# Automorphisms and classification of particular $\mathbb{F}_2$-braces

Valerio Fedele
University of L'Aquila

joint work with R. Civino & N. Gavioli

Young Researchers Algebra Conference 2023 - L'Aquila

26th July 2023

# The setting

- $V$ finite dimensional vector space over $\mathbb{F}_2$;
- $T_+$ the group of translations of $V$;
- $T_\circ = \{\tau_v : \ v \in V\}$ abelian regular subgroup of the affine group, such that $T_+ < \mathrm{N}_{\mathrm{Sym}(V)}(T_\circ)$;
- an operation on $V$ defined by $u \circ v = u\tau_v$ for $u, v \in V$.

## Problem

- *How to determine the automorphism group* $\mathrm{Aut}(V, +, \circ) = \mathrm{GL}(V) \cap \mathrm{Aut}(V, \circ)$?
- *How many such structures are there up to dimension 8? How many up to isomorphism?*

## Braces and radical algebras

Let us consider the operation on $V$ defined by

$$u \cdot v = u + v + u \circ v, \qquad u, v \in V$$

Then

- $(V, +, \cdot)$ is a **commutative $\mathbb{F}_2$-algebra** such that $V \cdot V \cdot V = 0$, [Caranti, 2020]
- $(V, +, \circ)$ is a **bi-skew brace** (with underlying $\mathbb{F}_2$-vector space $V$), [Childs, 2019]

| | | |
|---|---|---|
| **isomorphism classes** of $(V, +, \cdot)$ (respectively of $(V, +, \circ)$) | $\longleftrightarrow$ | **conjugacy classes** under $\mathrm{GL}(V)$ of $T_\circ < \mathrm{AGL}(V)$ such that $T_+ < \mathrm{N}_{\mathrm{Sym}(V)}(T_\circ)$ |

# Alternating bilinear maps

Let $W$ and $U$ be finite dimensional vector spaces over $\mathbb{F}_2$. A bilinear map

$$\phi : W \times W \longrightarrow U$$

is **alternating** if $\phi(w, w) = 0$ for every $w \in W$.

## Definition

Two alternating bilinear maps $\phi, \psi : W \times W \longrightarrow U$ are **equivalent** if there exist $A \in \mathrm{GL}(W)$, $D \in \mathrm{GL}(U)$ such that for every $u, v \in V$

$$\phi(u, v)D = \psi(u\,A, v\,A)$$

$$\begin{array}{ccc} W \times W & \xrightarrow{\phi} & U \\ \Big\downarrow{\scriptstyle A\times A} & & \Big\downarrow{\scriptstyle D} \\ W \times W & \xrightarrow{\psi} & U \end{array}$$

# Alternating matrices

Fixing basis of $W$ and $U$, the alternating bilinear map $\phi$ can be represented by a $d$-tuple $(B_1^\phi, \ldots, B_d^\phi)$ of $m \times m$ **alternating matrices** (i.e., **symmetric** and 0-**diagonal** matrices), such that

$$\phi(u, v) = (u\, B_1^\phi\, v^T, \ldots, u\, B_d^\phi\, v^T)$$

$$\phi(u, v) = (\phi_1(u, v), \ldots, \phi_d(u, v))$$

$$\{w_1, \ldots, w_m\} \text{ basis of } W, \quad B_k^\phi = \left[\phi_k(w_i, w_j)\right],\ 1 \leq k \leq d$$

$$\phi_k(u, v) = u\, B_k^\phi\, v^T$$

Conversely, given a $d$-tuple of alternating matrices, one can define an alternating bilinear map as such.

# Alternating matrices

Two alternating bilinear maps $\phi, \psi : W \times W \longrightarrow U$ **are equivalent if and only if** the associated alternating matrix spaces

$$\mathcal{B}^\phi = \langle B_1^\phi, \ldots, B_d^\phi \rangle$$

and

$$\mathcal{B}^\psi = \langle B_1^\psi, \ldots, B_d^\psi \rangle$$

are **congruent**, i.e., there exist $A \in GL(W)$ such that

$$A\mathcal{B}^\psi A^T = \mathcal{B}^\phi$$

($AB_j^\psi A^T \in \mathcal{B}^\phi$ for every $j \in \{1, \ldots, d\}$).

# Alternating matrices associated to a radical algebra

- $(V, +, \cdot)$ commutative $\mathbb{F}_2$-algebra such that $V \cdot V \cdot V = 0$;
- $\mathrm{Ann}(V) = \{\, u \in V \mid u \cdot v = 0 \;\; \forall\, v \in V \,\}$.

