Des. Codes Cryptogr. (2018) 86:611–621
https://doi.org/10.1007/s10623-017-0345-5

A family of semifields in odd characteristic

Jürgen Bierbrauer[1] · Daniele Bartoli[2] · Giorgio Faina[2] · Stefano Marcugini[2] · Fernanda Pambianco[2]

Received: 28 July 2016 / Revised: 22 December 2016 / Accepted: 14 February 2017 /
Published online: 1 March 2017

Abstract We study a large family of semifields in odd characteristic, which contains the commutative Budaghyan–Helleseth semifields as well as semifields which are not isotopic to commutative semifields. Using a large group of autotopisms we obtain a complete classification result in certain parametric subcases.

Keywords Semifields · Knuth semifields · Isotopy · Budaghyan–Helleseth semifields · Projective polynomials · Nuclei

Mathematics Subject Classification 12K10 · 51E15 · 51A40

1 Introduction

A family of presemifields $B(p, m, s, l, t)$ of order p^{2m} where p is an odd prime and $m \geq 3$ was studied in [1]. The main ingredient is a Galois automorphism $x \mapsto x^\sigma$ of $\mathbb{F}_{p^{2m}}$ where $\sigma = p^s$. The remaining parameters are an element $l \in (\mathbb{F}_{p^m})^*$ and a quadruple $t = [p_1, p_2, p_3, p_4]$ where $p_i \in \mathbb{F}_{p^m}$. The family contains the Budaghyan–Helleseth commutative semifields. The special case of order $729 = 3^6$ is studied in [2].

In the present paper we introduce a new type of isotopism (linear isotopy, Proposition 3) relating those presemifields. This leads to a group $GL(2, p^m) \times (\mathbb{F}_{p^m})^*$ (the restricted isotopy group of Sect. 5) acting on the quadruples t such that quadruples in the same orbit yield isotopic presemifields $B(p, m, s, l, t)$ (given p, m, s, l). We then specialize to the ternary case and prove that in each of the cases $p = 3, s = 1, m \geq 3$ and $p = 3, s = 2, m \geq 3$

Communicated by M. Lavrauw.

✉ Jürgen Bierbrauer
jbierbra@mtu.edu

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

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

odd there are precisely two isotopy types in the family, the uniquely determined Budaghyan–Helleseth semifield and another presemifield which is not isotopic to a commutative semifield. The characteristic 2 case has been studied in [3]. Here the situation is different. In fact it can be proved that none of those characteristic 2 semifields is isotopic to a commutative semifield.

The paper is organized as follows: In Sects. 2 and 3 we introduce basic terminology and sketch the relationship between Knuth semifields and the theory of projective polynomials over finite fields in odd characteristic. Given p, m, s, l the definition of a legitimate quadruple t in Definition 1 is in terms of projective polynomials. We show that t is legitimate if and only if $B(p, m, s, l, t)$ is a presemifield. A simple formula for the number of legitimate polynomials is derived in Theorem 3. Isotopies, in particular linear isotopies, are studied in Sect. 4. This leads to the definition of the restricted isotopy group and its action on the space Ω of legitimate quadruples in Sect. 5. The C-family of presemifields, defined by $p_2 = p_3 = 0$, is studied in Sect. 6. We determine the orbits of the restricted isotopy group on quadruples in the C-family and prove in Theorem 5 that in case $m/\gcd(m, s)$ even, each presemifield $B(p, m, s, l, t)$ is isotopic to a presemifield in the C-family. The nuclei and commutativity are considered in Sect. 7. Our semifields have order p^{2m}. In case $m = 2$ the middle nucleus has order p^2, see Sect. 7. The semifields of order p^4 one of whose nuclei has order p^2 have been classified in [5]. It follows that p^6 (case $m = 3$) is the smallest order of a member of our family which is potentially of independent interest. The final Sect. 8 contains the promised classification results in cases $p = 3, s = 1$ and $p = 3, s = 2$.

2 Projective polynomials and semifields

We use the following terminology. Let $q = p^m$ an odd prime power, $F = GF(q^2) \supset L = GF(q)$. Let $T : F \longrightarrow L$ be the trace. Choose $\omega \in F^*$ such that $T(\omega) = \omega + \omega^q = 0$ and write $x \in F$ in the form $x = (a, b) = a + b\omega$ where $a, b \in L$. The conjugate of x is $\overline{x} = x^q = (a, -b)$. Let $0 \leq s < 2m$ and $\sigma = p^s$. With the symbol σ we also denote the corresponding automorphism of F. Also, let $\mu = \omega^2$ (a non-square in L) and $N = \mu^{(\sigma-1)/2}$. Our basic definition is the following.

Definition 1 The quadruple $t = [p_1, p_2, p_3, p_4] \in L^4$ is **legitimate** if $p_1 \neq 0$ and the polynomial $p_{s,t}(X) = p_1X^{\sigma+1} + p_2X^\sigma + p_3X + p_4$ has no roots in L. Let $\Omega = \Omega(p, m, s)$ be the set of legitimate quadruples. Let further $l \in L$ be such that either $l = 0$ or $-l \in L^* \setminus (L^*)^{\sigma-1}$. The presemifield (of order p^{2m}) defined by

$$\begin{aligned} x * y = (&-p_1ac^\sigma - lp_1a^\sigma c + p_2bc^\sigma - lp_2a^\sigma d - p_3ad^\sigma \\ &+lp_3b^\sigma c + p_4bd^\sigma + lp_4b^\sigma d, ad + bc) \end{aligned} \tag{1}$$

will be denoted by $B(p, m, s, l, t)$.

