J Algebr Comb (2017) 45:455–473
DOI 10.1007/s10801-016-0713-7

# A family of semifields in characteristic 2

**Daniele Bartoli**[1] · **Jürgen Bierbrauer**[2] · **Gohar Kyureghyan**[3] · **Massimo Giulietti**[4] · **Stefano Marcugini**[4] · **Fernanda Pambianco**[4]

Received: 7 January 2016 / Accepted: 6 September 2016 / Published online: 16 September 2016

**Abstract** We construct and describe the basic properties of a family of semifields in characteristic 2. The construction relies on the properties of projective polynomials over finite fields. We start by associating non-associative products to each such polynomial. The resulting presemifields form the degenerate case of our family. They are isotopic to the Knuth semifields which are quadratic over left and right nuclei. The non-degenerate members of our family display a very different behavior. Their left and right nuclei agree with the center, the middle nucleus is quadratic over the center. None of those semifields is isotopic or Knuth equivalent to a commutative semifield. As a by-product we obtain the complete taxonomy of the characteristic 2 semifields which are quadratic over the middle nucleus, bi-quadratic over the left and right nuclei and not isotopic to twisted fields. This includes determining when two such semifields are isotopic and the order of the autotopism group.

The research of D. Bartoli, M. Giulietti, S. Marcugini, and F. Pambianco was supported in part by Ministry for Education, University and Research of Italy (MIUR) (Project PRIN 2012 ”Geometrie di Galois e strutture di incidenza”) and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The work of D. Bartoli was supported also by the European Community under a Marie-Curie Intra-European Fellowship (FACE Project: Number 626511). J. Bierbrauer’s research was supported in part by GNSAGA - INdAM.

✉ Daniele Bartoli
daniele.bartoli@unipg.it

[1] Department of Mathematics, Ghent University, 9000 Ghent, Belgium

[2] Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, USA

[3] Institut für Algebra und Geometrie, Otto-von-Guericke Universität Magdeburg, 39106 Magdeburg, Germany

[4] Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, 06123 Perugia, Italy

**Keywords** Semifields · Isotopy · Projective polynomials · Nuclei · Center · Knuth semifields · Twisted fields

**Mathematics Subject Classification** 12K10 · 51E15 · 51A40

## 1 Introduction

A finite **presemifield** of order $q = p^r$ ($p$ a prime) is an algebra $(F, +, *)$ of order $q$ which satisfies the axioms of the field of order $q$ with the possible exception of the associativity of multiplication and the existence of an identity element of multiplication. A presemifield is a **semifield** if in addition an identity element of multiplication exists. The addition in a presemifield may be identified with the addition in the field of the same order. A presemifield is **commutative** if its multiplication is commutative. A geometric motivation to study (pre)semifields comes from the fact that there is a bijection between presemifields and projective planes of the same order which are translation planes and also duals of translation planes. Presemifields $(F, +, *)$ and $(F, +, \circ)$ of order $q = p^r$ are defined to be **isotopic** if there exist elements $\alpha_1, \alpha_2, \beta \in GL(r, p)$ such that $\beta(\alpha_1(x) * \alpha_2(y)) = x \circ y$ always holds. This equivalence relation is motivated by the geometric link as well. In fact, two presemifields are isotopic if and only if they determine isomorphic projective planes (see Albert [1]).

General constructions of semifields which give families of examples that exist in arbitrary characteristic and in each characteristic $p$ for an infinity of dimensions $r$ are hard to come by. A classical example are the Albert twisted fields [2].

Recently, a new family of presemifields in odd characteristic $p$ has been defined in [4] by using the theory of projective polynomials and Albert twisted fields as ingredients. This is a large family, since it contains the Budaghyan–Helleseth family of odd characteristic commutative semifields (see [7]) and an infinity of semifields which are not isotopic to commutative semifields. Examples of the new family exist for each order $q = p^r$ where $p$ is a prime and $r = 2m$ is even.

The aim of the present paper is to construct and investigate an analogue of such a family in characteristic 2. A first step in this direction was taken in [5]. Our approach is based on the projection method, as described in [4]. Basic ingredients for our construction are **projective polynomials.** We use the theory of projective polynomials over finite fields as given in Bluher [6]. The definition of the characteristic 2 family $B(2, m, s, l, t)$ is in Sect. 1.2. The underlying projective polynomial is $p_{s,t}(X) = p_1 X^{2^s+1} + p_2 X^{2^s} + p_3 X + p_4 \in \mathbb{F}_{2^m}[X]$ in Definition 1.

In fact, the theory of presemifields sheds some more light on the theory of projective polynomials. This is seen in Sect. 2 where we associate a multiplication $*$ on $\mathbb{F}_{2^{2m}}$ to each such projective polynomial $p_{s,t}(X) \in \mathbb{F}_{2^m}[X]$ (see Definition 3) in such a way that $p_{s,t}(X)$ has no zeroes in $\mathbb{F}_{2^m}$ if and only if the algebra $(F, +, *)$ is a presemifield (Theorem 2). The resulting presemifields form the degenerate case $l = 0$ of our characteristic 2 family. We use this link to define the generic family $B(2, m, s, l, t)$ where $0 \neq l \in \mathbb{F}_{2^m}$ in Sect. 1.2 and to study its properties later on. In particular we prove that none of the presemifields $B(2, m, s, l, t)$ is isotopic to a commutative semifield (Sect. 9). This contrasts with the odd characteristic case where the Budaghyan–Helleseth family of commutative semifields is contained in our family and it remains an open problem if our family contains commutative examples which do not belong to the Budaghyan–Helleseth family. A similar feature concerns the nuclei. Here $x \in F$ belongs to the **left nucleus** of a semifield $(F, +, *)$ if the associativity equation $x * (y * z) = (x * y) * z$ holds for all $y, z$. Analogous statements characterize the **middle nucleus** and the **right nucleus.** Isotopic semifields have isomorphic nuclei. The nuclei correspond to certain important subgroups of the collineation group of the corresponding projective plane. We determine the nuclei of the semifields isotopic to $B(2, m, s, l, t)$ in Sect. 10. Again this is a more complete result than in the odd characteristic case where the determination of the middle nucleus remains an open problem. As a by-product of our results in a parametric special case we obtain a complete characterization of the semifields in characteristic 2 which are quadratic over one of the nuclei, quartic over the center and are not isotopic to generalized twisted fields.

The smallest order in which examples of our generic family exist is 256. The corresponding presemifields $B(2, 4, 2, l, t)$ where $0 \neq l \in L = \mathbb{F}_{16}, l^5 \neq 1$ and $t = [p_1, p_2, p_3, p_4] \in L^4$ is legitimate in the sense of Definition 1 come in three isotopy classes, each with autotopism group of order 450 (see Sect. 8). They correspond to three isomorphism classes of projective semifield planes of order $2^8$ each of which has $450 \times 2^{24}$ collineations.

In Sect. 1.1 we introduce compact notation. The definition of our family is in Sect. 1.2. We close this introduction with a detailed description of the results of this paper in Sect. 1.3.

### 1.1 A standard situation in characteristic 2

All our semifields have even dimension $r = 2m$. Let $F = GF(2^{2m}) \supset L = GF(2^m)$ and $T, N : F \longrightarrow L$ the norm and trace functions. Let $\mu \in L$ be of absolute trace $= 1$ and $z \in F$ such that $z^2 + z = \mu$. Then $z \notin L$ and we use $1, z$ as a basis of $F|L$. In particular we write $x = a + bz = (a, b)$ where $a, b \in L$ and refer to $a, b$ as the real and imaginary part $Re(x)$ and $Im(x)$, respectively.

Let $0 \leq s < 2m$ and $x \mapsto x^\sigma$ be the corresponding field automorphism, where $\sigma = 2^s$, let $K_1 = \mathbb{F}_{2^{\gcd(m,s)}}$ be the fixed field of $\sigma$ in $L$. Then $z^4 = z^2 + \mu^2 = z + \mu^2 + \mu$. Continuing like that we obtain the following:

**Lemma 1** *Let* $\mu_s = \sum_{i=0}^{s-1} \mu^{2^i}$. *Then* $z^\sigma = z + \mu_s$ *and* $x^\sigma = (a^\sigma + \mu_s b^\sigma, b^\sigma)$.

