Results Math (2026) 81:53
Online First

https://doi.org/10.1007/s00025-026-02612-9

Results in Mathematics

Classification of small binary bibraces via bilinear maps

Roberto Civino and Valerio Fedele

Abstract. We classify small binary bibraces, using the correspondence with alternating algebras over the field $\mathbb{F}_2$, up to dimension eight, also determining their isomorphism classes. These finite-dimensional algebras, defined by an alternating bilinear multiplication and nilpotency of class two, can be represented by subspaces of skew-symmetric matrices, with classification corresponding to $\mathrm{GL}(m, \mathbb{F}_2)$-orbits under congruence. Our approach combines theoretical invariants, such as rank sequences and the identification of primitive algebras, with computational methods implemented in `Magma`. These results also count the number of possible alternative operations that can be used in differential cryptanalysis.

Mathematics Subject Classification (2000). 16T25, 08A35, 94A60.

Keywords. Binary bibraces, alternating algebras, elementary abelian regular subgroups, differential cryptanalysis.

1. Introduction

The study of algebraic structures related to braces and their generalisations has seen rapid development in recent years, largely due to their central role in the theory of set-theoretic solutions of the Yang–Baxter equation. Since the seminal works of Rump [26] and Guarnieri and Vendramin [25], it has become clear that braces provide a natural framework for constructing and analysing such solutions. In this context, binary bibraces represent a particular family of structures that can be described equivalently in terms of binary alternating algebras over $\mathbb{F}_2$, that is, finite-dimensional algebras with alternating bilinear multiplication and nilpotency of class two [17]. This correspondence allows one to turn combinatorial problems on bibraces into linear-algebraic ones,

Published online: 24 February 2026

specifically into the study of subspaces of skew-symmetric matrices over $\mathbb{F}_2$ up to congruence.

The classification of these algebras is not only of independent algebraic interest but also motivated by applications. In fact, the problem of counting the number of admissible binary alternating algebras has been mentioned in different works [5,15], both in the algebraic and in the cryptographic contexts, as a challenging enumeration problem. Similar enumeration problems have been considered in other related algebraic settings as well, for instance on counting and classification of Hopf–Galois structures [9,20–22]. Furthermore, even if not explicitly mentioned in the remainder of this paper, our results provide in particular a counting argument for elementary abelian subgroups of the affine group that mutually normalise with the translation group. This interpretation follows from the equivalence between binary alternating algebras and certain alternative group operations defined on vector spaces over $\mathbb{F}_2$, and highlights an additional group-theoretic contribution of our classification [17].

In cryptographic applications, alternative group operations derived from bibraces have been employed in the study of differential attacks [8,27], where they can replace the usual XOR operation in the propagation of differences [3, 6,11–13]. While this connection will be mentioned only briefly here, it provides a concrete motivation: the parameters of these algebras quantify the number of admissible alternative operations, and therefore the extent of possible attack strategies. In particular, the cases of dimension four and eight are especially relevant, since they cover the most common sizes of S-boxes used in block ciphers [2,7,24].

The main difficulty of the classification problem lies in the combinatorial explosion of possibilities as the dimension increases. The problem translates into understanding the orbits of the action of $\mathrm{GL}(m, \mathbb{F}_2)$ on d-dimensional subspaces of the space of $m \times m$ skew-symmetric matrices. While conceptually straightforward, this orbit problem is computationally prohibitive: the number of subspaces grows extremely rapidly, and direct computation quickly becomes infeasible. For example, already in dimension eight, the number of candidate structures exceeds billions, and naive orbit enumeration clashes with the complexity of the problem.

To overcome these difficulties, we employ a twofold strategy. On the one hand, we use algebraic invariants, such as rank sequences of matrix spaces, to partition the set of subspaces into coarser equivalence classes, thereby reducing the search space. On the other hand, we use the computational algebra system `Magma` [4] to carry out explicit orbit computations when possible, and group-theoretic arguments when direct computations are infeasible. These tools, while not sufficient to fully classify higher-dimensional cases in general, prove to be powerful enough to obtain a complete classification in small cases.

In particular, we extend the enumeration results of binary alternating algebras (and hence bibraces) to all structures of dimension at most eight,

providing criteria for primitivity and rank-based invariants that help distinguish nonisomorphic cases. These results solve, in the range up to dimension eight, the problem of counting such structures mentioned in previous works. At the same time, from the cryptographic perspective, our results clarify the landscape of possible alternative operations for differential attacks, showing that the range of admissible structures of dimensions four and eight (the dimensions most relevant for S-boxes) can be completely enumerated and understood. While it has long been known that there are 105 operations on 4-bit blocks, here we find that there are 117.833.335.446.015 operations on 8-bit blocks, corresponding to roughly 47 bits of entropy for the search of an alternative operation for differential cryptanalysis.

The paper is organised as follows. In Section 2 we recall the necessary background on binary alternating algebras, their correspondence with binary bibraces, and the matrix representation of the induced bilinear maps. Section 3 develops the classification techniques, introducing invariants such as rank sequences and the notion of primitivity, needed to obtain the complete classification up to dimension eight summarised in Table 1.