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

Proof As $x * y$ is $\mathbb{F}_p$-linear in both arguments, it suffices to prove that there are no divisors of zero. Assume therefore $x * y = 0, xy \neq 0$. Use Eq. (1). If $d = 0$, then $b = 0$ and the real part shows $p_1ac = 0$, contradiction. By homogeneity it can be assumed $d = 1$, hence $a = -bc$. The real part is then $(b + lb^\sigma)p_{s,t}(c) = 0$. The first factor is nonzero by the basic assumption on l, the second factor is nonzero by definition of legitimacy. □

In order to obtain an expression of $x * y$ 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

$$p_1 = -v_+, p_2 = \mu h_+, p_3 = -\mu N h_-, p_4 = \mu N v_-,$$

where $v_- = v_1 - v_2, v_+ = v_1 + v_2, h_- = h_1 - h_2, h_+ = h_1 + h_2$. The pair (C_1, C_2) is legitimate if and only if its corresponding quadruple is legitimate.

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

$$x * y = (1/2)T((C_1 y^\sigma + C_2 \overline{y}^\sigma)x) + (l/2)T((\overline{C_1} y + C_2 \overline{y})x^\sigma) + (xy - \overline{xy})/2. \quad (2)$$

Proof This is a direct calculation. □

If σ is the identity on L, then $(kx) * y = x * (ky) = k(x * y)$ holds for all $k \in L$ and all $x, y \in F$. This implies that a semifield isotopic to $(F, *)$ has center of order at least p^m (see [1, Proposition 3]). It follows from [6], Theorem 2 that the semifield is a field. It can therefore be assumed in the sequel that $s \neq 0, m$.

Observe a slight change in terminology in comparison with [1]. The presemifields $B(p, m, s, l, t(C_1, C_2))$ were called $B(p, m, s, l, C_1, C_2)$ in [1]. It was proved in Sect. 8 of [1] that they are indeed presemifields.

3 The associated product

Case $l = 0$ of Definition 1 yields a relation between projective polynomials and non-associative algebras.

Definition 3 Let $C_1 = (v_1, h_1), C_2 = (v_2, h_2) \in F = GF(q^2)$, q odd prime power, and $\sigma = p^s, 0 \leq s < 2m$, an automorphism of F. Let $t = t(C_1, C_2) = [p_1, p_2, p_3, p_4]$. Consider the projective polynomials

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

as well as the multiplication

$$x * y = (1/2)T((C_1 y^\sigma + C_2 \overline{y}^\sigma)x) + (xy - \overline{xy})/2 \quad (4)$$

on F. Call $*$ the **multiplication associated** to (C_1, C_2, s).

Comparison with (2) shows in fact that $x * y$ in Definition 3 is precisely the multiplication in $B(p, m, s, 0, t)$. The main results in Sect. 7 of [1] are as follows.

Theorem 2 *Let C_1, C_2, s be as in Definition 3. Then the following are equivalent:*

- *$(F, *)$ is a presemifield (of order q^2 where $L = GF(q)$).*
- *$T(C_1 x \overline{x}^\sigma + C_2 x^{\sigma+1}) \neq 0$ for all $0 \neq x \in F$.*
- *$P_{C_1,C_2,s}(X)$ has no root $z \in F$ such that $z\overline{z} = 1$.*
- *$p_1 \neq 0$ and $p_{s,t}(X)$ (see Definition 1) has no root in L.*

Definition 4 Given p, m, s let $g = \gcd(q - 1, \sigma + 1)$, the number of cosets of $(L^*)^{\sigma+1}$ in L^*.

Observe that $g = 2$ if $m/\gcd(m, s)$ is odd whereas $g = p^{\gcd(m,s)} + 1$ if $m/\gcd(m, s)$ is even.
If the conditions of Theorem 2 are satisfied, then $p_1 \neq 0$ and $C_1^{q+1} \neq C_2^{q+1}$. Comparison with Definition 1 shows that the conditions of Theorem 2 are equivalent to the pair (C_1, C_2) and the corresponding quadruple being legitimate. The presemifields $B(p, m, s, 0, t)$ are isotopic to the Knuth semifields which are quadratic over the left and over the right nucleus (see [1]). In the sequel we will always assume $l \neq 0$. It is important to have a simple expression for the number of legitimate quadruples. Here is a first step in this direction.