In particular $\mu_0 = 0$, $\mu_1 = \mu$, $\mu_2 = \mu + \mu^2$ and $\mu_m = tr_{L|\mathbb{F}_2}(\mu) = 1$ (because of the transitivity of the trace), and $\overline{z} = z^{2^m} = z + 1$. Further $\mu_{s+m} = \mu_s + 1$. We have $\overline{x} = (a + b, b)$, $T(x) = Im(x) = b$, and

$$(a, b)(c, d) = (ac + \mu bd, ad + bc + bd).$$

In particular $1/z = (1/\mu, 1/\mu)$ and $1/(a, b) = (1/D)(a + b, b)$, where $D = a^2 + ab + \mu b^2$. The conjugates of $x$ are

$$x^2 = (a^2 + \mu b^2, b^2), x^4 = (a^4 + (\mu^2 + \mu)b^4, b^4), \dots, x^\sigma = (a^\sigma + (\mu^{2^{s-1}} + \cdots + \mu)b^\sigma, b^\sigma).$$

### 1.2 A family of semifields

**Definition 1** Let $m, s, \sigma$ as in Sect. 1.1. The quadruple $t = [p_1, p_2, p_3, p_4] \in L^4$ is **legitimate** if the polynomial $p_{s,t}(X) = p_1 X^{\sigma+1} + p_2 X^\sigma + p_3 X + p_4$ has no roots in $L$. Let $\Omega = \Omega(m, s)$ be the set of legitimate quadruples. Let further $l \in L$ such that either $l = 0$ or $l \in L^* \setminus (L^*)^{\sigma-1}$ where $L^* = L \setminus \{0\}$. Consider the multiplication

$$x \circ y = \big(p_1 ac^\sigma + lp_1 a^\sigma c + p_2 bc^\sigma + lp_2 a^\sigma d + p_3 ad^\sigma + lp_3 b^\sigma c + p_4 bd^\sigma + lp_4 b^\sigma d, ad + bc\big) \tag{1}$$

where $x, y \in F$. We will see in Theorem 3 that it defines a presemifield. This presemifield will be denoted $B(2, m, s, l, t)$.

In order to obtain an expression of $x \circ y$ using constants from the larger field $F$ we use the following terminology:

**Definition 2** Let $C_1 = (v_1, h_1), C_2 = (v_2, h_2) \in F$. The quadruple $t = t(C_1, C_2) = [p_1, p_2, p_3, p_4] \in L^4$ **corresponding to** the pair $(C_1, C_2) \in F^2$ is defined by

$$p_1 = h_1 + h_2, p_2 = v_1 + v_2 + h_1 + h_2, p_3 = v_1 + v_2 + \mu_s h_1 + (\mu_s + 1)h_2,$$
$$p_4 = \mu_s v_1 + (\mu_s + 1)v_2 + (\mu_s + \mu)h_1 + (\mu_s + \mu + 1)h_2.$$

**Proposition 1** *Let $t = t(C_1, C_2) = [p_1, p_2, p_3, p_4]$. Then*

$$x \circ y = T\left(\left(C_1\overline{y}^\sigma + C_2 y^\sigma\right)x\right) + lT\left(\left(C_2 y + \overline{C_1 y}\right)x^\sigma\right) + T(x\overline{y})z. \tag{2}$$

*Proof* This is a direct calculation, using $xy^\sigma = (a, b)(c^\sigma + \mu_s d^\sigma, d^\sigma) = (ac^\sigma + \mu_s ad^\sigma + \mu bd^\sigma, ad^\sigma + bc^\sigma + (\mu_s + 1)bd^\sigma)$, $x\overline{y}^\sigma = (a, b)(c^\sigma + (\mu_s + 1)d^\sigma, d^\sigma) = (ac^\sigma + (\mu_s + 1)ad^\sigma + \mu bd^\sigma, ad^\sigma + bc^\sigma + \mu_s bd^\sigma)$ and analogous expressions. □

### 1.3 The structure of the paper

In the remainder of the paper we study the presemifields $B(2, m, s, l, t)$ and the semifields isotopic to them. The proof that the $B(2, m, s, l, t)$ are indeed presemifields is in Sect. 3. The multiplication $x \circ y$ in $B(2, m, s, l, t)$ is given in (1) (on the level of the field $L$), as well as in Proposition 1 in terms of the larger field $F$. If the automorphism associated to $\sigma$ is the identity on $L$ (cases $s = 0, s = m$), it follows from the general form of $x \circ y$ that $L$ is in the center of a semifield isotopic to $B(2, m, s, l, t)$ (see [4], Proposition 3). This implies that we are in the field case. It may therefore be assumed that $s \neq 0, s \neq m$. Isotopies are studied in Sect. 4. In Sect. 5 we use this to define a group, direct product of a cyclic group and a group $GL(2, L)$, which permutes our presemifields (for given $m, s, l$).

Observe that the condition on $l \in L$ is independent of the conditions on the quadruple $t$. The special case $l = 0$ is degenerate but interesting as the corresponding semifields are those which are quadratic over left and right nuclei (Knuth [12], see Sect. 6). In the remainder of the paper we exclude the degenerate case $l = 0$ from the discussion. Cases $m/\gcd(m,s)$ even and $m/\gcd(m,s)$ odd behave rather differently. It is shown in Sect. 7 that in the former case the multiplication simplifies. We study the case $s = m/2$ in Sect. 8. The semifields which are quadratic over one of the nuclei and quartic over the center have been classified in Cardinali et al. [8]. Using this we show that up to equivalence in the Knuth cube (see [12]) our semifields in case $s = m/2$ are precisely those characteristic 2 semifields which have this property and are not isotopic to generalized twisted fields [2] or to Hughes–Kleinfeld semifields [11]. We also obtain a complete taxonomy of those characteristic 2 semifields in Sect. 8. We determine when two of them are isotopic and we determine the autotopism groups (Theorem 6). In Sect. 9 it is shown that $B(2,m,s,l,t), s \neq 0, s \neq m$ is never isotopic to a commutative semifield. The nuclei of the semifields isotopic to $B(2,m,s,l,t), l \neq 0$ are studied in Sect. 10: the left and right nuclei agree with the center of order $2^{\gcd(m,s)}$, whereas the middle nucleus is a quadratic extension of the center.

We start in Sect. 2 by associating non-associative products to projective polynomials. This is done here in characteristic 2 but it works over any positive characteristic. This leads to case $l = 0$ of Definition 1 and to Knuth semifields.

## 2 The associated product

**Definition 3** Let $C_1 = (v_1, h_1), C_2 = (v_2, h_2) \in F, t = t(C_1, C_2) = [p_1, p_2, p_3, p_4]$,

$$P_{C_1,C_2,s}(X) = C_2 X^{\sigma+1} + \overline{C_1} X^{\sigma} + C_1 X + \overline{C_2} \in F[X] \tag{3}$$

and

$$x * y = T((C_1 y^{\sigma} + C_2 \overline{y}^{\sigma})x) + T(xy)z \quad \text{(where } x, y \in F\text{)}, \tag{4}$$

$x, y \in F$, be the multiplication **associated to** the projective polynomial $P_{C_1,C_2,s}(X)$. Consider also the isotope

$$x \circ y = x * \overline{y} = T((C_1 \overline{y}^{\sigma} + C_2 y^{\sigma})x) + T(x\overline{y})z \tag{5}$$

Comparison with (2) shows that $x \circ y$ in Definition 3 is precisely the multiplication in $B(2, m, s, 0, t)$.