2. Preliminaries and Background

This section collects the essential definitions, notation, and previous results on binary bibraces and binary alternating algebras that will be used in the sequel. All algebraic structures are considered over the field $\mathbb{F}_2$. Here we follow the notation of a previous paper where bibraces were singled out as a particular construction and given a name [17]. The classification results rely on and are inspired by a broader line of research on more general structures, carried out by many authors over the years [1,10,14,16,18,19,23].

Definition 2.1. A *binary bibrace* is a triple $(R, +, \circ)$ where:

- $(R, +)$ and $(R, \circ)$ are both elementary abelian 2-groups (vector spaces over $\mathbb{F}_2$);
- the operations satisfy the *biskew brace* identities:

$$(x + y) \circ z = x \circ z + z + y \circ z, \quad x \circ y + z = (x + z) \circ z \circ (y + z)$$

for all $x, y, z \in R$.

The previous identities are equivalent to the *dual normalisation*, meaning that the group $T_\circ(R) = \{t_x : y \mapsto y \circ x \mid x \in R\}$ of $\circ$-translations normalises the group $T_+(R)$ of $+$-translations and vice versa.

Definition 2.2. A *binary alternating algebra* is an $\mathbb{F}_2$-algebra $(R, +, \cdot)$ satisfying

(1) *alternating law:* $x \cdot x = 0$ for all $x \in R$;
(2) *nilpotency of class two:* $x \cdot y \cdot z = 0$ for all $x, y, z \in R$.

The *annihilator* of R is the subspace $\mathrm{Ann}(R) = \{a \in R \mid a \cdot R = 0\}$, while the *square* is $R^2 = \langle x \cdot y \mid x, y \in R \rangle$. The nilpotency condition implies $R^2 \subseteq \mathrm{Ann}(R)$.

The algebraic structures of Definitions 2.1 and 2.2 are equivalent, meaning that, given a binary alternating algebra $(R, +, \cdot)$, the operation

$$x \circ y = x + y + x \cdot y$$

defines a binary bibrace on R. Conversely, any binary bibrace $(R, +, \circ)$ corresponds to a binary alternating algebra of nilpotency class two [17], equipped with the product defined by

$$x \cdot y = x + y + x \circ y.$$

This equivalence implies that the classification of binary alternating algebras directly determines the possible bibrace structures with the same support, i.e., all alternative operations for differential cryptanalysis under the dual normalisation constraint.

2.1. Representation Via Skew-Symmetric Matrices and Bilinear Maps

Given a nondegenerate alternating bilinear map $\varphi : V \times V \longrightarrow W$ over $\mathbb{F}_2$-vector spaces V and W, it is possible to define a product on the direct sum $V \oplus W = R$ that equips it with the structure of a binary alternating algebra $(R, +, \cdot)$ such that $\mathrm{Ann}(R) = 0_V \oplus W$, where

$$(x_1, y_1) \cdot (x_2, y_2) = (0, \varphi(x_1, x_2))$$

for all $x_1, x_2 \in V$, $y_1, y_2 \in W$ (here *alternating* means $\varphi(x, x) = 0$ for all $x \in V$).

Conversely, the product of a binary alternating algebra $(R, +, \cdot)$ induces an alternating bilinear map

$$\widehat{\varphi} : R \times R \longrightarrow \mathrm{Ann}(R), \quad \widehat{\varphi}(x, y) = x \cdot y$$

and its restriction to a complement V of the annihilator $W = \mathrm{Ann}(R)$ is a nondegenerate alternating bilinear map.

Let us consider the finite-dimensional case and let $(v_1, \ldots, v_m, w_1, \ldots, w_d)$ be an ordered basis of R, where $v_1, \ldots, v_m$ and $w_1, \ldots, w_d$ are bases of V and W, respectively. Then the bilinear map $\widehat{\varphi}$ defined over the entire space is determined by a sequence $(\widehat{B}_1, \ldots, \widehat{B}_d)$ of d binary square $(m + d) \times (m + d)$ matrices. More precisely, we can write

$$\widehat{\varphi}(x, y) = \varphi_1(x, y)w_1 + \cdots + \varphi_d(x, y)w_d,$$

where

$$\varphi_k : R \times R \longrightarrow \mathbb{F}_2, \quad \varphi_k(x, y) = x\widehat{B}_k y^t$$

is a bilinear form for $1 \leq k \leq d$. Conversely, if $\varphi_1, \ldots, \varphi_d$ are given, then the matrix $\widehat{B}_k$ is defined by

$$\widehat{B}_k = \left[\begin{array}{c|c} \varphi_k(v_i, v_j) & 0 \\ \hline 0 & 0 \end{array}\right], \quad 1 \leq i, j \leq m.$$

We denote by B_k the $m \times m$ submatrix of $\widehat{B}_k$ whose (i, j)-entry $B_k[i, j]$ is given by $v_i \widehat{B}_k v_j^t$ for each $1 \leq i, j \leq m$ and $1 \leq k \leq d$. Then the matrices B_k are the $m \times m$ matrices associated to the bilinear map $\varphi : V \times V \longrightarrow W$.

