores a list of orbit representatives of $d$-dimensional symplectic semifield subspaces of $\text{PG}(9, q)$, together with a Schreier vector (for constructive recognition) and the stabiliser of the representative. At the next step, for each representative $W$, the algorithm computes the orbits on the set of all possible extensions (to $(d + 1)$-dimensional symplectic semifield subspaces) of $W$ under the stabiliser of $W$. This gives a list of all $(d + 1)$-dimensional symplectic semifield subspaces containing a representative of the $d$-dimensional symplectic semifield subspaces. The list of $(d + 1)$-dimensional symplectic semifield subspaces is then reduced (using the stored Schreier vectors) by removing the representatives from the list which belong to the same $K$-orbit as a representative which comes earlier in the list.

The numbers of symplectic semifield subspaces and of maximal symplectic semifield subspaces in $\text{PG}(9, q)$, for $q \leq 9$, up to $K$-equivalence, are listed in the following two tables below.

For completeness, we include the values for $d = 0$ in Table 1, but note that this follows from the well-known classification of non-singular quadrics in $\text{PG}(3, q)$. The values in Table 1 in the last row for $q = 2, 3, 4, 5, 7$ confirm previous results mentioned in the introduction. The other values in Table 1 are new. The values in the last row give the number of $K$-orbits of symplectic semifield solids and lead to the following classification results.

**Theorem 1** There exist no non-associative $4$-dimensional symplectic semifields over $\mathbb{F}_q$, $q$ even, $q \leq 8$.

**Proof** The values in the last row of Table 1 for $q = 2, 4, 8$ indicate that $K$ acts transitively on the set of semifield solids in $\text{PG}(9, q)$. Let $q \in \{2, 4, 8\}$. Since the finite field $\mathbb{F}_q^4$, when considered as a $4$-dimensional algebra $\mathbb{A}$ over $\mathbb{F}_q$, gives rise to a semifield solid $U$ in $\text{PG}(9, q)$, the unique $K$-orbit of semifield solids equals the orbit of $U$ under $K$. This implies that each $4$-dimensional symplectic semifield over $\mathbb{F}_q$ is isotopic to $\mathbb{A}$, and is therefore associative. □

| $d$ | 2 | 3 | 4 | 5 | 7 | 8 | 9 |
|-----|---|---|---|---|---|---|---|
| $d = 0$ | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| $d = 1$ | 5 | 7 | 9 | 13 | 16 | 17 | 22 |
| $d = 2$ | 6 | 18 | 31 | 59 | 106 | 100 | 149 |
| $d = 3$ | 1 | 2 | 1 | 2 | 2 | 1 | 2 |
Table 2  The number of isotopism classes of maximal symplectic semifield subspaces in PG(9, q)

| q  | 2 | 3 | 4 | 5 | 7 | 8 | 9 |
|----|---|---|---|---|---|---|---|
| d=0| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| d=1| 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| d=2| 5 | 13| 30| 49| 90| 99|124|
| d=3| 1 | 2 | 1 | 2 | 2 | 1 | 2 |

Theorem 2  A non-associative 4-dimensional symplectic semifield over \( \mathbb{F}_q \), q odd, \( q \leq 9 \) is Knuth-equivalent to a Dickson commutative semifield.

Proof  The Dickson commutative semifield, which we denote by \( S_D \), is defined by the binary operation

\[(x, y) \circ (u, v) = (xu + \eta(yv)^\sigma, xv + yu)\]

