A projection construction for semifields*

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, MI 49931

William M. Kantor
Department of Mathematics
University of Oregon
Eugene, OR 97403

December 30, 2011

Abstract

Simple constructions are given for finite semifields that include as special cases both old semifields and recently constructed semifields.

1 Introduction

A finite *semifield* is a finite non-associative algebra $(F, +, *)$ (i.e., not necessarily associative algebra) with identity element 1 such that $x * y = 0 \Rightarrow x = 0$ or $y = 0$. Thus, $(F, +)$ is an abelian group, and both distributive laws hold. A finite *presemifield* satisfies the same conditions except for the existence of an identity element. Semifields first arose in the study of algebras resembling fields [8], and soon afterwards were used to construct finite nondesarguesian projective planes [18]. A fundamental result of Albert [1] states that two semifields (or

*This research was supported in part by NSA grant H98230-10-1-0159 and NSF grant DMS 0753640.

presemifields) $(F,+,*)$ and $(F',+,*')$ determine isomorphic planes if and only if the algebras are *isotopic*: there are additive group isomorphisms $A,B,C\colon F\to F'$ such that $A(x)*'B(y)=C(x*y)$ for all $x,y\in F$. Each presemifield is isotopic to a semifield (cf. Section 3.2). There are many surveys of finite semifields (e.g., [7, Ch. V] and [13]).

If $F=\oplus_i U_i$ is a direct decomposition of the group $(F,+)$, with corresponding projection maps E_i, then $x*y=\sum_i E_i(x*y)$. We will slightly generalize this trivial observation and reverse this process (Proposition 2.2) in order to obtain both new views of well-known semifields and new semifields. In Section 3 we collect some general information concerning some presemifields, the corresponding semifields and their nuclei. In Section 4 it is shown that the Dickson semifields [8], the Hughes-Kleinfeld semifields [10] and some of the Knuth semifields [15] can be constructed via Proposition 2.2 using as ingredients semifields isotopic to fields.

Our new constructions are based on (isotopes of) fields and the *twisted fields* of Albert [2]. Our presemifields and some of their properties are obtained in Sections 5-8, and are summarized in the following

Theorem 1.1. *There are presemifields of order p^{2m} with p a prime of the following sorts (where $\sigma=p^s$ with $1\le s<m$; $v\in L=\mathbb{F}_{p^m}$; $l,n,N,R\in L^*$; $\beta\in F^*=\mathbb{F}^*_{p^{2m}}$):*

- (a) *$A(p,m,s,l,\mu)$ with $-l\notin L^{\sigma-1}$ and $\overline{\mu}/\mu$ not in the subgroup of F^{*p^m-1} of index* $\gcd(p^m+1,\sigma+1)$.
- (b) *$B(p,m,s,l,n,N)$ with p odd, where $-l\notin L^{\sigma-1}$ and the polynomial $t^{\sigma+1}+(1-1/N)t+(1/n-1)/N$ has no root in L.*
- (c) *$C(p,m,s,l,R)$ with p odd, where $-l\notin L^{\sigma-1}$ and $R\notin L^{\sigma+1}$.*

For odd p the nuclei are described in Theorems 8.21, 8.23, 8.25, *and* Propositions 8.1, 8.29.

Some of these semifields are isotopic to commutative ones, but most are not when p is odd. Section 7 handles this isotopism question for odd p, using a criterion due to Ganley [9, Theorem 4]. We use a semifield associated with a given presemifield (see Proposition 3.5) to extend the Ganley criterion to presemifields (Corollary 3.9). A simple, direct proof of the Ganley criterion is given in Theorem 3.8.

The right nucleus $\mathbb{N}_r$, middle nucleus $\mathbb{N}_m$ and left nucleus $\mathbb{N}_l$ of a semifield F are the sets of all r,m or $l\in F$ behaving as follows for all

$x, y \in F$.