It is proved that $B_1, \ldots, B_d$ are *skew-symmetric* (symmetric and zero-diagonal) [17]. Moreover, it is shown that

$$\dim R^2 = \dim\langle B_1, \ldots, B_d\rangle. \tag{1}$$

Conversely, starting from a sequence $B_1, \ldots, B_d$ of binary skew-symmetric matrices of size m, one can define a binary alternating algebra by endowing the vector space $\mathbb{F}_2^m \oplus \mathbb{F}_2^d$ with the product

$$(x_1, y_1) \cdot (x_2, y_2) = (0, (x_1 B_1 x_2^t, \ldots, x_1 B_d x_2^t)).$$

Ensuring the nondegeneracy of the bilinear map $\varphi(x_1, x_2) = (x_1 B_1 x_2^t, \ldots, x_1 B_d x_2^t)$ requires only that the matrix formed by horizontally concatenating $B_1, ..., B_d$ has a rank of m. We remark that the nondegeneracy condition is equivalent to requiring that the annihilator of the associated algebra coincides with the subspace $0_m \oplus \mathbb{F}_2^d$.

Definition 2.3. Let $V = \langle v_1, \ldots, v_m\rangle$ and $W = \langle w_1, \ldots, w_d\rangle$ be two finite-dimensional vector spaces over $\mathbb{F}_2$, and let $R = V \oplus W$. Given a nondegenerate bilinear map $\varphi : V \times V \longrightarrow W$, we denote by $\cdot_\varphi$ the algebra product induced by φ over R as

$$(x_1, y_1) \cdot (x_2, y_2) = (0, \varphi(x_1, x_2)).$$

The matrices $B_1, \ldots, B_d$ satisfying

$$\varphi(x_1, x_2) = (x_1 B_1 x_2^t, \ldots, x_1 B_d x_2^t) \quad \text{for } x_1, x_2 \in V$$

are called the *defining matrices of* $(R, +, \cdot_\varphi)$.

The matrix space generated by the defining matrices of a binary alternating algebra is a subspace of the space

$$\Lambda_m = \{m \times m \text{ skew-symmetric matrices over } \mathbb{F}_2\}.$$

To determine the isomorphism classes of small binary alternating algebras, we use the fact that two such algebras are isomorphic if and only if their corresponding d-dimensional subspaces are in the same orbit under the action of $\mathrm{GL}(m, \mathbb{F}_2)$ by congruence. The classification of binary alternating algebras is equivalent to the classification of $\mathrm{GL}(m, \mathbb{F}_2)$-orbits of d-dimensional subspaces of Λ_m, which we address in the remainder of the paper.

3. Number of Binary Structures

Let R be a vector space of dimension $m+d$ over $\mathbb{F}_2$ and let W be a subspace of R of dimension d. The number of binary alternating algebras that one can impose on the vector space R such that $\mathrm{Ann}(R) = W$ is given by the number of the length-d ordered sequences of skew-symmetric matrices over $\mathbb{F}_2$ whose horizontal concatenation has rank m [17], i.e.,

$$s_{m,d} = \#\left\{(B_1, \ldots, B_d) : \ B_i \in \Lambda_m, \ \mathrm{Rank}\left[B_1, \ldots, B_d\right] = m\right\}.$$

Since

$$t_{m,d} = \frac{(2^{m+d}-1)(2^{m+d}-2)\ldots(2^{m+d}-2^{d-1})}{(2^d-1)(2^d-2)\ldots(2^d-2^{d-1})},$$

that is the Gaussian binomial coefficient $\binom{m+d}{d}_2$, counts the number of d-dimensional subspaces of R, which corresponds in turn to the possible choices for the annihilator of the algebra, the total number of such algebras is given by the product $s_{m,d} \cdot t_{m,d}$. In Table 1, we indicate $s_{m,d}$ and $t_{m,d}$ for each couple of parameters (m,d) within the range $3 \leq m+d = n \leq 8$. In the remainder of the paper, we show how we computed $s_{m,d}$ in the relevant cases. We recall that not all values of $d = \dim(\mathrm{Ann}(R))$ are admissible for a binary alternating algebra of a given total dimension. Indeed, by construction one always has $R^2 \subseteq \mathrm{Ann}(R)$, so that $1 \leq d \leq \dim(R) - 2$, and additional restrictions arise from the alternating property of the bilinear map. In particular, when the total dimension of R is even, the case $d = 1$ cannot occur. As a consequence, some values of d are forbidden and therefore do not appear in Table 1.

3.1. Primitive Binary Alternating Algebras

Let $(R, +, \cdot_\varphi)$ be a binary alternating algebra of dimensional parameters m and d. Assume that R^2 is a proper subspace of $\mathrm{Ann}(R)$, i.e., $\mathrm{Ann}(R) = R^2 \oplus U$ for some nonzero subspace U of dimension $1 \leq k \leq d-1$. Then U is a null subalgebra of R and the quotient algebra R/U is isomorphic to an algebra of dimensional parameters m and $d-k$.

Conversely, starting from an algebra with a defining sequence $[B_1, \ldots, B_d]$ such that $\mathrm{Ann}(R) = R^2$, it is easy to construct an algebra of dimensional parameters m and $d+k$, for example by extending the sequence with k zero matrices

$$[B_1, \ldots, B_d, 0, \ldots, 0].$$

Therefore, for classification purposes, it is convenient to use $\dim(R^2)$ and m as parameters. Since the dimension of the annihilator and the counting of operations are relevant in cryptographic applications, we distinguish the two classification approaches by introducing the following definition.