**Lemma 2** *With notation as in Definition 3 we have*

$$v_1 = (\mu_s + \mu)p_1 + \mu_s p_2 + p_3 + p_4, h_1 = \mu_s p_1 + p_2 + p_3,$$
$$v_2 = (\mu_s + \mu + 1)p_1 + (\mu_s + 1)p_2 + p_3 + p_4, h_2 = (\mu_s + 1)p_1 + p_2 + p_3.$$

**Theorem 1** *The following are equivalent:*

- *$(F, *)$ is a presemifield.*
- *$T(C_1x\overline{x}^\sigma + C_2x^{\sigma+1}) \neq 0$ for all $0 \neq x \in F$.*
- *$P_{C_1,C_2,s}(X)$ has no root of norm 1.*

*Proof* Assume $x * y = 0$ for $xy \neq 0$. The imaginary part of (4) shows $T(xy) = 0$, equivalently $y = e\overline{x}$ for some $e \in L$. The real part shows $T(C_1x\overline{x}^\sigma + C_2x^{\sigma+1}) = 0$. Write this out, divide by $\overline{x}^{\sigma+1}$. This gives

$$\overline{C}_1\left(\frac{x}{\overline{x}}\right)^\sigma + \overline{C}_2 + C_1\left(\frac{x}{\overline{x}}\right) + C_2\left(\frac{x}{\overline{x}}\right)^{\sigma+1} = 0,$$

that is $\theta = \frac{x}{\overline{x}}$ is a root of $P_{C_1,C_2,s}(X)$ having norm 1. On the other hand, if $\theta$ is a root of $P_{C_1,C_2,s}(X)$ of norm 1, let $x \in F$ be such that $x^{q-1} = 1/\theta$ and $y = e\overline{x}$ for some $e \in L^*$. Therefore $x * y = 0$ and $xy \neq 0$. □

**Corollary 1** *If the conditions of the previous theorem are satisfied, then $p_1 \neq 0$.*

*Proof* Case $X = 1$ shows $T(C_1) + T(C_2) = h_1 + h_2 = p_1 \neq 0$. □

**Theorem 2** *The statements in Theorem 1 are also equivalent to $p_{s,t}(X)$ (see Definition 1) having no root in $L$.*

*Proof* Assume $x \circ y = x * \overline{y} = 0$, $xy \neq 0$. Use the special case $l = 0$ of (1). If $d = 0$ the imaginary part shows $b = 0$, $ac \neq 0$. Then $p_1 = 0$, contradiction. Let $d \neq 0$. By homogeneity it can be assumed $d = 1$ and therefore $a = bc$. Divide by $b$. □

**Lemma 3** *If the conditions of Theorem 1 are satisfied, then $N(C_1) \neq N(C_2)$.*

*Proof* Assume $N(C_1) = N(C_2)$, equivalently $C_1 = z_0C_2 \neq 0$ for $N(z_0) = 1$. Let $z$ be defined by $z^\sigma = z_0$. Then $P_{C_1,C_2,s}(z) = 0$. □

**Definition 4** Given $m, s$ we call a pair $(C_1, C_2) \in F^2$ **legitimate** if the conditions of Theorem 1 are satisfied.

Observe that $(C_1, C_2)$ is legitimate if and only if $t(C_1, C_2)$ is legitimate, see Definition 1. We will see in Proposition 7 that the semifields isotopic to the presemifields in Theorem 1 are precisely those which are quadratic over right and left nuclei.

## 3 The presemifield property

We consider the multiplication $x \circ y$ in $B(2, m, s, l, t)$, see (1) or (2). Let $x * y = x \circ \overline{y}$. Clearly

$$x * y = T((C_1y^\sigma + C_2\overline{y}^\sigma)x) + lT((\overline{C_1}y + C_2\overline{y})x^\sigma) + T(xy)z. \tag{6}$$

**Theorem 3** *$B(2, m, s, l, t)$ in Definition 1 is indeed a presemifield (of order $2^{2m}$).*

*Proof* For $l = 0$ this is Theorem 1. Let $l \neq 0$, assume $x * y = 0, xy \neq 0$. The imaginary part shows $y = e\overline{x}$ for $e \in L$. The real part factorizes: $(e^\sigma + le)T(C_1 x\overline{x}^\sigma + C_2 x^{\sigma+1}) = 0$. The first factor is nonzero by the condition on $l$, the non-vanishing of the trace term is the second condition of Theorem 1. □

Observe that the condition on $l$ in Definition 1 can be met for $l \neq 0$ only if $\gcd(m, s) \neq 1$. In particular $m$ has to be a composite number. The smallest choice is therefore $m = 4$ and the resulting semifields have order $2^8$.

**Corollary 2** *$B(2, m, s, l, t)$ where $l \neq 0, s \notin \{0, m\}$ is not isotopic to a field.*

*Proof* The restriction to $L$ is $x * y = (h_1 + h_2)(xy^\sigma + lx^\sigma y)$. When $l \neq 0$ and $\sigma$ is not the identity on $L$, then this is isotopic to a twisted field. In fact, a twisted field $(L, \bullet)$ is defined by $x \bullet y = xy^\sigma + lx^\sigma y$. □

## 4 Isotopies

In this section we study isotopies among the presemifields $B(2, m, s, l, t)$. The opposite of a presemifield $(F, *)$ is defined by $x \circ y = y * x$. The proof of the following assertion is straightforward.

**Proposition 2** *The opposite of $B(2, m, s, l, t(C_1, C_2)), l \neq 0$ is isotopic to $B(2, m, s, 1/l, t(\overline{C_1}, \overline{C_2}))$. Here $t(\overline{C_1}, \overline{C_2}) = [p_1, p_2 + p_1, p_3 + p_1, p_4 + p_1 + p_2 + p_3]$.*

**Proposition 3**

- *$B(2, m, s, l, t), l \neq 0$ is isotopic to $B(2, m, s, \lambda^{\sigma-1} l, t)$ for arbitrary $\lambda \in L^*$;*
- *$B(2, m, s, l, t)$ is isotopic to $B(2, m, s, l, \lambda t)$ for arbitrary $\lambda \in L^*$ (**scalar isotopy**);*
- *$B(2, m, s, l, [p_1, p_2, p_3, p_4])$ is isotopic to $B(2, m, s, l^2, [p_1^2, p_2^2, p_3^2, p_4^2])$ (**Galois isotopy**);*
- *$B(2, m, s, l, [p_1, p_2, p_3, p_4])$ is isotopic to $B(2, m, s, l, [k_1^{\sigma+1} p_1, k_1^\sigma k_2 p_2, k_1 k_2^\sigma p_3, k_2^{\sigma+1} p_4])$ for arbitrary $k_1, k_2 \in L^*$ (**diagonal isotopy**).*

*Proof* For the first statement use the substitution $x \mapsto \lambda x, y \mapsto y$. Scalar isotopy is obvious. As for Galois isotopy, apply the inverse of the Frobenius map to $a, b, c, d$, and then apply the Frobenius map to the real and to the imaginary part. Diagonal isotopy follows from the substitution $a \mapsto k_1 a, b \mapsto k_2 b, c \mapsto k_1 c, d \mapsto k_2 d$. □

Diagonal isotopy is a special case of linear isotopy, as follows.

**Proposition 4** (Linear isotopy) *$B(2, m, s, l, [p_1, p_2, p_3, p_4])$ is isotopic to $B(2, m, s, l, [p_1', p_2', p_3', p_4'])$ where*

$$
\begin{aligned}
p_1' &= \alpha^{\sigma+1} p_1 + \alpha^\sigma \gamma p_2 + \alpha \gamma^\sigma p_3 + \gamma^{\sigma+1} p_4 \\
p_2' &= \alpha^\sigma \beta p_1 + \alpha^\sigma \delta p_2 + \beta \gamma^\sigma p_3 + \gamma^\sigma \delta p_4 \\
p_3' &= \alpha \beta^\sigma p_1 + \beta^\sigma \gamma p_2 + \alpha \delta^\sigma p_3 + \gamma \delta^\sigma p_4 \\
p_4' &= \beta^{\sigma+1} p_1 + \beta^\sigma \delta p_2 + \beta \delta^\sigma p_3 + \delta^{\sigma+1} p_4
\end{aligned}
$$

*and $\alpha, \beta, \gamma, \delta \in L$ such that $\alpha\delta \neq \beta\gamma$.*

*Proof* This corresponds to the substitutions $a' = \alpha a + \beta b, b' = \gamma a + \delta b, c' = \alpha c + \beta d, d' = \gamma c + \delta d$, where $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL(2, L)$. □

**Corollary 3** *$B(2, m, s, l, [p_1, p_2, p_3, p_4])$ is isotopic to $B(2, m, s, l, [1, 0, u, v])$ for suitable $v$, where $u \in \{0, 1\}$.*

*Proof* As $p_1 \neq 0$ it follows from scalar isotopy that we may assume $p_1 = 1$. Linear isotopy with $\alpha = 1, \gamma = 0, \beta = p_2\delta$ leads to a quadruple $[1, 0, *]$. Assume this quadruple has $p_3 \neq 0$. Application of linear isotopy to this quadruple with $\alpha = 1, \beta = \gamma = 0$ yields the claim. □

The following special case of linear isotopy is interesting in its own right.