on \( \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} \), where \( q \) is odd, \( \sigma \) is a generator of the Galois group of \( \mathbb{F}_{q^k} \) over \( \mathbb{F}_q \), and \( \eta \) is a non-square. The isotopism class \( [S_D]^{td} \), which is the transpose dual of the isotopism class \( [S_D] \), belongs to the Knuth orbit of \( S_D \) and is symplectic. Thus if \( k=2 \), then \( [S_D]^{td} \) corresponds to a \( K \)-orbit of semifield solids in PG(9, q). Moreover, since \( S_D^{td} \) is non-associative this \( K \)-orbit is distinct from the \( K \)-orbit of semifield solids obtained from the finite field \( \mathbb{F}_{q^4} \), considered as a 4-dimensional algebra over \( \mathbb{F}_q \). Since the value for \( q = 9 \) in the last row of Table 1 is equal to two, there is a unique such \( K \)-orbit in PG(9, 9). Hence if \( S \) is any non-associative 4-dimensional symplectic semifield over \( \mathbb{F}_9 \), then the associated symplectic semifield solid belongs to this \( K \)-orbit, and therefore \( S \) is isotopic to \( S_D^{td} \). This concludes the proof.

Since the algorithm keeps track of all the \( K \)-orbits of intermediate symplectic subspaces, we can also recover those semifield subspaces which do not extend to a larger symplectic subspace, i.e. the maximal ones. For instance, out of the 59 representatives for the \( K \)-orbits on symplectic 2-dimensional semifield subspaces in PG(9, 5) all but 10 are maximal. For \( q = 7 \) there are 90 \( K \)-orbits on 2-dimensional maximal symplectic semifield subspaces in PG(9, 7). We summarize this in the Table 2 for the values of \( q \leq 9 \).

4 Symplectic semifield lines

As before, let \( K \) denote the lift of PGL(4, q) through the Veronese map, i.e. \( K \cong \text{PGL}(4, q) \), \( K \) is a lift of PGL(10, q), and consider its action on subspaces of PG(9, q). In this section we list the representatives for the \( K \)-orbits of \( d \)-dimensional symplectic semifield subspaces in PG(9, q), for \( d \in \{1, 2\} \), and \( q \in \{8, 9\} \). For simplicity and clarity these subspaces are represented by symmetric 3 \( \times \) 3 matrices where the entries below the diagonal are omitted, and where the symbols \( x, y, z \) are used as parameters.

4.1 Symplectic semifield lines in PG\( (9, 8) \)

There are 17 one-dimensional symplectic semifield subspaces of PG(9, 8) up to \( K \)-equivalence, where \( K \cong \text{PGL}(4, 8) \), \( K \) is a lift of PGL(10, 8). We list a representative for each of the 17 \( K \)-orbits. The parameters \( (x, y) \) run over the elements of PG(1, 8) and \( x \) is a primitive element of \( \mathbb{F}_8 \) with minimal polynomial \( X^3 + X + 1 \in \mathbb{F}_2[X] \).
4.2 Symplectic semifield lines in $\text{PG}(9,9)$

There are 22 $K$-orbits of symplectic semifield subspaces of dimension one in $\text{PG}(9,9)$, where $K \cong \text{PGL}(4,9)$, $K \leq \text{PGL}(10,9)$. For each of the $K$-orbits we list a representative. The parameters $(x,y)$ run over the elements of $\text{PG}(1,9)$ and $\alpha$ is a primitive element of $\mathbb{F}_9$ with minimal polynomial $X^2 - X - 1 \in \mathbb{F}_3[X]$.
5 Symplectic semifield subspaces of dimension two