Definition 3.1. Let $(R, +, \cdot_\varphi)$ be a binary alternating algebra, let $W = \mathrm{Ann}(R)$ and let V be a complement of W. We say that R is primitive if $\mathrm{Ann}(R/R^2) = 0$ or, equivalently, $W = R^2$.

TABLE 1. Number of small binary structures

n	m	d	# d-dimensional spaces	# operations over standard basis
3	2	1	7	1
4	2	2	35	3
5	4	1	31	28
5	3	2	155	42
5	2	3	155	7
6	4	2	651	3360
6	3	3	1395	462
6	2	4	651	15
7	6	1	127	13888
7	5	2	2667	937440
7	4	3	11811	254968
7	3	4	11811	3990
7	2	5	2667	31
8	6	2	10795	1012435200
8	5	3	97155	1065765120
8	4	4	200787	16716840
8	3	5	97155	32550
8	2	6	10795	63

In what follows, we denote by E_{ij} the standard basis of Λ_m, i.e., for $1 \leq i < j \leq m$,

$$E_{ij} = e_{ij} + e_{ji},$$

where e_{ij} denotes an elementary matrix ($e_{ij}[i,j] = 1$ and $e_{ij}[h,k] = 0$ for $(i,j) \neq (h,k)$).

Proposition 3.2. *Let $(R, +, \cdot_\varphi)$ be a primitive binary alternating algebra, $R = V \oplus R^2$, $V \simeq \mathbb{F}_2^m$, $R^2 \simeq \mathbb{F}_2^d$. The following statements hold:*

(1) $1 + (m \mod 2) \leq \dim(R^2) \leq \dim(\Lambda_m)$;
(2) if $\dim(R^2) = 1$, *then the isomorphism class of R is unique among binary alternating algebras with underlying vector space $\mathbb{F}_2^m \oplus \mathbb{F}_2^d$ (m even);*
(3) if $m = 3$, *then R belongs to one of the two isomorphism classes identified by the following sequences of matrices:*

$$(E_{12}, E_{13}, E_{23}), \quad (E_{12}, E_{23}).$$

Proof. Let $B_1, \ldots, B_d \in \Lambda_m$ be the defining matrices of $(R, +, \cdot_\varphi)$. By Eq. (1), $\dim(R^2) = \dim\langle B_1, \ldots, B_d\rangle \leq \dim(\Lambda_m)$. Since the bilinear map φ is nondegenerate, $\mathrm{Rank}\left(\begin{bmatrix} B_1 & \ldots & B_d \end{bmatrix}\right) = m$. Now, if $d = \dim(R^2) = 1$, then $\mathrm{Rank}(B_1) = m$

TABLE 2. Isomorphism classes in small cases

n	m	d	# classes	# primitive
*	2	$\geqslant 1$	1	1
*	3	$\geqslant 3$	2	2
5	3	2	1	1
5	4	1	1	1
6	4	2	4	3
7	4	3	9	5
7	5	2	2	2
7	6	1	1	1
8	4	4	13	4
8	5	3	18	16
8	6	2	9	8

and so m is even. On the other hand, if m is odd, $\mathrm{Rank}(B) \leq m-1$ for each $B \in \Lambda_m$ and so $d \geq 2$.

The uniqueness of the isomorphism class in the case $d = 1$ follows by the fact that any two skew-symmetric matrices of the same rank are congruent.

Finally, for $m = 3$, an easy check shows that the seven 2-dimensional subspaces of Λ_3 are pairwise congruent. Thus, the only two isomorphism classes of primitive algebras are determined by a sequence of matrices that generates the entire space Λ_3 when $d = 3$ or a 2-dimensional subspace when $d = 2$. □

Table 2 shows the classification of binary alternating algebras with underlying vector space $\mathbb{F}_2^m \oplus \mathbb{F}_2^d$ up to dimension $n = m+d = 8$. For each pair of parameters m and d, we indicate the number of isomorphism classes of binary structures, or, equivalently, the number of congruence classes of k-dimensional subspaces of Λ_m, where $k \leq d$. Moreover, we indicate the isomorphism classes of primitive algebras (i.e., the number of congruence classes of d-dimensional subspaces of Λ_m).

This classification was obtained through direct computation, via `Magma`, of the congruence classes of the skew-symmetric matrix subspaces. More precisely, we computed the action by congruence of $\mathrm{GL}(m, \mathbb{F}_2)$ on the set of k-dimensional subspaces, for $k \leq d$. In the last case, where $m = 6$ and $d = 2$, we used a different approach because this type of direct computation would have required an excessive amount of time and virtual memory. Thus, we identified appropriate representatives of the congruence classes and calculated the cardinality of each class as the ratio between the order of $\mathrm{GL}(6, \mathbb{F}_2)$,

$$\#\,\mathrm{GL}(6, \mathbb{F}_2) = \prod_{j=0}^{5} (2^6 - 2^j) = 20158709760,$$

and the order of the *self-congruence group* of a space $\mathcal{B} \subseteq \Lambda_m$, which we will introduce in the following sections along with the details of the procedure.