$r \in \mathbb{N}_r$	$m \in \mathbb{N}_m$	$l \in \mathbb{N}_l$
$(x * y) * r = x * (y * r)$	$(x * m) * y = x * (m * y)$	$(l * x) * y = l * (x * y)$

These nuclei are significant for the planes (it is an old and elementary result about projective planes [11, Theorem 8.2] that the nuclei correspond to three natural homology groups – important types of collineation groups). In particular, isotopic semifields have isomorphic nuclei. We emphasize that nuclei are only dealt with in odd characteristic. In that case, in all parts of Theorem 1.1 the left and right nuclei are identical, of order $p^{\gcd(s,m)}$. Whenever we are able to determine the middle nucleus, it turns out to be at most a quadratic extension of the left (right) nucleus. Moreover, the method used in Section 6 in odd characteristic in order to obtain the B- and C-families from the A-family undoubtedly works in characteristic 2, but the calculations become tedious and so have been avoided. The efforts used in Section 8 to study nuclei would again be more detailed in characteristic 2.

Several instances of our constructions have already appeared. The families of commutative semifields constructed in Budaghyan-Helleseth [5] are special cases of $A(p, m, s, 1/N, \mu)$ in odd characteristic. Their first family is isotopic to members of the C-family (see Theorem 7.1 and Proposition 7.9); the members of their second family not in the first are isotopic to $B(p, m, s, 1/\omega^{\sigma-1}, n, n^{(\sigma-1)/2})$, where $n \in L$ is a non-square (see Proposition 7.16).

Planar functions possess at least two different analogues in characteristic 2: commutative semifields and APN functions. The latter form a core part of the theory of cryptographic S-boxes. The projection method works also in this context, and the APN hexanomials of Budaghyan-Carlet [4] are characteristic 2 analogues of a special case of the A-family.

2 A projection construction

All algebras will be finite.

Definition 2.1. *Let $(F, +, *_i)$, $i = 1, \ldots, n$, be non-associative algebras with the same additive group F, and let $A_i \subset F$ be additive subgroups. Then the set $\{(*_i, A_i)\}$ is called* compatible *if $x *_i y \in A_i$ for $i = 1, \ldots, n$ imply that x or $y = 0$.*

The following is evident:

Proposition 2.2. *Let $F = \oplus_i U_i$. Suppose that $(F, +, *_i)$ are non-associative algebras, $i = 1, \dots, n$, such that the set $\{(*_i, A_i)\}$ is compatible and $\dim_{\mathbb{F}_p} A_i + \dim_{\mathbb{F}_p} U_i = \dim_{\mathbb{F}_p} F$. If $f_i\colon F \to U_i$ is any $\mathbb{F}_p$-linear map such that $\ker(f_i) = A_i$, then*

$$x \circ y = \sum_i f_i(x *_i y) \tag{2.3}$$

defines a presemifield on F.

Conversely:

Proposition 2.4. *Any presemifield $(F, +, *)$ can be constructed in many ways using* Proposition 2.2.

Proof. Use an arbitrary direct sum decomposition $F = \oplus_{i=1}^n U_i$, $U_i \neq 0$, with f_i the projections to the U_i. Define $x *_i y = f_i(x * y) \in U_i$. If $A_i = \oplus_{j \neq i} U_j$ then the set $\{(*_i, A_i)\}$ is compatible, and Proposition 2.2 yields $(F, +, *)$. □

The preceding proof shows that the construction in Proposition 2.2 yields all presemifields, and each one in ridiculously many ways. We will make this construction more interesting by using ingredients $x *_i y$ that are sufficiently elementary.

Although the proof of Proposition 2.2 is trivial, it has several interesting instances. It was first used for odd characteristic commutative semifields in [3], where the generalization to the non-commutative case was already alluded to. In the applications we will concentrate on the case when $n = 2, r = 2m$ and $r_1 = r_2 = m$. *The advantage of the notion of compatibility is that the maps f_i are essentially ignored.* In the next section we will discuss the isotopy of some of the presemifields (2.3) for different choices of these maps.

3 Basic considerations

3.1 Projections

Assume that $F = \mathbb{F}_{q^{2m}} \supset L = \mathbb{F}_{q^m}$, $x \to \overline{x}$ is the involutory automorphism of F and $T\colon F \to L$ is the trace map.

Let $\omega \in F^*$ with $T(\omega) = 0$, where $\omega = 1$ in characteristic 2.