**Theorem 4** *$B(2, m, s, l, t(C_1, C_2))$ is isotopic to $B(2, m, s, l, t(\alpha\overline{\alpha}^{\sigma} C_1, \alpha^{\sigma+1} C_2))$ for all $0 \neq \alpha \in F$.*

*Proof* Use Eq. (2) and the substitutions $x \mapsto \alpha x, y \mapsto \alpha y$ for an arbitrary nonzero $\alpha \in F$. □

**Proposition 5** *$B(2, m, s, l, t(C_1, C_2))$ is isotopic to $B(2, m, s + m, l, t(C_2, C_1))$.*

*Proof* This follows from basic properties of the trace. □

Note that by Proposition 5 we may assume $s \leq m$. The following proposition shows that we may in fact assume $s \leq m/2$.

**Proposition 6** *Let $s < m, \sigma{=}2^s, \tau{=}2^{m-s}$. Then $B(2, m, s, l, [p_1, p_2, p_3, p_4]), l \neq 0$ is isotopic to $B(2, m, m - s, 1/l, [p_1, p_3, p_2, p_4])$.*

*Proof* Apply $\tau$ to $a, b, c, d$, then divide the real part by $l$, apply $\sigma$ to the imaginary part. □

## 5 The restricted isotopy group

**Definition 5** Given $m$ and $s$, the **restricted isotopy group** is the direct product $G_1 = GL(2, L) \times L^*$ where $GL(2, L)$ and $L^*$ act on the legitimate pairs $(C_1, C_2)$ and on the legitimate quadruples $[p_1, p_2, p_3, p_4]$ by linear isotopy and scalar isotopy, respectively.

Observe that $|G_1| = (q - 1)(q^2 - 1)(q^2 - q)$, where $q = 2^m$.

**Lemma 4** *Let $\Omega = \Omega(m, s)$ be the set of legitimate quadruples, see Definition 4. Then $|\Omega| = \frac{(q+1)q(q-1)^2 2^d}{2(2^d+1)}$. Here $d = \gcd(m, s)$.*

*Proof* Use a formula from Bluher theory [6]: let $N_0$ be the number of elements $b \in L$ such that $X^{\sigma+1} + bX + b$ has no zeroes in $L$. Then $N_0 = 2^{d-1}(2^m + 1)/(2^d + 1)$ provided $m/d$ is odd, and $N_0 = 2^{d-1}(2^m - 1)/(2^d + 1)$ if $m/d$ is even.
Let also $g = \gcd(2^m - 1, 2^s + 1)$ and observe that $g = 1$ if $m/d$ odd, whereas $g = 2^d + 1$ if $m/d$ is even. Elementary counting shows

$$|\Omega| = (q-1)\{q(q-1-(q-1)/g) + q(q-1)N_0\} = q(q-1)^2(1 - 1/g + N_0).$$

In both cases the same formula results. □

We will use the action of $G_1$ on the set $\Omega$ of legitimate quadruples and the fact that for each $l$ where either $l = 0$ or $l \neq 0, l \notin (L^*)^{\sigma-1}$ legitimate quadruples in the same orbit under $G_1$ yield isotopic presemifields $B(2, m, s, l, t)$.

## 6 The degenerate case $l = 0$ : Knuth semifields

**Proposition 7** *The semifields isotopic to $B(2, m, s, 0, t)$ where $s \notin \{0, m\}$ are precisely those which are quadratic over the left and the right nuclei (in characteristic 2).*

*Proof* The condition on $s$ says that $K_1$ ( the fixed field of the automorphism associated to $\sigma$ in $L$) is properly contained in $L$. It can be assumed that $p_1 = 1, p_2 = 0, p_3 \in \{0, 1\}$. Start from (1) for $l = 0$, and apply the substitution $b \mapsto b^{1/\sigma}, c \mapsto c^{1/\sigma}, d \mapsto d^{1/\sigma}$; then take the $\sigma-$th power of the imaginary part. This leads to $(a, b) * (c, d) = (ac + p_4 b^{1/\sigma} d, a^\sigma d + bc)$ when $p_3 = 0$, and to $(a, b) * (c, d) = (ac + ad + p_4 b^{1/\sigma} d, a^\sigma d + bc)$ in case $p_3 = 1$. When $p_3 = 0$ this is the standard form given in Knuth [12], Section 7.4, type IV, case $g = 0$. In case $p_3 = 1$ apply the additional substitution $c \mapsto c + d$ to obtain the standard form in [12], Section 7.4, type IV, case $g = 1$. □

In the sequel we will always assume $l \neq 0$. We saw in Corollary 2 that the corresponding semifields are not fields.

## 7 Case $m/\gcd(m, s)$ even: the C-family

We refer to the semifields isotopic to the $B(2, m, s, l, [1, 0, 0, p_4]), l \neq 0$ as the C-family of semifields. Let $g = \gcd(q - 1, \sigma + 1)$ denote the number of cosets of $(L^*)^{\sigma+1}$ in $L^*$.

**Lemma 5** *If $m/\gcd(m, s)$ is odd, then there is no legitimate quadruple $[1, 0, 0, u]$. If $m/\gcd(m, s)$ is even, then there are $q - 1 - (q-1)/(2^d + 1) = 2^d(q-1)/(2^d + 1)$ legitimate quadruples $[1, 0, 0, u]$ where $d = \gcd(m, s)$.*

*Proof* The quadruple $[1, 0, 0, u]$ is legitimate if $u \notin (L^*)^{\sigma+1}$. If $m/d$ is odd, then $g = 1$ and $[1, 0, 0, u]$ is never legitimate. If $m/d$ is even, then $g = 2^d + 1$. □

**Lemma 6** *Let $m/\gcd(m,s)$ be even. Then $[1,0,0,u_1]$ and $[1,0,0,u_2]$ are in the same orbit under $G_1$ if and only if either $u_2 \in u_1(L^*)^{\sigma+1}$ or $u_2 \in (1/u_1)(L^*)^{\sigma+1}$. The stabilizer of $[1,0,0,u]$ under $G_1$ has order $(q-1)(2^d+1)$.*

*Proof* We have $g = 2^d + 1$ and $K_1 = \mathbb{F}_{2^d} \subseteq (L^*)^{\sigma+1}$. Let the matrix $M$ map $[1:0:0:u_1] \mapsto [1:0:0:u_2]$. We have three conditions:

$$\alpha^\sigma \beta = u_1\gamma^\sigma\delta, \alpha\beta^\sigma = u_1\gamma\delta^\sigma, \beta^{\sigma+1} + u_1\delta^{\sigma+1} = u_2(\alpha^{\sigma+1} + u_1\gamma^{\sigma+1}).$$

We have $\beta = 0$ if and only if $\gamma = 0$ which leads to $u_2$ and $u_1$ in the same coset. Also $\alpha = 0$ iff $\delta = 0$ and this leads to $u_2$ in the same coset as $1/u_1$. Assume all entries of $M$ are nonzero. By homogeneity it can be assumed that $\alpha = 1$. The first two equations show $\beta = u_1\gamma^\sigma\delta, \beta^\sigma = u_1\gamma\delta^\sigma$. Comparison shows $c = u_1\gamma^{\sigma+1} \in K_1$. This yields the contradiction $u_1 \in (L^*)^{\sigma+1}$. □

**Theorem 5** *Given $m, s$ and $l \neq 0$ such that $m/\gcd(m,s)$ is even, all members of $B(2,m,s,l,t)$ belong to the C-family. There are $2^{d-1}$ orbits under $G_1$, where $d = \gcd(m,s)$.*

*Proof* We know from Lemma 6 that there are precisely $2^{d-1}$ orbits under $G_1$ which belong to the C-family. The stabilizer always has order $(q-1)(2^d+1)$, so each orbit has length $(q^2-1)(q^2-q)/(2^d+1)$. As there are $2^{d-1}$ such orbits this exhausts all of $\Omega$. □

## 8 The special case $s = m/2$

Case $s = m/2$ is equivalent with $\sigma \neq 1$ but $\sigma^2 = 1$ on $L$. These are the presemifields $B(2,2s,s,l,t), l \neq 0$. We have $m = 2s$, hence $d = s$ and $m/d = 2$. In particular it follows from Theorem 5 that we can assume up to isotopy $p_1 = 1, p_2 = p_3 = 0, p_4 \notin K = \mathbb{F}_{2^s}$.

For the remainder of this section we will use the following notation:

$$q = 2^s, \quad K = \mathbb{F}_q \subset L = \mathbb{F}_{q^2} \subset F = \mathbb{F}_{q^4}.$$

Let $\tau : L \longrightarrow K$ be the trace function. We keep the notation used in Introduction with respect to a basis $1, z$ of $F \mid L$.