3.2. Ranks Criterion

The tool we are about to introduce allows to determine a nonisomorphism criterion for alternating algebras.

Definition 3.3. We call *(ascending) sequence of (matrix) ranks* of a k-dimensional matrix vector space $\mathcal{B} \subseteq \mathbb{F}_2^{m\times m}$ any sequence of length $2^k - 1$ of the matrix ranks $(r_1, \dots, r_{2^k-1})$, where $r_i = \mathrm{Rank}(B_i)$, $0 \neq B_i \in \mathcal{B}$, and such that

$$r_1 \leq r_2 \leq \cdots \leq r_{2^k-1}.$$

To introduce the ranks criterion, we need the following result.

Theorem 3.4. ([17]). *Let $(R, +, \cdot_\varphi)$ and $(S, +, \cdot_\psi)$ be two nilpotent algebras of class two over $\mathbb{F}_2$, with underlying vector space $\mathbb{F}_2^m \oplus \mathbb{F}_2^d$ and defining matrices $B_1, \dots, B_d$ and $C_1, \dots, C_d$ respectively. Then R and S are isomorphic algebras if and only if $\langle B_1, \dots, B_d\rangle$ and $\langle C_1, \dots, C_d\rangle$ are congruent (i.e., there exists an invertible matrix A such that $A\langle C_j\rangle_j A^t = \langle B_i\rangle_i$).*

Theorem 3.5 *Let $R = \mathbb{F}_2^m \oplus \mathbb{F}_2^d$, $(R, +, \cdot_\varphi)$ and $(R, +, \cdot_\psi)$ be two nilpotent algebras of class two with defining matrices $B_1, \dots, B_d$ and $C_1, \dots, C_d$ respectively. If the matrix spaces $\langle B_i\rangle_i$ and $\langle C_i\rangle_i$ have different sequences of ranks, then the two algebras are not isomorphic.*

Proof. The sequence of ranks of the space $\langle B_i\rangle_i$ is preserved under the action $A\langle B_i\rangle_i A^t$ for each $A \in \mathrm{GL}(m, \mathbb{F}_q)$. Therefore if $\langle B_i\rangle_i$ and $\langle C_i\rangle_i$ have different sequences of ranks, the two spaces are not congruent and the claim follows by Theorem 3.4. □

The following counterexample shows that, in general, two binary alternating algebras with the same sequence of ranks are not isomorphic.

Example 3.6. Let us consider the following two 3-dimensional matrix vector subspaces of Λ_4,

$$\mathcal{B} = \langle E_{14}, E_{23}, E_{13} + E_{24}\rangle, \quad \mathcal{C} = \langle E_{12}, E_{23}, E_{13} + E_{24}\rangle.$$

By a direct computation with `Magma`, we can verify that every 2-dimensional subspace of $\mathcal{B}$, respectively of $\mathcal{C}$, has one of the following rank chains

$$(2, 2, 4),\ (2, 4, 4),\ (4, 4, 4),$$

respectively

$$(2, 2, 2),\ (2, 4, 4).$$

Now, for each $A \in \mathrm{GL}(4, \mathbb{F}_2)$, the space $A\langle E_{14}, E_{23}\rangle A^t$ has rank chain $(2, 2, 4)$ and so it is not contained in $\mathcal{C}$. Thus, $\mathcal{B}$ is not congruent to $\mathcal{C}$. However, both have the same rank chain as shown in Table 3.

TABLE 3. Ranks and subspaces of Example 3.6

Rank	$\mathcal{B}$	$\mathcal{C}$
2	E_{14}	E_{12}
2	E_{23}	E_{23}
2	$E_{14} + E_{23} + E_{13} + E_{24}$	$E_{12} + E_{23}$
4	$E_{13} + E_{24}$	$E_{13} + E_{24}$
4	$E_{14} + E_{13} + E_{24}$	$E_{12} + E_{13} + E_{24}$
4	$E_{23} + E_{13} + E_{24}$	$E_{23} + E_{13} + E_{24}$
4	$E_{14} + E_{23}$	$E_{12} + E_{23} + E_{13} + E_{24}$

We conclude this section by observing that the set of k-dimensional subspaces of Λ_m identified by a fixed sequence of ranks is partitioned into congruence classes. Therefore, the partition induced by the rank sequences on the set of k-dimensional subspaces is a coarser partition than that induced by the congruence classes. However, it simplifies the identification of suitable representatives of the congruence classes when the number of spaces is very large.

3.3. Binary Alternating Algebras with 2-Dimensional Annihilator

In this section, we will address the case of 2-dimensional spaces of Λ_m with the aim of classifying binary alternating algebras of dimension 8 with a 2-dimensional annihilator. Indeed, given that the cardinality of $\mathrm{GL}(6, \mathbb{F}_2)$ is large, it is computationally infeasible to use the method used for previous cases, which involves directly calculating the group's action on the set of subspaces.

For a given 2-dimensional subspace $\mathcal{B}$ of Λ_6, the results presented here have allowed us to compute the cardinality of the congruence class of $\mathcal{B}$ as the ratio of $\#\,\mathrm{GL}(6, \mathbb{F}_2)$ to the cardinality of the *self-congruence group* of $\mathcal{B}$, which is defined as follows.