Corollary 1 *For given p, m, s the number of legitimate pairs (C_1, C_2) is $|\Omega_{p,m,s}| = (q - 1)q\{(q - 1)(N_0 + 1) - (q - 1)/\gcd(q - 1, \sigma + 1)\}$. Here N_0 is the number of values $B \in L$ such that the polynomial $Y^{\sigma+1} - B(Y - 1)$ has no roots in L.*

Proof The shape of $p_{s,t}(X)$ shows that the number in question is the number of a, b, c, d such that $a \neq 0$ and $aX^{\sigma+1} + bX^{\sigma} + cX + d \in L[X]$ has no roots in L. We can assume $a = 1$ and obtain a factor of $q - 1$. The substitution $Y = X + b$ leads to the equivalent polynomial $Y^{\sigma+1} + (c - b^{\sigma})Y + d - bc$. Clearly $d \neq bc$. Assume $c = b^{\sigma}$. Then $bc - d$ must be outside the $(\sigma + 1)$-st powers. This yields a contribution of $q(q - 1 - (q - 1)/\gcd(q - 1, \sigma + 1))$; since b is arbitrary, c is then uniquely determined, and finally d such that $bc - d$ is as required.

Assume now $c \neq b^{\sigma}$. Use the substitution $Y \mapsto rY$, followed by division by $r^{\sigma+1}$ for some $r \in \mathbb{F}_q^*$. This produces the equivalent polynomial $Y^{\sigma+1} + (c - b^{\sigma})/r^{\sigma} Y + (d - bc)/r^{\sigma+1}$. Choose $r = (bc - d)/(c - b^{\sigma})$. The polynomial has the form $Y^{\sigma+1} - B(Y - 1)$ where $B = (b^{\sigma} - c)/r^{\sigma}$. We know that there are N_0 values of B such that the condition is satisfied. This yields a contribution of $q(q - 1)N_0$, since b is arbitrary, $c \neq b^{\sigma}$, and for each of the N_0 choices of B then $r^{\sigma} = (b^{\sigma} - c)/B$ and $d = r(b^{\sigma} - c) + bc$. □

Here is the final result:

Theorem 3 *We have $|\Omega| = (q + 1)q(q - 1)^2 p^d/\{2(p^d + 1)\}$. Here $d = \gcd(m, s)$.*

Proof Observe that $|\Omega|$ is the number of different presemifields in the B-family for given p, m, s, l. This number is given in Corollary 1 in terms of the numbers N_0. The numbers N_0 are determined in Bluher [4]. We distinguish two cases (recall that p is odd): if m/d is even, then $g = \gcd(q - 1, \sigma + 1) = p^d + 1$, $N_0 = p^d(q - 1)/(2(p^d + 1))$; if m/d is odd, then $\gcd(q - 1, \sigma + 1) = 2$, $N_0 = (p^{m+d} - 1)/(2(p^d + 1))$. In both cases the same formula for $|\Omega|$ results. □

A special case arises if C_1 or C_2 vanishes. If $C_2 = 0$, then the condition is $z^{\sigma-1} \neq -C_1/\overline{C_1}$ for $z\bar{z} = 1$ and for $C_1 = 0$ the condition reads $z^{\sigma+1} \neq -\overline{C_2}/C_2$ for $z\bar{z} = 1$.

4 Isotopies

We consider isotopies between the presemifields $B(p, m, s, l, t)$ in this section, in odd characteristic p. It was proved in [1] that the opposite of the presemifield $B(p, m, s, l, t(C_1, C_2))$, $l \neq 0$ is isotopic to the presemifield $B(p, m, s, 1/l, t(\overline{C_1}, \overline{C_2}))$. Here the opposite of a presemifield $(F, *)$ is the presemifield $(F, \circ)$ where $x \circ y = y * x$. The obvious isotopy of the presemifields $B(p, m, s, l, t(C_1, C_2))$ and $B(p, m, m + s, l, t(C_2, C_1))$ allows us to assume $s \leq m$.

Recall that if $s = 0$ or $s = m$, the general form of the multiplication shows that L is in the center of the associated semifield. This semifield is therefore a field. It follows that we may

assume $0 < s < m$. It was shown in [1] that the presemifield $B(p, m, s, l, [p_1, p_2, p_3, p_4])$, $l \neq 0$, $s \leq m$, is isotopic to the presemifield $B(p, m, m-s, 1/l, [p_1, p_3, p_2, p_4])$. This allows us to assume $0 \leq s \leq m/2$. The following elementary isotopy relations are from [1] as well.

Proposition 2
- *The presemifield $B(p, m, s, l, t)$ is isotopic to the presemifield $B(p, m, s, \lambda^{\sigma-1} l, t)$ for arbitrary $\lambda \in L^*$.*
- **scalar isotopy** *The presemifield $B(p, m, s, l, t)$ is isotopic to the presemifield $B(p, m, s, l, \lambda t)$ for arbitrary $\lambda \in L^*$.*
- **Galois isotopy** *The presemifield $B(p, m, s, l, [p_1, p_2, p_3, p_4])$ is isotopic to the presemifield $B(p, m, s, l^p, [p_1^p, p_2^p, p_3^p, p_4^p])$.*
- **Diagonal isotopy** *The presemifield $B(p, m, s, l, [p_1, p_2, p_3, p_4])$ is isotopic to the presemifield $B(p, m, s, l, [k_1^{\sigma+1} p_1, k_1^{\sigma} k_2 p_2, k_1 k_2^{\sigma} p_3, k_2^{\sigma+1} p_4])$ for arbitrary $k_1, k_2 \in L^*$.*

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 to a, b, c, d, then apply the Frobenius to the real and to the imaginary part. Diagonal isotopy follows from the substitution $a \mapsto k_1 a, b \mapsto k_2 b, c \mapsto k_1 c, d \mapsto k_2 d$. □