Assume that $(*_1, u_1 L)$ and $(*_2, u_2 L)$ are compatible, where $u_i \in F$ (Definition 2.1). We will consider the corresponding presemifield $(F, *)$ of Proposition 2.2 up to isotopy, using the L-linear mappings $f_i(x) = T((\omega/u_i)x)z_i$ on F, $i = 1, 2$, where $z_i \in F^*$ and $z_2/z_1 \notin L$.

Up to isotopy we can choose $z_1 = 1$ and $z_2 = z$ an arbitrarily fixed element not in L. The corresponding presemifield product therefore has the form $x * y = T\big((\omega/u_1)(x *_1 y)\big) + T\big((\omega/u_2)(x *_2 y)\big)z$. Let $*_i'$ be defined by $x *_i' y = (x *_i y)/u_i$. Then $(*_1', L)$ is compatible with $(*_2', L)$ and we have $x * y = T\big(\omega(x *_1' y)\big) + T\big(\omega(x *_2' y)\big)z$. Replacing the products $x *_i y$ by multiples $\beta_i(x *_i y)$ we can therefore assume that the compatibility condition has $A_1 = A_2 = L$. Using any $z \notin L$, (2.3) has the form

$$x * y = T\big(\omega(x *_1 y)\big) + T\big(\omega(x *_2 y)\big)z. \tag{3.1}$$

Of course, different choices for z produce isotopic presemifields. For example, in odd characteristic we can choose $z = 1/\omega$, which corresponds to $f_2(x) = x - \overline{x}$ and

$$x * y = \frac{1}{2}\big[\omega(x *_1 y - \overline{x *_1 y}) + (x *_2 y - \overline{x *_2 y})\big].$$

Neighbors. In the setting of Definition 2.1 we call n-tuples $\{(*_i, A_i)\}$ and $\{(*_i', A_i)\}$ *neighbors* if $x *_i y - x *_i' y \in A_i$ for all $x, y \in F$. Then $\{(*_i, A_i)\}$ compatible if and only if $\{(*_i', A_i)\}$ is. *The resulting presemifield products* (2.3) *are then identical.* Thus, apparently different ingredients $\{(*_i, A_i)\}$ can produce the same semifields.

For example, consider the field product xy in odd characteristic and a Dickson-Knuth product $x \underset{DK}{\circ} y = ac + b^\sigma d^\tau \mu + (ad + bc)\omega$ where $x = a + b\omega, y = c + d\omega$ and $a, b, c, d \in L$. Then $x \underset{DK}{\circ} y - xy \in L$ for all $x, y \in L$. Whenever (xy, L) is used as one member of a compatible pair it can be replaced by $(x \underset{DK}{\circ} y, L)$ without changing the resulting presemifield.

3.2 Isotopes

Any presemifield $(F, +, *)$ *is isotopic to a semifield.* The traditional approach [14, p. 957] is to fix *any* $0 \neq e \in F$ and define $\star$ by

$$(x * e) \star (e * y) = x * y \tag{3.2}$$

for all $x, y \in F$. Then $(F,+,\star)$ is a semifield with identity element $e * e$, and is obviously isotopic to $(F,+,*)$. We will use a different isotope with the property that e, not $e * e$, is the identity element. Define $\beta, \gamma \colon F \to F$ by

$$e * \beta(x) = x \quad \text{and} \quad \gamma(x) * e = e * x \tag{3.3}$$

(so that $\gamma(e) = e$, $\gamma(\beta(x)) * e = x$ and $\beta(e * y) = y$), and

$$x \circ y := \beta\bigl(\gamma(x) * y\bigr). \tag{3.4}$$

Then $(F,+,\circ)$ *is a semifield isotopic to* $(F,+,*)$ *with identity element* e, since $x \circ e = \beta\bigl(\gamma(x) * e\bigr) = \beta(e * x) = x$ and $e \circ y = \beta\bigl(\gamma(e) * y\bigr) = \beta(e * y) = y$ for any $x, y \in F$. If $(F,+,*)$ is commutative then so are $(F,+,\star)$ and $(F,+,\circ)$ (since $\gamma(x) = x$)).