Definition 3.7. Let $\mathcal{B} \subseteq \Lambda_m$ be a subspace of skew-symmetric matrices over $\mathbb{F}_2$. We define

$$\mathrm{SC}(\mathcal{B}) = \{\, A : \, A \in \mathrm{GL}(m, \mathbb{F}_2) \mid A\mathcal{B}A^t = \mathcal{B} \,\}$$

as the *self-congruence group* of the space $\mathcal{B}$.

Clearly, this method requires that determining $\#\,\mathrm{SC}(\mathcal{B})$ is computationally feasible and that it is possible to identify a set of representatives for the congruence classes. For this last requirement, we have used the rank criterion introduced in Section 3.2, along with the fact that the cardinalities of the congruence classes are distinct (in pairs) and that their sum coincides with the

TABLE 4. Spaces related to nondegenerate bilinear maps

Class	Ranks	Cardinality
C_1	$(6,6,6)$	13332480
C_2	$(4,6,6)$	27998208
C_3	$(4,6,6)$	26248320
C_4	$(2,6,6)$	2187360
C_5	$(4,4,6)$	69995520
C_6	$(2,4,6)$	4666368
C_7	$(4,4,4)$	15554560
C_8	$(4,4,4)$	8749440

total number of 2-dimensional spaces of Λ_6, namely

$$\frac{(2^{15}-1)(2^{15}-2)}{6}.$$

We illustrate the results in Tables 4 and 5. The first 8 congruence classes contain 168732256 subspaces. The horizontal concatenation of any two nonzero matrices $B_1, B_2, B_3 = B_1 + B_2$ in each of these spaces gives rise to a rank 6 matrix. Indeed, for each $i, j \in \{1,2,3\}$, $i \neq j$,

$$\text{Rank}\left[B_i\ B_j\right] = \text{Rank}\left[B_1\ B_2\ B_3\right],$$

because the span of the columns of $B_3 = B_1 + B_2$, $C(B_1 + B_2)$ is contained in the span of $C(B_1) \cup C(B_2)$. In particular, the bilinear map associated with (B_i, B_j) is nondegenerate, and the congruence class is an isomorphism class of alternating binary algebras. Clearly, the number of these algebras corresponds to the number of ordered bases of each space, which is 6 times the number of subspaces, i.e., 1012393536. Now, the total number of algebras with a 2-dimensional annihilator is given by

$$1012393536 + 3 \times 13888 = 1012435200,$$

where 13888 is the number of skew-symmetric matrices B with a rank of 6 and 3 is the number of defining matrices sequences of length 2 which yield a 1-dimensional R^2 space, i.e., $(B,0), (0,B), (B,B)$.

The subspaces contained in the last 6 classes are related to degenerate bilinear maps, i.e., the horizontal concatenation of two matrices taken in any of these subspaces has rank less than 6.

We conclude this section by illustrating the results used for the classification. Given a sequence S of matrices defined over a field of characteristic different from 2, the `Magma` function `IsometryGroup(`S`)` returns the isometry group of the system, which we have defined as the self-congruence group of Definition 3.7. In characteristic 2, the algorithm for computing such group is not implemented in `Magma`; to overcome this, we relied on Proposition 3.10,

TABLE 5. Spaces related to degenerate bilinear maps

Class	Ranks	Cardinality
C_9	$(4,4,4)$	6562080
C_{10}	$(4,4,4)$	36456
C_{11}	$(2,4,4)$	73728
C_{12}	$(2,4,4)$	3072
C_{13}	$(2,2,4)$	182280
C_{14}	$(2,2,2)$	9765

which we are now going to prove. Here Sp denotes the symplectic group. The following proposition shows that if two 2-dimensional spaces $\langle B_1, B_2\rangle$, $\langle C_1, C_2\rangle$ are congruent, then the two subgroups $\mathrm{Sp}(B_1)\cap\mathrm{Sp}(B_2)$ and $\mathrm{Sp}(C_1)\cap\mathrm{Sp}(C_2)$ are conjugated in $\mathrm{GL}(m,\mathbb{F}_2)$. Notice that $\mathrm{Sp}(B_1)\cap\mathrm{Sp}(B_2) < \mathrm{Sp}(B_1+B_2)$, indeed for every $X\in\mathrm{Sp}(B_1)\cap\mathrm{Sp}(B_2)$,

$$X(B_1+B_2)X^t = XB_1X^t + XB_2X^t = B_1+B_2.$$

In particular, $\mathrm{Sp}(B_1)\cap\mathrm{Sp}(B_2) = \mathrm{Sp}(B_1)\cap\mathrm{Sp}(B_2)\cap\mathrm{Sp}(B_1+B_2)$.