The following important isotopy relation is new:

Proposition 3 (Linear isotopy) *$B(p, m, s, l, [p_1, p_2, p_3, p_4])$ is isotopic to $B(p, m, s, l, [p'_1, p'_2, p'_3, p'_4])$ 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 substitution $a' = \alpha a + \beta b$, $b' = \gamma a + \delta b$, $c' = -\alpha c + \beta d$, $d' = \gamma c - \delta d$ where $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL(2, L)$. □

Corollary 2 *$B(p, m, s, l, [p_1, p_2, p_3, p_4])$ is isotopic to $B(p, m, s, l, [1, 0, u, v])$ 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 $\alpha = 1, \gamma = 0$ 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. □

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

Proof Use the substitution $x \mapsto \alpha x$, $y \mapsto \overline{\alpha} y$ for an arbitrary nonzero $\alpha \in F$. □

Theorem 4 is a special case of linear isotopy, written with different terminology.

5 The restricted isotopy group

Definition 5 Given p, m, 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 by linear isotopy and scalar isotopy, respectively.

The formulas show in fact that $GL(2, L)$ and L^* form a direct product. We have $|G_1| = (q-1)(q^2-1)(q^2-q)$ where $q = p^m$. The important point is that the elements of G_1 permute the legitimate pairs and quadruples and that pairs or quadruples in the same orbit describe isotopic presemifields. In case $l = 1$ we can work with a larger group, the semidirect product $G_0 = G_1 \rtimes \langle\phi\rangle$ of G_1 and the group of Galois isotopisms.

6 The C-family

We refer to the semifields isotopic to the presemifields $B(p, m, s, l, [1, 0, 0, p_4])$, $l \neq 0$, as the C-family of semifields. Observe that $p_2 = p_3 = 0$ is equivalent to $\{C_1, C_2\} \subset L$. We will use the following terminology:

Definition 6 Let $C(p, m, s, l, R), l \neq 0$ be the semifield associated to the presemifield

$$(a, b) * (c, d) = ([ac^\sigma + Rbd^\sigma] + l[a^\sigma c + Rb^\sigma d], ad + bc)$$

where $-l \notin (L^*)^{\sigma-1}$, $R \notin (L^*)^{\sigma+1}$.

In fact, the substitution $a \mapsto -a, b \mapsto -b$ shows that the semifield $C(p, m, s, l, R)$ is isotopic to the presemifield $B(p, m, s, l, [1, 0, 0, p_4])$ where $R = -p_4$. Proposition 2 shows that l may be replaced by an arbitrary element of its coset mod $(L^*)^{\sigma-1}$ and R may be replaced by an arbitrary element of its coset mod $(L^*)^{\sigma+1}$ without changing isotopy. The quadruple $[1, 0, 0, u]$ is legitimate if $R = -u \notin (L^*)^{\sigma+1}$ (see Definition 1).

Lemma 1 *Given $p, m, s, l \neq 0$, we have that $[1, 0, 0, u_1]$ and $[1, 0, 0, u_2]$ are in the same orbit under G_1 if and only if $R_i = -u_i$ satisfy the following: either $R_2 \in R_1(L^*)^{\sigma+1}$ or $R_2 \in (1/R_1)(L^*)^{\sigma+1}$.*

Proof Let $d = \gcd(m, s)$ and $g = \gcd(q-1, \sigma+1)$ (see Definition 4). A trivial case occurs if m/d is odd. Then $g = 2$ and $R(L^*)^{\sigma+1}$ is the coset of non-squares. Assume therefore m/d even. We have $g = p^d + 1$ in this case and $K_1 = \mathbb{F}_{p^d} \subseteq (L^*)^{\sigma+1}$. Let the matrix M map $[1 : 0 : 0 : u_1] \mapsto [1 : 0 : 0 : u_2]$. We have three conditions:

$$\alpha\beta^\sigma = R_1\gamma\delta^\sigma, \quad \alpha^\sigma\beta = R_1\gamma^\sigma\delta, \quad R_1\gamma^{\sigma+1} - \alpha^{\sigma+1} = (R_1/R_2)(\beta^{\sigma+1}/R_1 - \delta^{\sigma+1}).$$

We have $\beta = 0$ if and only if $\gamma = 0$ which leads to R_2 and R_1 in the same coset. Also $\alpha = 0$ if and only if $\delta = 0$ and this leads to R_2 in the same coset as $1/R_1$. Assume all entries of M are nonzero. By homogeneity it can be assumed that $\beta = 1$. The first two equations show $\alpha = R_1\gamma\delta^\sigma, \alpha^\sigma = R_1\gamma^\sigma\delta$. Comparison shows $c = R_1\delta^{\sigma+1} \in K_1$. This yields the contradiction $R_1 \in (L^*)^{\sigma+1}$. □

Theorem 5 *Let $p, m, s, l \neq 0$ be given, $d = \gcd(m, s)$. If m/d is odd, then there is precisely one G_1-orbit of legitimate quadruples in the C-family. Its length is $|\Omega|/p^d$.*
If m/d is even, all the presemifields $B(p, m, s, l, t)$ belong to the C-family. There are $(p^d + 1)/2$ orbits under G_1. One of those orbits has length $(1/p^d)|\Omega|$, each of the remaining $(p^d - 1)/2$ orbits has length $(2/p^d)|\Omega|$.