5.1 Two-dimensional symplectic semifield subspaces of PG(9, 8)

The following is a list of representatives of the $K$-orbits of two-dimensional symplectic semifield subspaces of PG(9, 8), where $K \cong \text{PGL}(4, 8)$, $K \leq \text{PGL}(10, 8)$. The parameters $(x, y, z)$ run over the elements of PG(2, 8) and $\alpha$ is a primitive element of $\mathbb{F}_8$ with minimal polynomial $X^3 + X + 1 \in \mathbb{F}_2[X]$.
| 40 | \[\begin{array}{c|c|c|c|c}
  x & y & z & 0 & a z \\
  x + a z & a^2 z & y + a^2 z & x + y + a^2 z & x + a^4 z \\
\end{array}\] |
| 41 | \[\begin{array}{c|c|c|c|c}
  x & y & z & 0 & a z \\
  x + a^4 z & a^5 z & y + a z & x + y + a^2 z & x + a^4 z \\
\end{array}\] |
| 42 | \[\begin{array}{c|c|c|c|c}
  x & y & z & 0 & a z \\
  x + a^3 z & a z & y + a z & x + y + a^2 z & x + a^4 z \\
\end{array}\] |
| 43 | \[\begin{array}{c|c|c|c|c}
  x & y & z & 0 & a z \\
  x + a^5 z & a^2 z & y + a^2 z & x + y + a^2 z & x + a^4 z \\
\end{array}\] |
| 44 | \[\begin{array}{c|c|c|c|c}
  x & y & z & 0 & a z \\
  x + a^5 z & a^2 z & y + a^2 z & x + y + a^2 z & x + a^4 z \\
\end{array}\] |
| 45 | \[\begin{array}{c|c|c|c|c}
  x & y & z & 0 & a z \\
  x + a^5 z & a^2 z & y + a^2 z & x + y + a^2 z & x + a^4 z \\
\end{array}\] |
| 46 | \[\begin{array}{c|c|c|c|c}
  x & y & z & 0 & a z \\
  x + a^5 z & a^2 z & y + a^2 z & x + y + a^2 z & x + a^4 z \\
\end{array}\] |
| 47 | \[\begin{array}{c|c|c|c|c}
  x & y & z & 0 & a z \\
  x + a^5 z & a^2 z & y + a^2 z & x + y + a^2 z & x + a^4 z \\
\end{array}\] |
| 48 | \[\begin{array}{c|c|c|c|c}
  x & y & z & 0 & a z \\
  x + a^5 z & a^2 z & y + a^2 z & x + y + a^2 z & x + a^4 z \\
\end{array}\] |

Symplectic 4-dimensional semifields of order $8^4$ and $9^4$
5.2 Two-dimensional symplectic semifield subspaces in PG(9, 9)

The following is a list of representatives of the $K$-orbits of two-dimensional symplectic semifield subspaces of PG(9, 9), where $K \cong \mathrm{PGL}(4, 9)$, $K \leq \mathrm{PGL}(10, 9)$. The parameters $(x, y, z)$ run over the elements of PG(2, 9) and $\alpha$ is a primitive element of $\mathbb{F}_9$ with minimal polynomial $X^3 + X + 1 \in \mathbb{F}_3[X]$.