**Definition 6** Let $w \in L \setminus K$ such that $tr_{K|\mathbb{F}_2}(1/\tau(w)) = 0$. Define a multiplication on $F$ by

$$(a,b) \star (c,d) = (ac + bd^q + wb^q d, a^q d + bc).$$

Let $B_q(w) = (F, \star)$.

The condition on $w$ in this definition can be expressed in an equivalent form.

**Lemma 7** *Let $a \in K^*$. Then $a$ can be written in the form $a = l + 1/l$ for some $l \in K$ if and only if $tr_{K|\mathbb{F}_2}(1/a) = 0$.*

*Proof* If $a$ can be written in the required form, then $1/a = l/(1+l^2) = (u+1)/u^2 = 1/u + 1/u^2$ where $u = l+1$. This shows $tr_{K|\mathbb{F}_2}(1/a) = 0$. The same argument works also in the opposite direction. □

**Proposition 8** *$B_q(w)$ in Definition 6 is a semifield of order $q^4$. It has middle nucleus $L$, left and right nuclei $K$ and is not isotopic to a commutative semifield.*

*Proof* Clearly $1 = (1,0)$ is the unit of multiplication. The imaginary part vanishes if and only if both $c = ea^q$ and $d = eb$ hold for some $e \in L$. The real part is then $e(a^{q+1} + (e^{q-1} + w)b^{q+1})) = 0$, with $e \neq 0$. Let $t = e^{q-1} \neq 0$ and observe that $t^q = 1/t$. If $a = 0$, then $w = t$. If $a \neq 0$, then divide by $ea^{q+1}$. In both cases $t + w \in K$. It follows $\tau(w) = t + 1/t$. Let $a = \tau(w)$. By our assumptions and Lemma 7, we have $tr_{K|\mathbb{F}_2}(1/a) = 0$; equivalently $\tau(w) = l + 1/l$ for some $l \in K$. As $t + 1/t = l + 1/l$, we have $t \in K$ and therefore $t = 1$. This leads to the contradiction $w \in K$. The nuclei are determined by a direct calculation. Another direct calculation using the Ganley criterion [9] shows non-commutativity. □

Consider now the presemifields $B(2, 2s, s, l, [1, 0, 0, p_4]), l \neq 0$. By isotopy it may be assumed $l \in K, l \neq 1$.

**Proposition 9** *$B(2, 2s, s, l, [1, 0, 0, p_4])$, with $l \in K^*$, is isotopic to $B_q(w)$, where $w = (l^2 p_4 + p_4^q)/(l\tau(p_4))$.*

*Proof* We have

$$x \circ y = \left(ac^q + la^q c + p_4 bd^q + lp_4 b^q d, ad + bc\right).$$

Substitute $a \mapsto a^q$, then apply $u \mapsto \frac{1}{l^2+1}(lu + u^q)$ to the real part. This yields the product $(ac + \frac{l\tau(p_4)}{l^2+1} bd^q + \frac{p_4^q + l^2 p_4}{l^2+1} b^q d, a^q d + bc)$. Finally, apply the substitutions $b \mapsto \lambda b, d \mapsto \lambda d$, with $\lambda \in L$ such that $\lambda^{q+1} = \frac{l^2+1}{l\tau(p_4)}$. Observe that $w$ does indeed satisfy the condition of Definition 6. In fact, $\tau(w) = (l^2+1)/l$, hence $1/\tau(w) = l/(l^2+1) = 1/u + 1/u^2$, with $u = l+1$; then $1/\tau(w)$ has absolute trace 0. □

**Corollary 4** *The semifields $B(2, 2s, s, l, t)$ coincide with the $B_q(w)$, up to isotopy.*

*Proof* We saw that $p_1 = 1$, $p_2 = p_3 = 0$ can be assumed. Also, the mapping $p_4 \mapsto w$ is given by $w = \frac{p_4^q + l^2 p_4}{l\tau(p_4)}$. Let now $w$ be given. As $tr_{L|\mathbb{F}_2}(1/\tau(w)) = 0$, we can write $\tau(w) = l + 1/l$ for some $l \in L$. Let $p_4 = w + 1/l$. This describes the inverse of the mapping above. □

In the sequel we give a complete census of those semifields.

**Theorem 6** *$B_q(w)$ is isotopic to $B_q(v)$ if and only if $v = \phi(w)$ for some field automorphism $\phi$ of $L = \mathbb{F}_{q^2}$. The order of the autotopism group of $B_q(w)$ is $2\iota(q^2-1)^2$ where $\iota$ is the order of the stabilizer of $w$ in the Galois group of $L$ over $\mathbb{F}_2$.*

In the remainder of this section we prove Theorem 6. One direction is obvious: $B_q(w)$ is isotopic to $B_q(\phi(w))$ for each field automorphism $\phi$ of $L$.

**Lemma 8** *Let $x * y$ denote the product in $B_q(w)$. The triple $(\alpha_1, \alpha_2, \beta)$ defines an isotopic semifield with middle nucleus $L$, left and right nuclei $K$ and satisfying $(a, 0) \circ (c, 0) = (ac, 0)$, $(0, b) \circ (c, 0) = (0, bc)$, $(a, 0) \circ (0, d) = (0, a^q d)$ if and only if for some field automorphism $\phi$ of $L$ the following hold:*

$$\alpha_1(a, 0) = A * \phi(a) = \phi(a)A, \alpha_2(c, 0) = \phi(c) * B = \left(\phi(c)B_1, \phi(c)^q B_2\right).$$
$$\alpha_1(0, c) = C * \phi(c) = (\phi(c)C_1, \phi(c)C_2), \alpha_2(0, d) = \phi(d^q) * D = \left(\phi(d^q)D_1, \phi(d)D_2\right)$$

*where $A = (A_1, A_2), \dots, D = (D_1, D_2)$ are nonzero constants and the following compatibility conditions are satisfied:*

$$A_1^q D_2 = B_1 C_2, A_2 D_1 = B_2 C_1^q, \tag{7}$$
$$w A_2^q D_2 = B_1 C_1 + B_2^q C_2, w B_2 C_2^q = A_1 D_1 + A_2 D_2^q. \tag{8}$$

*Proof* Let $x \circ y = \beta(\alpha_1(x) * \alpha_2(y))$ and $\alpha_1(1, 0) = A, \alpha_2(1, 0) = B, \alpha_1(0, 1) = C, \alpha_2(0, 1) = D$. Then $x \circ y$ defines a semifield if $\beta^{-1}(x) = A * \alpha_2(x) = \alpha_1(x) * B$ always holds. We refer to this as the compatibility condition. It is easy to check that the middle nucleus $M$ of a semifield $(F, *)$ and the middle nucleus $M'$ of a semifield $(F, \circ)$ where $x \circ y = \beta(\alpha_1(x) * \alpha_2(y))$ are related by $M' = \beta(A * M * B)$ where $A = \alpha_1(1), B = \alpha_2(1)$. In our case this says $\beta(A * L * B) = L$, equivalently $\alpha_1(a, 0) = A * \phi(a) = \phi(a)A, \alpha_2(c, 0) = \phi(c) * B = (\phi(c)B_1, \phi(c)^q B_2)$. Here $\phi : L \longrightarrow L$ and $\phi(1) = 1$. Compatibility is already satisfied.

Condition $(ac, 0) = \beta(\alpha_1(a, 0) * \alpha_2(c, 0))$ yields $\phi(ac) = \phi(a)\phi(c)$; in other words, $\phi$ is a field automorphism of $L$.