Proof The stabilizer of $[1, 0, 0, u]$ in G_1 is described by

$$\alpha\beta^\sigma = R\gamma\delta^\sigma, \quad \alpha^\sigma\beta = R\gamma^\sigma\delta, \quad \alpha^{\sigma+1} + \beta^{\sigma+1}/R = R\gamma^{\sigma+1} + \delta^{\sigma+1}.$$

Let $g = \gcd(q-1, \sigma+1)$. We have $\beta = 0$ if and only if $\gamma = 0$, condition $(\alpha/\delta)^{\sigma+1} = 1$. This yields the first contribution of $g(q-1)$ to the order of the stabilizer. Also $\alpha = 0$ if and only if $\delta = 0$, with condition $(\beta/\gamma)^{\sigma+1} = R^2$. The second contribution is therefore 0 if $R^2 \notin (L^*)^{\sigma+1}$, it is $g(q-1)$ otherwise. Assume all those coefficients are nonzero, $\beta = 1$. The first two equations yield

$$\alpha = R\gamma\delta^\sigma, \qquad \alpha^\sigma = R\gamma^\sigma\delta.$$

By comparison this yields the condition $c \in K_1$ where $c = R\delta^{\sigma+1}$. Assume this is satisfied. We have $\alpha^{\sigma+1} = R^2\gamma^{\sigma+1}\delta^{\sigma+1} = cR\gamma^{\sigma+1}$. The last equation is therefore equivalent to $(c-1)(R^2\gamma^{\sigma+1} - 1) = 0$. The existence condition shows $c \neq 1$. This implies $\gamma^{\sigma+1} = 1/R^2$. To sum up the conditions in this last case:

$$\beta = 1, \quad c \in K_1 = \mathbb{F}_{p^d}, \quad \delta^{\sigma+1} = c/R, \quad \gamma^{\sigma+1} = 1/R^2, \quad \alpha = R\gamma\delta^\sigma = c\gamma/\delta.$$

Assume m/d odd. Then $g = 2$, R is a non-square, the first two cases together yield a contribution of $4(q-1)$, the last case yields $2(p^d-1)(q-1)$. The stabilizer order is then $2(p^d+1)(q-1)$ and the orbit length is $|GL(2,q)|/(2(p^d+1)) = |\Omega|/p^d$.

Let now m/d be even. Then $g = p^d + 1$ and R is a representative of one of the cosets. This is not the trivial coset, because of the existence condition. Consider at first the generic case that R is not in the coset of order 2, equivalently $R^2 \notin (L^*)^{\sigma+1}$. Then the second and third contributions are 0, the stabilizer order is $g(q-1)$ and the orbit length is $|GL(2,q)|/(p^d+1) = (2/p^d)|\Omega|$.

The final case is m/d even, $R^2 \in (L^*)^{\sigma+1}$. This time the last contribution vanishes, the stabilizer order is $2g(q-1)$ and the orbit length is $(1/p^d)|\Omega|$.

We know from Lemma 1 that there are precisely $(p^d+1)/2$ orbits under G_1 which belong to the C-family. By the section above $(p^d-1)/2$ of those orbits (corresponding to values R which are not involutory mod L^*) have length $(2/p^d)|\Omega|$ each, the involutory R yields an orbit of length $(1/p^d)|\Omega|$. We see that those orbits together exhaust all of Ω. □

Corollary 3 *Given p, m, s such that $m/\gcd(m,s)$ is even, there is only one orbit containing commutative presemifields. It corresponds to $l = 1/N$, $R = \mu N$. This is then the uniquely determined isotopy class of Budaghyan–Helleseth semifields.*

Proof We saw this essentially in [1]. □

7 The nuclei and commutativity

In [1] it is proved that the center, the left, and the right nucleus of the semifield associated to the presemifield $B(p, m, s, l, t(C_1, C_2))$, $s < m$, $l \neq 0$, agree with $K_1 = \mathbb{F}_{p^{\gcd(m,s)}}$ (Theorem 9). We also saw that the middle nucleus of the semifield associated to the presemifield $B(p, m, s, l, [1, 0, 0, p_4])$, $l \neq 0$, is a quadratic extension of the center (Corollary 3). Further we saw the following; see [1, Corollary 5].

Theorem 6 *The presemifield $B(p, m, s, l, [1, 0, 0, p_4])$, $l \neq 0$ is isotopic to a commutative semifield if and only if either $l \in (L^*)^{\sigma-1}$ or $l^{\sigma+1}/p_4^{\sigma-1} \in L^{\sigma^2-1}$.*

Corollary 4 *Given p, m, s such that $m/\gcd(m, s)$ is odd, there is precisely one isotopy class of presemifields in the C-family which are isotopic to commutative semifields.*

Proof We can choose R to be an arbitrary non-square. For each choice of l there is precisely one G_1-orbit. Notice that the unique choice satisfying the condition of Theorem 6 is $l = 1$. □

We will also use the following commutativity criteria in the special cases $C_1 = 0$ or $C_2 = 0$; see [1, Corollary 4].