The following observations build on $(F,+,\circ)$ to obtain information concerning the nuclei of any semifield isotopic to a given presemifield. (The *center* of a semifield is the set of elements in all three nuclei that commute with all elements.)

Proposition 3.5. *Consider fields* $F_1 \subseteq F_2 \subseteq F$ *and a presemifield* $(F,+,*)$. *Assume that*

(i) $(ax) * y = x * (ay) = a(x * y)$ *for all* $x, y \in F$, $a \in F_1$, *and*

(ii) $(xk) * y = x * (ky)$ *for all* $x, y \in F, k \in F_2$.

If β, γ *and* $x \circ y$ *are defined as above using* $e = 1$, *then* $(F,+,\circ)$ *is a semifield with identity element* 1, *center containing* F_1 *and middle nucleus containing* F_2, *such that* $k \circ y = yk$ *for all* $y \in F$, $k \in F_2$.

Proof. By (i,ii), β and γ are F_1-linear, so that $x \circ a = ax = a \circ x$ for all $x \in F, a \in F_1$. Then (i) and (3.4) imply that F_1 is a subfield of the center of F.

If $k \in F_2$, $y \in F$, we obtain the final assertion of the proposition:

$$k \circ y = \beta\bigl(\gamma(k) * y\bigr) = \beta([1k] * y) = \beta(1 * [ky]) = ky$$

by (ii) and the definitions of β, γ and $\circ$. Finally, we claim that k is in the middle nucleus of $(F,+,\circ)$. For, if also $x \in F$, then, again by (ii) and definition,

$$x \circ (k \circ y) = x \circ (yk) = \beta[\gamma(x) * (yk)] = \beta[\bigl(k\gamma(x)\bigr) * y],$$

while $(x \circ k) \circ y = \beta[\gamma(x \circ k) * y]$. Finally, for the same reasons, $\gamma(x \circ k) = \gamma\bigl(\beta(\gamma(x) * [k1])\bigr) = \gamma\bigl(\beta([k\gamma(x)] * 1)\bigr) = k\gamma(x)$, as required. □

Proposition 3.6. *Let F be a field and $(F, +, *)$ a presemifield, and define β, γ and $x \circ y$ as above using $e = 1$.*

(a) *Any $x \in F$ satisfying $(\gamma(x)y) * z = \gamma(x)(y * z)$ for all $y, z \in F$ is in the left nucleus of $(F, \circ, +)$.*

(b) *Any $z \in F$ satisfying $x * (yz) = z(x * y)$ for all $x, y \in F$ is in the right nucleus of $(F, \circ, +)$ and satisfies $y \circ z = yz$ for all $y \in F$.*

Proof. (a) We have $\gamma(x \circ y) = \gamma(x)\gamma(y)$ for all y since $\gamma(x \circ y) * 1 = 1 * (x \circ y) = \gamma(x) * y$ by the definitions of $\circ$ and γ, while the definition of γ and two applications of our hypothesis concerning x yield $[\gamma(x)\gamma(y)] * 1 = \gamma(x)[\gamma(y) * 1] = \gamma(x)(1 * y) = [\gamma(x)1] * y$.

By the definition of $\circ$ and hypothesis, if $z \in F$ then $1*[(x\circ y)\circ z] = \gamma(x \circ y) * z = [\gamma(x)\gamma(y)] * z = \gamma(x)[\gamma(y) * z] = \gamma(x)[\gamma(y) * z] = [\gamma(x)1] * (y \circ z) = 1 * [x \circ (y \circ z)]$, so that x is in the left nucleus.