Proposition 3.8. *Let $\langle B_1, B_2\rangle, \langle C_1, C_2\rangle \in \Lambda_m$ be 2-dimensional spaces of skew-symmetric matrices over $\mathbb{F}_2$. If they are congruent, then $\mathrm{Sp}(B_1)\cap\mathrm{Sp}(B_2)$ is conjugate to $\mathrm{Sp}(C_1)\cap\mathrm{Sp}(C_2)$.*

Proof. Assume that $\langle B_1, B_2\rangle, \langle C_1, C_2\rangle \in \Lambda_m$ are congruent. Then there exists $Z\in\mathrm{GL}(m,\mathbb{F}_2)$ such that

$$ZC_1Z^t = a_{11}B_1 + a_{12}B_2,$$
$$ZC_2Z^t = a_{21}B_1 + a_{22}B_2,$$

for some invertible matrix $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22}\end{bmatrix}$. Now, let $X\in\mathrm{Sp}(B_1)\cap\mathrm{Sp}(B_2)$. Then, for $i\in\{1,2\}$,

$$XZC_iZ^tX^t = X(a_{i1}B_1 + a_{i2}B_2)X^t = a_{i1}B_1 + a_{i2}B_2 = ZC_iZ^t.$$

Thus, $Z^{-1}XZ\in\mathrm{Sp}(C_1)\cap\mathrm{Sp}(C_2)$, i.e., $Z^{-1}(\mathrm{Sp}(B_1)\cap\mathrm{Sp}(B_2))Z\subseteq\mathrm{Sp}(C_1)\cap\mathrm{Sp}(C_2)$. The opposite inclusion follows by the symmetry of the congruence relation. □

Remark 3.9. In the hypotheses of the previous proposition, we explicitly observe that given an invertible matrix $Z\in\mathrm{GL}(m,\mathbb{F}_2)$ and setting $G_B = \mathrm{Sp}(B_1)\cap\mathrm{Sp}(B_2)$, $G_C = \mathrm{Sp}(C_1)\cap\mathrm{Sp}(C_2)$, then

$$Z\langle C_1, C_2\rangle Z^t = \langle B_1, B_2\rangle \quad\Longrightarrow\quad Z^{-1}G_BZ = G_C.$$

Proposition 3.10. *Let $\mathcal{B} = \langle B_1, B_2\rangle \subseteq \Lambda_m$ be a 2-dimensional subspace of skew-symmetric matrices over $\mathbb{F}_2$, let $G = \mathrm{Sp}(B_1)\cap\mathrm{Sp}(B_2)$ and let $N = N_{\mathrm{GL}(m,\mathbb{F}_2)}(G)$. Then the following statements hold:*

(1) $G \leq \mathrm{SC}(\mathcal{B}) \leq N$ *(in particular,* $\mathrm{SC}(\mathcal{B}) = \{A \in N \mid A\mathcal{B}A^t = \mathcal{B}\}$*);*
(2) if T *is a right transversal for* G *in* N*, and* S *is the subset of* T *formed by the matrices* A *such that* $A\mathcal{B}A^t = \mathcal{B}$*, then* $\mathrm{SC}(\mathcal{B}) = \langle G \cup S \rangle$*;*
(3) $[\,\mathrm{GL}(m, \mathbb{F}_2) : \mathrm{SC}(\mathcal{B})\,]$ *is the number of 2-dimensional subspaces of* Λ_m *congruent to* $\mathcal{B}$*.*

Proof. Clearly $G \leq \mathrm{SC}(\mathcal{B})$. Let $Z \in \mathrm{SC}(\mathcal{B})$. By Proposition 3.8, $Z^{-1}GZ = G$ and so $Z \in N$.

Now, it follows by construction that $\langle G \cup S \rangle \subseteq \mathrm{SC}(\mathcal{B})$. To prove the opposite inclusion, let us consider $Z \in \mathrm{SC}(\mathcal{B})$ and observe that, by item (1), $Z \in N$. So Z is contained in a right coset of G in N, i.e., $Z = Z_G Z_N$ for some $Z_G \in G$ and $Z_N \in N$. Now, $\mathcal{B} = Z\mathcal{B}Z^t = Z_G Z_N \mathcal{B} Z_N^t Z_G^t$. This means that $\mathcal{B} = Z_G^{-1}\mathcal{B}(Z_G^{-1})^t = Z_N \mathcal{B} Z_N^t$. Thus, $Z_N \in GZ_S$ for some $Z_S \in S$, i.e., $Z = Z'_G Z_S$, $Z'_G \in G$. Finally, it is clear that two invertible matrices, belonging to the same right coset of $\mathrm{SC}(\mathcal{B})$, yield the same matrix space by acting on $\mathcal{B}$. So the index of $\mathrm{SC}(\mathcal{B})$ in $\mathrm{GL}(m, \mathbb{F}_2)$ coincides with the number of spaces which are congruent to $\mathcal{B}$. □

Thanks to item (1) of the previous proposition, it is possible to restrict the search for invertible matrices such that $A\mathcal{B}A^t = \mathcal{B}$ to the normaliser of G in $\mathrm{GL}(m, \mathbb{F}_2)$. In particular, it suffices to check the self-congruence property for the matrices belonging to a system of representatives of the right cosets of G in N. This is particularly convenient in the case $m = 6$.

Author contributions R. Civino and V. Fedele wrote the main manuscript text. All authors reviewed the manuscript.

Funding Open access funding provided by Università degli Studi dell'Aquila within the CRUI-CARE Agreement. R. Civino is member of INdAM-GNSAGA and is supported by the Centre of EXcellence on Connected, Geo-Localized and Cybersecure Vehicles (EX-Emerge), funded by Italian Government under CIPE resolution n. 70/2017 (Aug. 7, 2017). R. Civino thankfully acknowledges support by MUR-Italy via PRIN 2022RFAZCJ 'Algebraic methods in cryptanalysis'.