Corollary 5 *The presemifield $B(p, m, s, l, t(0, C_2))$ for $l \neq 0, s < m$ is isotopic to a commutative semifield if and only if either $l \in (1/N)L^{\sigma-1}$ or there is $a_0 \in F$ such that $a_0^{p^{m+s}-1} = C_2/(l\overline{C_2})$.*

Observe that the choice $l = 1/N$ is possible if and only if $-N \notin L^{\sigma-1}$ which is equivalent to one of m/d or s/d being even.

Corollary 6 *The presemifield $B(p, m, s, l, t(C_1, 0))$ for $l \neq 0, s < m$, is isotopic to commutative if and only if either $l \in -(1/N)L^{\sigma-1}$ or there is $a_0 \in F$ such that $a_0^{\sigma-1} = C_1/(l\overline{C_1})$.*

This is analogous to the previous lemma. The choice $l = -1/N$ is possible if $N \notin L^{\sigma-1}$ which is equivalent to s/d being odd.

8 The ternary case

Let p, m, s be fixed, $d = \gcd(m, s)$ and $l \neq 0$ such that $-l \notin (L^*)^{\sigma-1}$. As l may be multiplied by an arbitrary element of $(L^*)^{\sigma-1}$ and because of Galois isotopy, the number of cases for l to consider is the number of orbits of the Frobenius on the nontrivial elements of the factor group $L^*/(L^*)^{\sigma-1}$ (of order $p^d - 1$).

Theorem 7 *For each $m \geq 3$ there are precisely two isotopy classes of presemifields $B(3, m, 1, l, t), l \neq 0$. One of them contains commutative semifields, the other does not.*

Proof We have $q = 3^m, \sigma = 3$ is the Frobenius, $d = 1$. The parameter l is essentially uniquely determined. In fact, $-l$ is an arbitrary non-square (see Proposition 2). We choose $l = -\mu$. The number of legitimate quadruples t is $|\Omega| = (3/8)(q+1)q(q-1)^2$ by Theorem 3. Consider the action of the restricted isotopy group G_1 of order $(q^2-1)q(q-1)^2$ on Ω (see Definition 5). We are going to show that G_1 has precisely two orbits on Ω, an orbit $\mathcal{O}_1$ of length $|\Omega|/3$ containing commutative semifields in the C-family and an orbit $\mathcal{O}_2$ of length $2|\Omega|/3$ consisting of presemifields which are not isotopic to commutative semifields. This proves then the theorem. We will also see that $\mathcal{O}_2$ contains members of the C-family if and only if m is even.

Choose at first $t = [1, 0, 0, -\mu^2]$. Then $-p_4 \notin L^4$ and t is legitimate. This quadruple describes an orbit of length $|\Omega|/3$ in the C-family. The presemifield is isotopic to a commutative semifield. In fact, the second condition of Theorem 6 is satisfied.

In order to complete the proof we need to find a $B(3, m, 1, l, t)$ which is not isotopic to a commutative semifield and whose stabilizer in G_1 has order $4(q-1)$.

Consider at first the case when m is even. In this case we saw what we need in the proof of Theorem 5. There are $p^d + 1 = 4$ cosets mod $(L^*)^{\sigma+1}$ in all. The trivial one is not legitimate,

the involutorial one yields a value of $R = -p_4$ which leads to a commutative semifield, and the two remaining values lead to the non-commutative semifield that we need here.

Finally consider the case when m is odd. We have $\mu = N = -1$ and choose $\omega = i$ as an element of order 4. Also $v_2(q+1) = 4$ (see Definition 2) and $\langle i \rangle$ is a Sylow-2-subgroup of $\mathbb{Z}_{q+1}$. Further $v_2(q^2-1) = 8$ and $\langle i-1 \rangle$ is a Sylow-2-subgroup of F^*. We want to find a semifield which is not isotopic to a commutative semifield, in case $C_1 = 0$. The existence condition of Theorem 2 says that $-C_2/\overline{C_2}$ is not a fourth power in $\mathbb{Z}_{q+1}$. Theorem 4 shows that up to isotopy C_2 may be multiplied by an arbitrary fourth power. This amounts to multiplying $-C_2/\overline{C_2}$ by an arbitrary element in $\mathbb{Z}_{(q+1)/4}$, so we can assume that $-C_2/\overline{C_2} \in \langle i \rangle$. The value 1 is excluded by the existence condition, so we can assume $-C_2/\overline{C_2} \in \{-1, i, -i\}$. We use Corollary 5 to decide commutativity. The first of the two conditions is never satisfied, the second says that we have commutativity if and only if $C_2/\overline{C_2}$ is an 8-th power and therefore has odd order. This is the case when $-C_2/\overline{C_2} = -1$, so we are reduced to $-C_2/\overline{C_2} \in \{i, -i\}$. Those do describe presemifields which are not isotopic to commutative semifields. We can choose $C_2 = i-1$. This yields the quadruple $[1, -1, 1, 1]$. Linear isotopy with $M = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ yields $[-1, 0, -1, 1]$, after scalar isotopy $[1, 0, 1, -1]$. Consider the stabilizer in G_1. The conditions are

$$\alpha^3\beta = \gamma^3(\beta+\delta),$$
$$-\alpha^4 + \alpha\gamma^3 + \gamma^4 = \alpha\beta^3 - \alpha\delta^3 - \gamma\delta^3 = \beta^4 - \beta\delta^3 - \delta^4 \neq 0.$$