Equality $(0, bc) = \beta(\alpha_1(0, b) * \alpha_2(c, 0))$ yields $\alpha_1(0, bc) = \phi(c)\alpha_1(0, b)$. The case $b = 1$ implies $\alpha_1(0, c) = C * \phi(c) = (\phi(c)C_1, \phi(c)C_2)$. Analogously $(0, a^q d) = \beta(\alpha_1(a, 0) * \alpha_2(0, d))$ yields $\alpha_2(0, a^q d) = (\phi(a), 0) * \alpha_2(0, b)$. The case $d = 1$ implies $\alpha_2(0, d) = \phi(d^q) * D = (\phi(d^q)D_1, \phi(d)D_2)$. The compatibility equation is

$$(A_1, A_2) * (\phi(b^q)D_1, \phi(b)D_2) = (\phi(b)C_1, \phi(b)C_2) * (B_1, B_2)$$

for all $b \in L$. The imaginary part yields Eq. (7), the real part is

$$\phi(b^q)A_1 D_1 + g(A_2, \phi(b)D_2) = \phi(b)B_1 C_1 + g(\phi(b)C_2, B_2),$$

which, by comparing coefficients of $\phi(b)$ and $\phi(b^q)$, yields (8). □

**Proposition 10** *Let $x * y$ denote the product in $B_q(w)$. The triple $(\alpha_1, \alpha_2, \beta)$ defines an isotopy from $B_q(w)$ to $B_q(v)$ if and only if the conditions of Lemma 8 are satisfied, as well as*

$$\phi(v)A_1 B_2^q = (A_2 B_1)^q + (C_2 D_1)^q, \phi(v)A_2 B_1 = A_1^q B_2 + C_1^q D_2 \tag{9}$$

*and*

$$\phi(v^q)wA_2^qB_2 = A_1B_1 + A_2B_2^q + C_1D_1 + C_2D_2^q, \phi(v)\left(A_1B_1 + A_2B_2^q\right)$$
$$= w\left(A_2^qB_2 + C_2^qD_2\right). \qquad (10)$$

*Proof* The condition is

$$(0, b) \circ (0, d) = (bd^q + vb^qd, 0),$$

where $v \notin K$. Equivalently, for $r = bd^q + vb^qd$,

$$\begin{aligned}(\phi(b)C_1, \phi(b)C_2) * (\phi(d^q)D_1, \phi(d)D_2) &= \alpha_1(r, 0) * (B_1, B_2)\\ &= (\phi(r)A_1, \phi(r)A_2) * (B_1, B_2).\end{aligned}$$

The imaginary part is

$$\phi(b^qd)C_1^qD_2 + \phi(bd^q)C_2D_1 = \phi(r^q)A_1^qB_2 + \phi(r)A_2B_1.$$

Comparing coefficients this becomes (9). In the same manner the real part yields (10). □

**Proposition 11** *If $(\alpha_1, \alpha_2, \beta)$ defines an isotopy from $B_q(w)$ to $B_q(v)$ where $w, v \in L \setminus K$ then at least one of the coefficients $A_1, \ldots, D_2$ must vanish. $B_q(w)$ is isotopic to $B_q(v)$ if and only if $v = \phi(w)$ for some field automorphism $\phi$ of $L = \mathbb{F}_{q^2}$.*

*Proof* Note that $1/\tau(w) \in K$ has absolute trace 0; equivalently, $w + w^q = l + 1/l$ for some $l \in K$, and $\{l, 1/l\}$ is uniquely determined by $\tau(w)$. As a consequence $w^{q+1} \neq 1$ as otherwise we would have $w \in \{l, 1/l\} \subset K$. Assume at first all our parameters $A_1, \ldots, D_2$ are nonzero. By (7), both $D_1$ and $D_2$ can be eliminated as

$$D_1 = B_2C_1^q/A_2, \quad D_2 = B_1C_2/A_1^q.$$

Using this in (8) we obtain $(A_1/A_2)(C_1/C_2)^q = w + \frac{A_2B_1^q}{A_1B_2} = w^q + \frac{A_1B_2}{A_2B_1^q}$. As $w + w^q = l + 1/l$ it follows $\frac{A_1B_2}{A_2B_1^q} \in \{l, 1/l\}$, hence $B_2 = l(A_2/A_1)B_1^q$ where $l \in K$ is one of the two values satisfying $l + 1/l = \tau(w)$. This implies $(C_1/C_2)^q = (A_2/A_1)(l + w^q)$, equivalently $C_1 = (l + w)(A_2/A_1)^qC_2$.

Use this in Eq. (9). The first one simplifies to

$$\phi(v) = (A_1B_1)^{q-1}/l + (l + w)(C_2/A_1)^{q+1},$$

whereas the second becomes

$$\phi(v) = l(A_1B_1)^{q-1} + (l + w^q)(C_2/A_1)^{q+1}.$$

This shows $0 = (l + 1/l)((A_1B_1)^{q-1} + (C_2/A_1)^{q+1})$ which implies $(A_1B_1)^{q-1} = (C_2/A_1)^{q+1} = 1$ and $\phi(v) = w^q$. The last equation of (10) simplifies to $(A_2/A_1)^{q+1} = 1/l$, whereas the first yields $w^2 = l(C_1/A_1)^{q+1} + 1$. This gives $w \in K$, which is a contradiction.

Next we consider the case $C_2 = 0$. Then $A_1D_2 = 0$. Assume $A_1 = 0$. Then $B_1 = 0 = D_2$. It follows that if $C_2 = 0$ then $D_2 = 0$. It also follows $A_1 = B_1 = 0$. Only $A_2, B_2, C_1, D_1$ are in play and they satisfy $A_2D_1 = B_2C_1^q$. Only Eq. (10) need to be considered. They read as

$$wA_2^qB_2 + \phi(v)A_2B_2^q = 0, \quad A_2^qB_2 + \phi(v)w^qA_2B_2^q = (C_1D_1)^q.$$

Solving both for $\phi(v)$ and substituting $D_1$ yields the compatibility equation $A_2^{2q}(1 + w^{q+1}) = C_1^{q+1}B_2^{q-1}$; equivalently $B_2^{q-1} = A_2^{q-1}$ and $(C_1/A_2)^{q+1} = 1 + w^{q+1}$. The resulting value is $\phi(v) = w$, so $v$ is obtained by applying Galois isotopy to $w$. We count $\iota(q^2 - 1)^2$ autotopisms (case $v = w$) in this case, where $\iota$ is the order of the stabilizer of $w$ in the Galois group of $L$ : in fact, we have $\iota$ choices for $\phi$, for arbitrary $A_2$, then $q + 1$ choices for $C_1$ and $q - 1$ choices for $B_2$.

Condition $D_2 = 0$ implies $C_2 = 0$, so it can be assumed that $C_2D_2 \neq 0$. We have $A_2 = 0$ if and only if $B_2 = 0$, and this implies $C_1 = D_1 = 0$. Consider this case when $A_1, B_1, C_2, D_2$ are the nonzero parameters. We have $D_2 = B_1C_2/A_1^q$. Aside of that only the last two equations need to be satisfied. The penultimate equation is $A_1B_1 = C_2D_2^q$. This yields $A_1^{2q}B_1^{q-1} = C_2^{q+1}$; equivalently $(A_1B_1)^{q-1} = (C_2/A_1)^{q+1}$. This implies $A_1B_1 \in K$ and $C_2/A_1$ in the non-split torus. The last equation is $\phi(v) = w(C_2/A_1)^{q+1} = w$. In case $v = w$ we obtain the same number of autotopisms as above.

We can assume now that $A_2B_2C_2D_2 \neq 0$. Assume $A_1B_1 = 0$. Then $A_1 = B_1 = 0$ and also $C_1 = D_1 = 0$. Choose $C_2 = wA_2^qD_2/B_2^q$. Then the first equation in (8) is satisfied. The second is satisfied if and only if $w^{q+1} = 1$, a contradiction. Assume $C_1D_1 = 0$ whereas all remaining constants are nonzero. Then we obtain $\phi(v) = w(A_2/B_2)^{q-1}$ and $\phi(v) = (1/w^q)(A_2/B_2)^{q-1}$. This yields $w^q = 1/w$, which is again a contradiction. □

This completes the proof of Theorem 6.

As mentioned earlier, the smallest order of interest is 256. We see that there are precisely 3 isotopy types of semifields $B_4(w)$ where the $w's$ are chosen as representatives of the orbits of the Galois group of $\mathbb{F}_{16}|\mathbb{F}_2$ on elements $w \in \mathbb{F}_{16} \setminus \mathbb{F}_4$. Each of those semifields has 450 autotopisms.