Data Availability Statement No datasets were generated or analyzed during the current study, and therefore no data are available to be shared.

Declarations

Conflicts of Interest The authors have no relevant financial or nonfinancial interests to disclose.

References

[1] Aragona, R., Civino, R., Gavioli, N., Scoppola, C.M.: Regular subgroups with large intersection. Annali di Matematica Pura ed Applicata (1923-) **198**(6), 2043–2057 (2019)

[2] Biham, E., Anderson, R., Knudsen, L.: Serpent: A New Block Cipher Proposal. International workshop on fast software encryption, pp. 222–238. Springer, Berlin (1998)

[3] Baudrin, J., Beierle, C., Felke, P., Leander, G., Neumann, P., Perrin, L., Stennes, L.: Commutative cryptanalysis as a generalization of differential cryptanalysis, Designs, Codes and Cryptography, 1–39 (2025)

[4] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I: the user language. J. Symb. Comput. **24**(3–4), 235–265 (1997)

[5] Brunetta, C., Calderini, M., Sala, M.: On hidden sums compatible with a given block cipher diffusion layer. Discret. Math. **342**(2), 373–386 (2019)

[6] Baudrin, J., Felke, P., Leander, G., Neumann, P., Perrin, L., Stennes, L.: Commutative cryptanalysis made practical. IACR Transactions on Symmetric Cryptology **2023**(4), 299–329 (2023)

[7] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher, Cryptographic Hardware and Embedded Systems-CHES,: 9th International Workshop, Vienna, Austria, September 10–13, 2007. Proceedings 9. Springer 2007, 450–466 (2007)

[8] Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**, 3–72 (1991)

[9] Byott, N.P.: Hopf-Galois structures on almost cyclic field extensions of 2-power degree. J. Algebra **318**(1), 351–371 (2007)

[10] Caranti, A.: Bi-skew braces and regular subgroups of the holomorph. J. Algebra **562**, 647–665 (2020)

[11] Civino, R., Blondeau, C., Sala, M.: Differential attacks: using alternative operations. Des. Codes Crypt. **87**, 225–247 (2019)

[12] Calderini, M., Civino, R., Invernizzi, R.: Differential experiments using parallel alternative operations. J. Math. Cryptology **18**(1), 20230030 (2024)

[13] Calderini, M., Civino, R., Invernizzi, R.: Optimal s-boxes against alternative operations and linear propagation. Discret. Math. **349**(3), 114870 (2026)

[14] Catino, F., Colazzo, I., Stefanelli, P.: Skew left braces with non-trivial annihilator. J. Algebra and Its Applications **18**(02), 1950033 (2019)

[15] Calderini, M., Civino, R., Sala, M.: On properties of translation groups in the affine general linear group with applications to cryptography. J. Algebra **569**, 658–680 (2021)

[16] Caranti, A., Dalla Volta, F., Sala, M.: Abelian regular subgroups of the affine group and radical rings. Publ. Math. Debrecen **69**(3), 297–308 (2006)

[17] Civino, R., Fedele, V.: Binary bibraces and applications to cryptography. Mediterr. J. Math. **22**(1), 29 (2025)

[18] Childs, L.N.: Bi-skew braces and Hopf Galois structures. New York J. Math. **25**, 574–588 (2019)

[19] Catino, F., Rizzo, R.: Regular subgroups of the affine group and radical circle algebras. Bull. Aust. Math. Soc. **79**(1), 103–107 (2009)

[20] Crespo, T., Salguero, M.: Computation of Hopf Galois structures on low degree separable extensions and classification of those for degrees p^2 and $2p$. Publ. Mat. **64**(1), 121–141 (2020)

[21] Darlington, A.: An algorithm for computing Hopf–Galois structures and skew bracoids of low degree, arXiv preprint arXiv:2508.03372 (2025)

[22] Darlington, A.: Hopf–Galois structures on parallel extensions, J. Algebra (2025)

[23] Del Corso, I.: Module braces: relations between the additive and the multiplicative groups. Annali di Matematica (1923-) **202**, 3005–3025 (2023)

[24] Daemen, J., Rijmen, V.: The design of Rijndael, vol. 2. Springer, Berlin (2002)

[25] Guarnieri, L., Vendramin, L.: Skew braces and the Yang-Baxter equation. Math. Comput. **86**(307), 2519–2534 (2017)

[26] Rump, W.: Braces, radical rings, and the quantum Yang-Baxter equation. J. Algebra **307**(1), 153–170 (2007)

[27] Wagner, D.: Towards a unifying view of block cipher cryptanalysis, Fast Software Encryption: 11th International Workshop, FSE: Delhi, India, February 5–7, 2004. Revised Papers 11. Springer **2004**, 16–33 (2004)

Roberto Civino and Valerio Fedele
DISIM, Università degli Studi dell'Aquila
via Vetoio
67100 Coppito AQ
Italy
e-mail: roberto.civino@univaq.it;
valerio.fedele@graduate.univaq.it

Received: August 20, 2025.
Accepted: January 24, 2026.