We have $\beta = 0$ if and only if $\gamma = 0$. This yields $q-1$ solutions $\delta = \alpha$, scalar matrices $diag(\alpha, \alpha)$. Case $\alpha = 0$ yields $q-1$ solutions $\begin{pmatrix} 0 & \beta \\ \beta & -\beta \end{pmatrix}$ and $\delta = 0$ yields the $q-1$ solutions $\begin{pmatrix} \alpha & \alpha \\ \alpha & 0 \end{pmatrix}$. Assume now $\alpha\beta\gamma\delta \neq 0$. Because of homogeneity it can be assumed that $\gamma = 1$. We want to show that this yields precisely one solution to the system.

The first equation shows $\delta = \beta(\alpha^3 - 1)$ (in particular $\alpha \neq 1$). Using this in the remaining equations and $y = -\alpha$ yield the system

$$-\delta^4 - \delta + 1 = -\gamma^3\delta + \gamma^3(\delta^9+1)(1-\delta) = \gamma^4 - \gamma^3(\delta^9+1)\gamma\delta^3,$$

after simplification

$$-y^4 - y + 1 = \beta^3(-y^{10} + y^9 + y + 1) = \beta^4(-y^4 - y + 1)^3 \neq 0.$$

We have

$$x^{10} - x^9 - x - 1 = (x^4 + x - 1)\underbrace{(x^6 - x^5 - x^3 - x^2 - x + 1)}_{f(x)}.$$

Comparing the last two terms shows $\beta = (-y^{10}+y^9+y+1)/(-y^4-y+1)^3 = f(y)/(-y^4-y+1)^2$. On the other hand comparison of the first two terms shows $\beta^3 = 1/f(y)$. The equation is $f(y)^4 = (y^4+y-1)^6$, equivalently

$$f(y)^2 = \pm(y^4+y-1)^3.$$

Observe that $y^4 + y - 1 \neq 0$ is equivalent to M being invertible. One solution is $y = 1$. So far we have $4(q-1)$ elements in the stabilizer, corresponding to a cyclic subgroup of order 4 of $S \subset PGL(2,q)$ generated by $\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$. We claim that this is all of S. We need to show that there are no solutions $x \in L \setminus \mathbb{F}_3$ to

$$f(x)^2 = \pm(x^4 + x - 1)^3.$$

We have $f(x) = (x^2 + x - 1)(x^4 + x^3 - 1)$ and the decomposition of those polynomials into irreducible factors is in fact

$$f(x)^2 + (x^4 + x^3 - 1)^3 = -x(x+1)(x^2+1)(x^4 - x^2 - 1)(x^4 + x^3 + x^2 + x + 1).$$
$$f(x)^2 - (x^4 + x^3 - 1)^3 = (x-1)(x^2 - x - 1)(x^4 + x^3 + x^2 + 1)(x^4 - x^3 + x^2 + x - 1).$$

□

To sum up, here is the complete census in case $p = 3$, $s = 1$, when m is odd. We have $\mu = N = -1$ and also $l = 1$. The commutative orbit has representative $C(3, m, 1, 1, -1)$ (in fact $l^{\sigma+1}R^{\sigma-1} = 1$). The second orbit is non-commutative and has representative $B(3, m, 1, 1, 0, i-1)$. In order to confirm non-commutativity, we use Corollary 5. We would have commutativity if one of two conditions is satisfied. The first is $1/N \in L^{\sigma-1}$, here $-1 \in L^2$ which is not true. The second condition is that $C_2/l\overline{C_2}$ is a $(3^{m+1} - 1)$-st power. In particular i has to be an 8-th power which is not true.

Let $p = 3$, $s = 1$ and m even. Choose $N = \mu$ as a generator of the Sylow-2-subgroup. Again $l = -\mu$ is uniquely determined. Both orbits belong to the C-family. Case $R = -\mu^2$ yields the commutative orbit (in fact $l^4R^2 = \mu^8 \in L^8$) and $R = \mu$ yields the non-commutative orbit (in fact $l^4R^2 = \mu^6 \notin L^8$).

Theorem 8 *Let $m \geq 3$ be odd. There are precisely two isotopy classes of presemifields $B(3, m, 2, l, t)$, $l \neq 0$. One of them contains commutative semifields, the other does not.*

Proof We have $d = 1$, $\mu = -1$, $N = 1$, $\omega = i$, $|\Omega| = (3/8)(q+1)q(q-1)^2$. Again l is uniquely determined: $l = 1$. Recall that the Sylow-2-subgroup of F^* is generated by $i - 1$, of order 8. Consider $[1, 0, 0, u]$. This is legitimate if and only if $R = -1/u$ is a non-square in L, equivalently if u is a square. We choose $u = 1$, the quadruple $[1, 0, 0, 1]$. The corresponding semifield is isotopic to a commutative semifield by Theorem 6. The order of the stabilizer is $8(q-1)$ and the orbit length is $|GL(2,q)|/8 = |\Omega|/3$.