$V = W \oplus \mathrm{Ann}(V), \quad m = \dim(W), \quad d = \dim(\mathrm{Ann}(V))$

Since $u \cdot v \in \mathrm{Ann}(V)$, there exist an alternating bilinear map

$$\phi : W \times W \longrightarrow \mathrm{Ann}(V)$$

such that

$$u \cdot v = \big(\, 0_w, \, \phi(u_w, v_w) \,\big)$$

A $d$-tuple $(B_1, \ldots, B_d)$ of $m \times m$ alternating matrices **determines** $\phi$ **if and only if**

$$\mathrm{Rank}\left[ B_1 \,|\, B_2 \,|\, \ldots \,|\, B_d \right] = m$$

# Characterization of isomorphisms and automorphisms

## Theorem

1) *Two commutative $\mathbb{F}_2$-algebras of nilpotency class 3, $(V, +, \cdot_\phi)$ and $(V, +, \cdot_\psi)$ are isomorphic if and only if their alternating matrix vector spaces $\mathcal{B}^\phi$ and $\mathcal{B}^\psi$ are congruent.*

2) $M \in \mathrm{Aut}(V, +, \cdot_\phi)$, $V = W \oplus \mathrm{Ann}(V)$ *if and only if* $M = \begin{bmatrix} A & C \\ 0 & D \end{bmatrix}$ *where* $A \in GL(W)$, $D = \left[D_{i,j}\right] \in GL(\mathrm{Ann}(V))$, $C \in \mathbb{F}_2^{m \times d}$ *such that*

$$AB_j^\phi A^T = \sum_{i=1}^{d} D_{i,j} B_i^\phi \qquad \forall j \in \{1, \ldots, d\}$$

*(i.e.,* $\phi(u_w A, v_w A) = \phi(u_w, v_w) D$ *for every* $u, v \in W$*).*

# Primitive algebras

## Definition

We say that $(V, +, \cdot)$ is **primitive** if the subspace

$$V \cdot V := \langle u \cdot v : \ u, v \in V \rangle_+ \subseteq \mathrm{Ann}(V)$$

coincides with $\mathrm{Ann}(V)$.

**If** $(V, +, \cdot)$ **is not primitive**, then

- $\mathrm{Ann}(V) = (V \cdot V) \oplus Z$, $\dim(Z) \geq 1$ and $V = W \oplus (V \cdot V) \oplus Z$.
- $V/Z$ is a primitive algebra and $\dim(V/Z) = \dim(W) + \dim(V \cdot V)$.

For the classification of these structures, it is convenient to use $m = \dim(W)$ and $d = \dim(V \cdot V)$ as parameters.

# Some particular cases

## Proposition

*Let $(V, +, \cdot_\phi)$ be a primitive algebra and $m$ the co-dimension of $V \cdot V$. The following statements hold:*

- $\dim(V \cdot V) = \dim(\mathcal{B}^\phi)$, *in particular, denoting by $\Lambda(m, \mathbb{F}_2)$ the full alternating matrix vector space,*

$$(m \bmod 2) + 1 \leq \dim(V \cdot V) \leq \dim(\Lambda(m, \mathbb{F}_2)) = \binom{m}{2}$$

- *There is a* **unique isomorphism class** *of primitive algebra with uni-dimensional $V \cdot V$ (and in this case $m$ is even).*
- *There is a* **unique isomorphism class** *of primitive algebras such that* $\dim(V \cdot V) = \dim \Lambda(m, \mathbb{F}_2) = \binom{m}{2}$;
- *For $m = 3$ there are* **two isomorphism classes** *determined by* $\dim(V \cdot V) \in \{2, 3\}$. *In particular,* $\mathcal{B}^\phi = \Lambda(3, \mathbb{F}_2) = \langle B_1, B_2, B_3 \rangle$ *or* $\mathcal{B}^\phi = \{0, B_1, B_2, B_1 + B_2\}$.

# Classification results up to $n = 8$

| $n$ | $m$ | $d$ | # classes | # primitive | # operations $\circ$ |
|---|---|---|---|---|---|
| * | 2 | $\geqslant 1$ | 1 | 1 | |
| * | 3 | $\geqslant 3$ | 2 | 2 | |
| 5 | 3 | 2 | 1 | 1 | 42 |
| 5 | 4 | 1 | 1 | 1 | 28 |
| 6 | 4 | 2 | 4 | 3 | 3360 |
| 7 | 4 | 3 | 9 | 5 | 254968 |
| 7 | 5 | 2 | 2 | 2 | 937440 |
| 7 | 6 | 1 | 1 | 1 | 13888 |
| 8 | 4 | 4 | 13 | 4 | 16716840 |

In particular, for $m = 4$ we have $13 = 1 + 3 + 5 + 4$ isomorphism classes of primitive algebras for $d = \dim(V \cdot V) \in \{1, 2, 3, 4\}$ which is the same number as the case $m = 4$ and $d = \dim(\mathrm{Ann}(V)) = 4$.

# ¿Questions?

# Bibliography


A. Caranti.
Bi-skew braces and regular subgroups of the holomorph.
*Journal of Algebra*, 562:647–665, 2020.

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

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

R. Civino, V. Fedele, and N. Gavioli.
Classification of binary bi-braces.
*Work in progress*, 2023.

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