## Comparison

In this subsection we are going to see that the semifields $B_q(w)$ are Knuth equivalent to the semifields of order $q^4$ in characteristic 2 which are quadratic over their middle nucleus, quartic over their center and not generalized twisted fields or Hughes–Kleinfeld semifields. In fact, it has been shown in [8] that the semifields of order $q^4$ in characteristic 2 which are quadratic over the left nucleus, quartic over the center and neither generalized twisted fields nor Hughes–Kleinfeld semifields are precisely those which can be described up to isotopy by a product

$$x * y = (ac + ubd + wbd^q, ad + bc^q), \tag{11}$$

where $u, w \in L^*$ satisfy a certain polynomial condition. We are going to see that this semifield is Knuth equivalent to a semifield $B_q(v)$. Observe at first that the substitution $b \mapsto \lambda b, d \mapsto \lambda d$ shows that we can assume $u = 1$. We start from Eq. (11) with $u = 1$. The opposite is obtained by $x \leftrightarrow y$. This is the multiplication

$$(ac + bd + wb^q d, a^q d + bc).$$

Next we apply the transpose operation (see [12]). In order to do this represent the symplectic form on $F^2 = L^4$ by

$$\langle (u_1, u_2, u_3, u_4), (v_1, v_2, v_3, v_4) \rangle = tr(u_1 v_3 + u_2 v_4 - u_3 v_1 - u_4 v_2),$$

where $tr : L \longrightarrow \mathbb{F}_p$ is the absolute trace on $L$. The spread space corresponding to the pair $(c, d)$ is $V_{c,d} = \{(a, b, ac + bd + wb^q d, a^q d + bc) \mid a, b \in L\}$. When is $(u, v, U, V)$ in the dual of $V_{c,d}$ with respect to the symplectic form? Using basic properties of the trace shows that this is equivalent to $U = uc + (vd)^q$, $V = ud + w^q u^q d^q + vc$. Choosing $u = a, v = b$ this yields the multiplication in the transpose in the form

$$(ac + (bd)^q, ad + w^q (ad)^q + bc). \tag{12}$$

We claim that this is isotopic to $B_q(w)$. Let $f(x) = x + w^q x^q$. Then $f^{-1}(x) = \kappa f(x)$ where $\kappa = 1/(1 + w^{q+1}) \in K$. Start from Eq. (12), let the new imaginary part be the old real part and let the new real part be the image of the old imaginary part under $f^{-1}$. This yields the product $(ad + \kappa(bc + w^q (bc)^q), ac + (bd)^q)$. Apply the substitution $c \mapsto d^q$, $d \mapsto c$ followed by applying $x \mapsto x^q$ to the imaginary part. This yields the product $(ac + \kappa(bd^q + w^q b^q d), a^q d + bc)$. Clearly we can choose $\kappa = 1$ and obtain the multiplication in $B_q(w^q)$ which as we know is isotopic to $B_q(w)$.

Observe that in this section we obtained a complete taxonomy of the semifields of order $q^4$ in characteristic 2 which are quadratic over the middle nucleus and quartic over left and right nuclei.

## 9 Non-commutativity

We use a generalization of the Ganley criterion, Corollary 2 of [4]. It says that $(F, \circ)$ is isotopic to a commutative semifield if and only if there is some $v \in F^*$ such that $\alpha(v \circ x) \circ y$ is invariant under the substitution $x \leftrightarrow y$ for all $x, y$. Here $\alpha(x)$ is defined by $\alpha(x) \circ 1 = x$ for all $x$. Let $v = (v_1, v_2)$.

**Theorem 7** *$B(2, m, s, l, t)$ for $s > 0$ is not isotopic to a commutative semifield.*

*Proof* We may assume $l \neq 0$. Let at first $m/\gcd(m, s)$ be even. It can be assumed that $\sigma^2$ is not the identity on $L$. We have $Im(\alpha(v \circ x)) = Im(v \circ x) = v_1 b + v_2 a$. Considering the imaginary part of the equation we obtain

$$Re(\alpha(v \circ x))d + (v_1 b + v_2 a)c = Re(\alpha(v \circ y))b + (v_1 d + v_2 c)a.$$

This shows $Re(\alpha(v \circ y)) = v_3 c + v_4 d$ for some $v_3, v_4 \in L$ and $v_3 = v_1$. Now compare the real parts. They yield eight equations. Four of them simply say $v_3 = v_1 = 0$. Two of the remaining four equations are redundant. The remaining conditions are $v_4 = l p_4 v_2^\sigma$ (the coefficient of $bc^\sigma$) and $p_4 v_2 = l v_4^\sigma$ (the coefficient of $ad^\sigma$). If $v_4 = 0$, then $v_2 = 0$, which is a contradiction. Assume $v_4 \neq 0$. Then $v_4^{\sigma^2-1} l^{\sigma+1} = v_4^{\sigma-1}$. This implies $l^{\sigma+1} \in (L^*)^{\sigma-1}$, which implies $l^2 \in (L^*)^{\sigma-1}$ and finally the contradiction $l \in (L^*)^{\sigma-1}$

Let now $m/\gcd(m, s)$ be odd. We may assume $p_1 = p_3 = 1$, $p_2 = 0$. The same procedure as above shows $\alpha(v \circ x) = (v_1 a + v_4 b, v_1 b + v_2 a)$. Comparison of the real parts yields eight equations as before. Five of those are redundant. The remaining ones are the following: the coefficient of $ac^\sigma$ yields $v_1 = l v_1^\sigma + l v_2^\sigma$, $bc^\sigma$ yields $v_4 = l p_4 v_2^\sigma$ and $b^\sigma c$ yields $l v_4^\sigma + l v_1^\sigma = v_1 + p_4 v_2$. Use the second equation to eliminate $v_4$, and then consider $w = v_1 + l v_1^\sigma$ instead of $v_1$. The remaining equations are $w = l v_2^\sigma = l v_4^\sigma + p_4 v_2$, $v_4 = l p_4 v_2^\sigma$. After division by the leading term this yields $X^{\sigma^2} + BX^\sigma + CX = 0$, where $B = 1/(l p_4)^\sigma$, $C = 1/(l^{\sigma+1} p_4^{\sigma-1})$. If our presemifield is isotopic to a commutative semifield, then this equation has a nonzero root $x \in L$. Let $y = x^{\sigma-1}$. Then $y^{\sigma+1} + By + C = 0$. A standard substitution shows that this is equivalent to $y^{\sigma+1} + b(y + 1) = 0$, where $b = B^{\sigma+1}/C^\sigma = 1/p_4^{2\sigma}$. On the other hand the condition from Definition 1 says that $X^{\sigma+1} + X + p_4$ has no root in $L$. This is equivalent to $X^{\sigma+1} + (1/p_4)(X + 1)$ having no root, which contradicts the condition that we just obtained. □

## 10 The nuclei

**Theorem 8** *Let* $0 < s < m, l \neq 0$. *Then* $K_1$ *is the center, the right and the left nuclei of the semifield associated to* $B(2, m, s, l, t), l \neq 0$.

*Proof* We know that $K_1$ is in the center. Then it will be enough to prove that the left and right nuclei have at most $2^{\gcd(m,s)}$ elements. It can be assumed that $s \leq m/2$. The case $s = m/2$ has been handled in Sect. 8, so we may actually assume $0 < s < m/2$. By Proposition 2 it is enough to consider the right nucleus. We work with the multiplication $x * y = x \circ \overline{y}$ of Eq. (6) which we write in polynomial form as $x * y = \sum_{k \in E} c_k(y) x^{2^k}$ where $E = \{0, m, s, m + s\}$ and

$$\begin{aligned} c_0(y) &= C_1 y^\sigma + C_2 \overline{y}^\sigma + yz, \\ c_m(y) &= \overline{C_2} y^\sigma + \overline{C_1}\,\overline{y}^\sigma + \overline{y} z \\ c_s(y) &= l(\overline{C_1} y + C_2 \overline{y}), c_{m+s}(y) = \overline{c_s(y)}. \end{aligned}$$

In particular $y$ is recovered from $y = c_0(y) + \overline{c_m(y)}$.

The right nucleus is in bijection with the invertible linear mappings $V(x) = \sum_{i=0}^{2m-1} a_i x^{2^i}$, where $a_i \in F$ such that for each $y \in F$ there exists $u = u(y) \in F$ satisfying $V(x * y) = x * u$ (see [4], Theorem 3). In coordinates this means

$$\sum_{i=0}^{2m-1} a_i \left( \sum_{k \in E} c_k(y) x^{2^k} \right)^{2^i} = \sum_{k \in E} c_k(u) x^{2^k} \tag{13}$$

Let $j \notin E$. The coefficient of $x^{2^j}$ in (13) shows

$$a_j c_0(y)^{2^j} + a_{j+m} \overline{c_m(y)}^{2^j} + (a_{j-s} + a_{j-s+m}) c_s(y)^{2^{j-s}} = 0. \tag{14}$$

This is a polynomial equation in $y$. The coefficient in $y^{2^{s+j}}$ shows $(a_j + a_{j+m}) C_1^{2^j} = 0$. The coefficient of $y^{2^{s+m+j}}$ shows $(a_j + a_{j+m}) C_2^{2^j} = 0$. As $C_1, C_2$ do not both vanish it follows $a_{j+m} = a_j$. Use this and $c_0(y) + \overline{c_m(y)} = y$ in (14):

$$a_j y^{2^j} + (a_{j-s} + a_{j-s+m}) c_s(y)^{2^{j-s}} = 0.$$

This shows $a_j = a_{j+m} = a_{j-s} + a_{j-s+m} = 0$. In particular $a_j \neq 0$ only if $j \in E$.