Choose $C_1 = i - 1, C_2 = 0$. We have $t = [1, -1, 1, 1]$. Linear isotopy with $M = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ yields the quadruple $[-1, 0, -1, 1]$, after scalar isotopy $[1, 0, 1, -1]$. The corresponding polynomial (Definition 1) is $X^{10} + X - 1$. The decomposition into irreducible factors over $\mathbb{F}_3$ is

$$X^{10} - X - 1 = (X^2 - X - 1)(X^8 + X^7 - X^6 - X^4 - X^3 + X^2 + 1).$$

In particular $X^{10} \pm X - 1$ have no roots in $L = \mathbb{F}_{3^m}$ (m odd). This confirms that $[1, 0, 1, -1]$ is legitimate. Corollary 6 shows that the corresponding presemifield is not isotopic to a commutative semifield.

The stabilizer equations for this quadruple are

$$\beta^9(\alpha + \gamma) = \gamma\delta^9, -\delta^{10} + \beta^9\delta + \beta^{10} = \gamma^9\delta - \alpha^9(\beta + \delta) = \gamma^{10} - \alpha^9\gamma - \alpha^{10}.$$

We need to show that the order of the stabilizer is $4(q-1)$. We have $\beta = 0$ if and only if $\gamma = 0$. This yields the scalar matrices as $q - 1$ solutions. Assume $\alpha = 0$. Then $\beta = \gamma = \delta$

yields another set of $q-1$ solutions. Assume $\delta = 0$ and $\beta = 1$. Then $\gamma = 1, \alpha = -1$. This yields a third set of $q-1$ solutions.

Assume now $\alpha\gamma\delta \neq 0$ and $\beta = 1$. Then $\alpha = \gamma(\delta^9 - 1)$ and

$$1 + \delta - \delta^{10} = \gamma^9(-\delta^{82} - \delta^{81} - \delta + 1) = \gamma^{10}(1 + \delta - \delta^{10})^9,$$

which must be nonzero because $det(M) = \gamma(\delta^{10} - \delta - 1)$. By comparison we obtain

$$\gamma^9 = (-\delta^{82} - \delta^{81} - \delta + 1)^9/(1 + \delta - \delta^{10})^{81} = (1 + \delta - \delta^{10})/(-\delta^{82} - \delta^{81} - \delta + 1),$$

equivalently $(1 + \delta - \delta^{10})^{41} = \pm((\delta^{82} + \delta^{81} + \delta - 1)^5$. Values $\delta \in \mathbb{F}_3$ certainly satisfy this. However the case $\delta = 0$ has been considered earlier and $\delta = 1$ leads to $\alpha = 0$ which has been considered before. The value $\delta = -1$ yields $\gamma = 1, \alpha = 1$ which gives us a fourth contribution of $q-1$ to the order of the stabilizer. We claim that this is all. In order to see this it can be verified that the polynomials

$$(1 + X - X^{10})^{41} \pm (X^{82} + X^{81} + X - 1)^5 \in \mathbb{F}_3[X]$$

do not have irreducible factors of odd degree > 1. We have found that Ω is the union of precisely two G_1-orbits, the second orbit of length $2|\Omega|/3$ not belonging to the C-family. □

Here is the census in this case: there are precisely two isotopy types. $C(3, m, 2, 1, -1)$ is a representative of the commutative orbit. A representative for the second orbit is $B(3, m, 2, 1, t(i-1, 0))$.

Finally we observe that the situation will probably not always be as simple as in the cases of Theorems 7 and 8. Consider case $p = 3$, $s = 2$, when m is divisible by 4. In this case there are many more orbits. Observe that $q-1$ is divisible by 16. Let μ be a generator of the Sylow-2-subgroup. Then $N = \mu^4$. We have that l is determined only up to cosets mod $(L^*)^8$, and $L^*/(L^*)^8$ has order 8. Because of the existence condition and Galois isotopy we can choose $l \in \{\mu, \mu^2, \mu^4, \mu^5\}$. Theorem 5 shows that for each such l there are 5 orbits of G_1 on Ω, for a grand total of 20 possible isotopy types. Everything belongs to the C-family and exactly one of those 20 presemifields is isotopic to a commutative semifield. It corresponds to the choice $l = \mu^4$, $R = \mu N = \mu^5$. The total number of isotopy types is between 2 and 20.

Acknowledgements The research of D. Bartoli, G. Faina, 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). J. Bierbrauer's research was supported in part by GNSAGA - INdAM.

References

1. Bierbrauer J.: Projective polynomials, a projection construction and a family of semifields. Des. Codes Cryptogr. **79**, 183–200 (2016).
2. Bierbrauer J., Bartoli D., Faina G., Marcugini S., Pambianco F.: A family of semifields of order 729. In: Proceedings of ACCT, pp. 41–45 (2014).
3. Bierbrauer J., Bartoli D., Kyureghyan G., Giulietti M., Marcugini S., Pambianco F.: A family of semifields in characteristic 2. J. Algebr. Comb. **45**(2), 455–473 (2017).
4. Bluher A.W.: On $x^{q+1} + ax + b$. Finite Fields Appl. **10**, 285–305 (2004).
5. 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).
6. Hughes D.R., Kleinfeld E.: Seminuclear extensions of Galois fields. Am. J. Math. **82**, 389–392 (1960).