\begin{align*}
1. \quad &\begin{bmatrix} x & y & 0 & z \\ x + a^3 z & y + a^5 z & a z & y + a^5 z \\ x & y & a z & y + a^5 z \\
\end{bmatrix} \\
2. \quad &\begin{bmatrix} x & y & 0 & z \\ x + a^3 z & a z & y + a^5 z & y + a^5 z \\ x & y & a z & y + a^5 z \\
\end{bmatrix} \\
3. \quad &\begin{bmatrix} x & y & z & z \\ x + a^2 z & 0 & y + a z & y \\ x & y + a z & y + a z & y \\
\end{bmatrix} \\
4. \quad &\begin{bmatrix} x & y & z & a z \\ x + a^3 z & a z & y + a^5 z & y + a^5 z \\ x & y & a z & y + a^5 z \\
\end{bmatrix} \\
5. \quad &\begin{bmatrix} x & y & z & 0 \\ x + a^3 z & a z & y + a^5 z & y + a^5 z \\ x & y & a z & y + a^5 z \\
\end{bmatrix} \\
6. \quad &\begin{bmatrix} x & y & z & a z \\ x + a^3 z & 0 & y + a z & y \\ x & y + a z & y + a z & y \\
\end{bmatrix} \\
7. \quad &\begin{bmatrix} x & y & 0 & z \\ x + a^3 z & a z & y + a^5 z & y + a^5 z \\ x & y & a z & y + a^5 z \\
\end{bmatrix} \\
8. \quad &\begin{bmatrix} x & y & 0 & z \\ x + a^3 z & a z & y + a^5 z & y + a^5 z \\ x & y & a z & y + a^5 z \\
\end{bmatrix} \\
9. \quad &\begin{bmatrix} x & y & z & 0 \\ x & a z & y + a^5 z & y \\ x + a z & y + a^5 z & y + a z \\
\end{bmatrix} \\
10. \quad &\begin{bmatrix} x & y & z & a z \\ x + a^3 z & a z & y + a^5 z & y + a^5 z \\ x & y & a z & y + a^5 z \\
\end{bmatrix} \\
11. \quad &\begin{bmatrix} x & y & z & 0 \\ x & a z & y + a^5 z & y \\ x + a z & y + a^5 z & y + a z \\
\end{bmatrix} \\
12. \quad &\begin{bmatrix} x & y & z & a z \\ x & a z & y + a^5 z & y \\ x + a z & y + a^5 z & y + a z \\
\end{bmatrix} \\
13. \quad &\begin{bmatrix} x & y & z & a z \\ x + a^3 z & a z & y + a^5 z & y + a^5 z \\ x & y & a z & y + a^5 z \\
\end{bmatrix} \\
14. \quad &\begin{bmatrix} x & y & z & z \\ x + 2 z & a^3 z & y & y + a z \\ x & y & y + a z & x + y + a z \\
\end{bmatrix} \\
15. \quad &\begin{bmatrix} x & y & z & a z \\ x + a z & y + a^5 z & y & x + y + a z \\ x + a z & y + a^5 z & y + a z & x + y + a z \\
\end{bmatrix}
\end{align*}
| 16. | \[ \begin{bmatrix} x & y & z \\ x+z & 2z & 0 \\ x+2z & 0 & y+z \end{bmatrix} \] |
| --- | --- |
| 17. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 18. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 19. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 20. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 21. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 22. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 23. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 24. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 25. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 26. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 27. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 28. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 29. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 30. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 31. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 32. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 33. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 34. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 35. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 36. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 37. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 38. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 39. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 39. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 39. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 39. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 40. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 41. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 42. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 43. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 44. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 45. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 46. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 47. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 48. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 49. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 50. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 51. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 52. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 53. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 54. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 55. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 56. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 57. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 58. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 59. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 60. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| 61. | \[ \begin{bmatrix} x & y & z \\ x+a & 0 & z \\ x+a & 0 & z \end{bmatrix} \] |
| 62. | \[ \begin{bmatrix} x & y & z \\ x+y & z & 2z \\ x+2z & 0 & y+z \end{bmatrix} \] |
| x | y | z | \(a^2z\) |
|---|---|---|---|
| x + a^2z | y + az | \(a^2z\) |
| x + a^2z | y + az | \(a^2z\) |
| x + a^2z | y + az | \(a^2z\) |
| x + a^2z | y + az | \(a^2z\) |

| x | y | z | \(a^2z\) |
|---|---|---|---|
| x + a^2z | y + az | \(a^2z\) |
| x + a^2z | y + az | \(a^2z\) |
| x + a^2z | y + az | \(a^2z\) |
| x + a^2z | y + az | \(a^2z\) |

| x | y | z | \(a^2z\) |
|---|---|---|---|
| x + a^2z | y + az | \(a^2z\) |
| x + a^2z | y + az | \(a^2z\) |
| x + a^2z | y + az | \(a^2z\) |
| x + a^2z | y + az | \(a^2z\) |
\begin{align*}
147. & \quad \begin{bmatrix}
xy & z & 0 \\
x + a^2 z & y + a^5 z & z \\
0 & x + a^3 y + a^3 z & x
\end{bmatrix} \\
148. & \quad \begin{bmatrix}
xy & z & z \\
x + a^2 z & y & z \\
0 & x + a^3 y + a^3 z & x
\end{bmatrix}
\end{align*}