We have $a_s + a_{s+m} = 0$, hence $V(x) = a_0 x + a_m \overline{x} + a_s (x^\sigma + \overline{x}^\sigma)$. Comparing coefficients of $x^\sigma$ and $\overline{x}^\sigma$ in (13) shows $a_0 + a_m \in L, a_s \in L$. It follows $u = c_0(u) + \overline{c_m(u)} = \lambda y$, where $\lambda = a_0 + \overline{a_m} \in L$. It follows $a_s = 0$. The formula for $c_s(u)$ shows that $a_m, a_0 \in L$. The formula for $c_0(u)$ shows $\lambda = \lambda^\sigma$ and finally $a_m = 0, a_0 \in L$. □

**Theorem 9** *The middle nucleus of the semifield associated to $B(2, m, s, l, t), s > 0, l \neq 0$ is a quadratic extension of the center.*

*Proof* Let at first $m/\gcd(m, s)$ be even. We know that we can assume $p_1 = 1, p_2 = p_3 = 0$ in this case and have $x \circ y = (ac^\sigma + la^\sigma c + p_4 bd^\sigma + lp_4 b^\sigma d, ad + bc)$. It can be assumed that $\sigma^2$ is not the identity on $L$, the case $s = m/2$ having been handled in Sect. 8. The condition to determine the middle nucleus is $V(x) \circ y = x \circ z$ where $z = z(y)$ (see [4], Theorem 2). An obvious polynomial argument shows that $V(x)$ has the form $V(a, b) = (Aa + Bb, Ca + Db)$, and $z = (Ec + Fd, Gc + Hd)$. Comparison of the imaginary parts shows $E = D, F = B, G = C, H = A$, hence $z = (Dc + Bd, Cc + Ad)$. Compare the real parts. The coefficients of $ac^\sigma, bc^\sigma, a^\sigma c, b^\sigma c, ad^\sigma, bd^\sigma, a^\sigma d, b^\sigma d$ yield eight equations for the unknowns $A, B, C, D \in L$. The latter four are redundant, the first four are $A = D^\sigma, B = p_4 C^\sigma, A^\sigma = D, B^\sigma = p_4 C$. Assume $B \neq 0$. Then $B^{\sigma^2 - 1} = p_4^{\sigma - 1}$, hence $p_4 / B^{\sigma+1} \in K_1$. This shows that $p_4 \in (L^*)^{\sigma+1}$, contradicting the existence condition of $p_4$. It follows $B = C = 0$ and $A \in K_2$, the fixed field of $\sigma^2$, $D = A^\sigma$. The solutions are $V(a, b) = (Aa, A^\sigma b)$, where $A \in K_2$.

Let now $m/\gcd(m, s)$ be odd. It can be assumed that $p_1 = 1, p_2 = 0, p_3 = 1$. Our presemifield product is $x \circ y = (ac^\sigma + la^\sigma c + ad^\sigma + lb^\sigma c + p_4 bd^\sigma + lp_4 b^\sigma d, ad + bc)$. As before we have $V(a, b) = (Aa + Bb, Ca + Db), z = (Dc + Bd, Cc + Ad)$ and the condition is $V(x) \circ y = x \circ z$. Compare the real parts. As before eight equations arise, the latter half of which are redundant. The other four are

$$A = D^{\sigma} + C^{\sigma}, B = p_4 C^{\sigma}, A^{\sigma} + C^{\sigma} = D, B^{\sigma} + D^{\sigma} = D + p_4 C.$$

Use the first two to eliminate $A, B$. This shows that the middle nucleus is in bijection with the space of $(C, D) \in L^2$ satisfying

$$C^{\sigma} + C^{\sigma^2} = D + D^{\sigma^2}, \quad p_4 C + p_4^{\sigma} C^{\sigma^2} = D + D^{\sigma}. \tag{15}$$

Combining those two equations yields $C^{\sigma} + C^{\sigma^2} + (p_4 C)^{\sigma} + p_4^{\sigma^2} C^{\sigma^3} = p_4 C + p_4^{\sigma} C^{\sigma^2}$; equivalently $f(C) = p_4^{\sigma} C^{\sigma^2} + C^{\sigma} + p_4 C = \lambda \in K_1$. Assume that $f(X)$ is not invertible. The substitution $X \mapsto X/p_4$ shows that $X^{\sigma+1} + X + p_4^2$ has a root in $L$. This contradicts the existence condition for $p_4$. Let now $\lambda \in K_1$ be given and $C \in L$ the unique element such that $f(C) = \lambda$. The sum of Eq. (15) is $\lambda + C^{\sigma^2} = D^{\sigma} + D^{\sigma^2}$; equivalently, $D + D^{\sigma} = \lambda + C^{\sigma}$. In order to obtain solutions $(C, D)$ it must be the case that $Tr(\lambda + C^{\sigma}) = 0$ where $Tr$ is the trace : $L \longrightarrow K_1$. As $Tr(\lambda) = \lambda$ we must show $Tr(C) = \lambda$. Clearly we are done when this has been proved. We apply the method used in [10]. In fact,

$$Tr(C)^2 = Tr(C^{\sigma+\sigma}) = Tr(C^{\sigma}(p_4^{\sigma} C^{\sigma^2} + p_4 C + \lambda)) = Tr(\lambda C^{\sigma}) = \lambda Tr(C).$$

This shows $Tr(C) \in \{0, \lambda\}$. Assume $Tr(C) = 0$. Then $C = u + u^{\sigma}$ for some $u \in L$. It follows $\lambda = f(C) = f(u) + f(u^{\sigma})$. Applying this twice shows $f(u^{\sigma^2}) = f(u)$. As $\sigma$ has odd order $2n + 1$ this yields $f(u^{\sigma^{2k}}) = f(u)$ and finally the contradiction $f(u) = f(u^{\sigma^{2k+1}}) = f(u) + \lambda$. □

## 11 Conclusion

We start from a relation between projective polynomials over finite fields and Knuth semifields which we use for the construction of a new family of semifields in characteristic 2. Those semifields are never isotopic to commutative semifields. We determine their nuclei. A parametric special case are the characteristic 2 semifields of order $q^4$ with middle nucleus of order $q^2$ and center of order $q$ which are different from the twisted fields and from the Hughes–Kleinfeld semifields. In this case we obtain a complete taxonomy. This includes the determination of the group of autotopisms.

## References

1. Albert, A.A.: Finite division algebras and finite planes. In: Proceedings of Symposia in Applied Mathematics (AMS), vol.10, pp. 53–70 (1960)
2. Albert, A.A.: Generalized twisted fields. Pac. J. Math. **11**, 1–8 (1961)
3. Bierbrauer, J.: Commutative semifields from projection mappings. Des. Codes Cryptogr. **61**, 187–196 (2011)

4. Bierbrauer, J.: Projective polynomials, a projection construction and a family of semifields. Des. Codes Cryptogr. **79**, 183–200 (2016)
5. Bierbrauer, J., Bartoli, D., Giulietti, M., Marcugini, S., Pambianco, F.: A projection construction for semifields and APN functions in characteristic 2. In: Proceedings of ACCT, pp. 46–50 (2014)
6. Bluher, A.W.: On $x^{q+1} + ax + b$. Finite Fields Appl. **10**, 285–305 (2004)
7. Budaghyan, L., Helleseth, T.: New commutative semifields defined by new PN multinomials. Cryptogr. Commun. **3**, 1–16 (2011)
8. Cardinali, I., Polverino, O., Trombetti, R.: Semifield planes of order $q^4$ with kernel $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$. Eur. J. Comb. **27**, 940–961 (2006)
9. Ganley, M.J.: Polarities in translation planes. Geom. Dedicata **1**, 103–116 (1972)
10. Helleseth, T., Kholosha, A.: $x^{2^l+1} + x + a$ and related affine polynomials over $GF(2^k)$. Cryptogr. Commun. **2**, 85–109 (2010)
11. Hughes, D.R., Kleinfeld, E.: Seminuclear extensions of Galois fields. Am. J. Math. **82**, 389–392 (1960)
12. Knuth, D.E.: Finite semifields and projective planes. J. Algebra **2**, 182–217 (1965)