Funding Open Access funding provided by the IReL Consortium

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest There are no conflicts of interest related to this article.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Bamberg J., Betten A., Cara P., De Beule J., Lavrauw M., Neunhoeffer M.: FinInG—a GAP package for Finite Incidence Geometry, 1.01 (2014). https://gap-packages.github.io/FinInG/.
2. Betten A., Braun M., Fripertinger H., Kerber A., Kohnert A., Wassermann A.: Error-Correcting Linear Codes. Classification by Isometry and Applications, Algorithms and Computation in Mathematics, vol. 18. Springer (2006).
3. Blokhuis A., Lavrauw M., Ball S.: On the classification of semifield flocks. Adv. Math. 180(1), 104–111 (2003).
4. Capparelli S., Pepe V.: On symplectic semifield spreads of PG(5, q^2), q even. J. Algebr. Comb. 46, 275–286 (2017).
5. Coulter R.S., Kosick P.: Commutative semifields of order 243 and 3125. In: Finite Fields: Theory and Applications, Contemp. Math., vol. 518, pp. 129–136. Amer. Math. Soc., Providence, RI (2010).
6. Dempwolff U.: Semifield planes of order 81. J. Geom. 89, 1–16 (2008).
7. Dickson L.E.: On finite algebras, Nachrichten der Gesellschaften der Wissenschaften zu Göttingen, pp. 358–393 (1905).
8. Kantor W.M.: Commutative semifields and symplectic spreads. J. Algebra 270, 96–114 (2003).
9. Kleinfeld E.: Techniques for enumerating Veblen-Wedderburn systems. J. Assoc. Comput. Mach. 7, 330–337 (1960).
10. Knuth D.E.: Finite semifields and projective planes. J. Algebra 2, 182–217 (1965).
11. Lavrauw M., Polverino O.: Finite Semifields. Chapter in Current Research Topics in Galois Geometries. Nova Academic Publishers (De Beule, J., Storme, L., eds.).
12. Lavrauw M.: Sublines of prime order contained in the set of internal points of a conic. Des. Codes Cryptogr. 38(1), 113–123 (2006).
13. Lavrauw M.: On the isomorphism classes of finite semifields, Finite Fields Appl. 14(4), 897–910 (2008).
14. Lavrauw M., Rodgers M.: Classification of 8-dimensional rank two commutative semifields. Adv. Geom. 19(1), 57–64 (2019).
15. Lunardon G., Marino G., Polverino O., Trombetti R.: Symplectic semifield spreads of PG(5, q) and the Veronese surface. Ric. Mat. 60(1), 125–142 (2011).
16. Marino G., Pepe V.: On symplectic semifield spreads of PG(5, q^2), q odd. Forum Math. 30, 497–512 (2018).
17. Marino G., Polverino O.: On isotopisms and strong isotopisms of commutative presemifields. J. Algebr. Comb. 36, 247–261 (2012).
18. Mueller J., Neunhöffer M., Noeske R.: The orb package. https://www.gap-system.org/Packages/orb.html.
19. Pepe V.: Symplectic semifield spreads of PG(5, q^4), q even. Ars Math. Contemp. 17, 515–524 (2019).
20. Rúa I.F., Combarro E.F., Ranilla J.: Classification of semifields of order 64. J. Algebra 322, 4011–4029 (2009).
21. Rúa I.F., Combarro E.F., Ranilla J.: New advances in the computational exploration of semifields. Int. J. Comput. Math. 88, 1990–2000 (2011).
22. Rúa I.F., Combarro E.F., Ranilla J.: Determination of division algebras with 243 elements. Finite Fields Appl. 18, 1148–1155 (2012).
23. Rúa I.F., Combarro E.F., Ranilla J.: Finite semifields with $7^4$ elements. Int. J. Comput. Math. 89, 1865–1878 (2012).
24. The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.6.2 (2013). http://www.gap-system.org.
25. Walker R.J.: Determination of division algebras with 32 elements. In: Proc. Sympos. Appl. Math., vol. 15, pp. 83-85. Amer. Math. Soc., Providence, RI (1962).
26. Zhou Y.: On equivalence of maximum additive symmetric rank-distance codes. Des. Codes Cryptogr. 88(5), 841–850 (2020).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.