(b) By definition and hypothesis, if $x, y \in F$ then $1 * (y \circ z) = \gamma(y) * (1z) = z[\gamma(y) * 1] = z(1 * y) = 1 * (yz)$ and hence $1 * [(x \circ y) \circ z] = \gamma(x \circ y) * [1z] = z[1 * (x \circ y)] = z[\gamma(x) * y] = \gamma(x) * (yz) = 1 * [x \circ (yz)] = 1 * [x \circ (y \circ z)]$, so that z is in the right nucleus. □

Corollary 3.7. *Let $(F, +, *_i)$ and the compatible set $\{(*_i, A_i)\}$ be as in* Definition 2.1 *for $i = 1, \ldots, n$. Use the presemifield multiplication* (2.3). *Let $F_1 \subseteq F_2$ be subfields of F behaving as in* Proposition 3.5(i),(ii), *for each $(F, +, *_i)$, where the f_i are F_1-linear. Then any semifield isotopic to $(F, +, *)$ has center of order at least $|F_1|$ and middle nucleus of order at least $|F_2|$.*

Proof. As the $*_i$ satisfy Proposition 3.5(i),(ii), the F_1-linearity of the f_i implies that the presemifield multiplication (2.3) also satisfies Proposition 3.5(i),(ii). The preceding proposition yields our claim. □

3.3 Isotopes of commutative semifields

The next result is due to Ganley [9, Theorem 4], who used a very different type of proof.

Theorem 3.8. *A semifield $(F, +, \circ)$ is isotopic to a commutative presemifield if and only if there is some $w \neq 0$ such that $(w \circ x) \circ y = (w \circ y) \circ x$ for all $x, y \in F$.*

Proof. If w exists, then $x \cdot y = (w \circ x) \circ y$ defines a commutative presemifield isotopic to $(F, +, \circ)$.

Conversely, if $(F,+,\circ)$ is a semifield isotopic to a commutative presemifield $(F,+,\cdot)$, then there are (additive) permutations α,β,γ of F such that $\gamma(x\cdot y)=\alpha(x)\circ\beta(y)$, and hence $\alpha(x)\circ\beta(y)=\alpha(y)\circ\beta(x)$, for all $x,y\in F$. Let $\beta(u)=1$ (the identity element of $(F,+,\circ)$) and $w=\alpha(u)$. Then $\alpha(x)=\alpha(x)\circ\beta(u)=\alpha(u)\circ\beta(x)=w\circ\beta(x)$, and hence $(w\circ\beta(x))\circ\beta(y)=(w\circ\beta(y))\circ\beta(x)$ for all $x,y\in F$. □

Of course, all commutative presemifields are isotopic to commutative ones by (3.2) or (3.4). The preceding proof did not use the additive group at all: it really provides a simple criterion for a loop to be isotopic to a commutative loop (and a similar statement holds for (3.2) and (3.4).)

Corollary 3.9. *Let* $(F,+,*)$ *be a presemifield. Let the maps* β,γ *in* (3.3) *define the associated semifield* (3.4). *The function* $\alpha(x)=\gamma(\beta(x))$ *is defined by* $\alpha(x)*1=x$. *Then* $(F,+,*)$ *is isotopic to a commutative semifield if and only if there is some* $v\neq 0$ *such that* $\alpha(v*x)*y=\alpha(v*y)*x$ *for all* x,y.

Proof. If $v\neq 0$ exists, then $x\cdot y=\alpha(v*x)*y$ defines an isotopic commutative presemifield.

Conversely, if $(F,+,*)$ is isotopic to a commutative presemifield then so is the semifield $(F,+,\circ)$ in (3.4). By Theorem 3.8, there is some $w\neq 0$ such that $(w\circ x)\circ y=(w\circ y)\circ x$ for all x,y. Let $v=\gamma(w)$. Then, by (3.4), $(w\circ x)\circ y=\beta(\alpha(v*x)*y)$ also equals $(w\circ y)\circ x=\beta(\alpha(v*y)*x)$. □

We will use Corollary 3.9 to show that many of our new semifields are isotopic to commutative ones and many are not.

4 Field multiplications as ingredients

It is natural to ask which presemifields can be constructed using as ingredients only products isotopic to field multiplication. In this section we briefly discuss examples showing that it is possible to apply Proposition 2.2 to isotopic copies of the same semifield product and obtain non-isotopic semifields.

The Hughes-Kleinfeld semifields. Consider $F=\mathbb{F}_{q^4}$ in odd characteristic, $T\colon F\to L=\mathbb{F}_{q^2}$ the trace, and $\omega\in F^*$ of trace 0 so that $n=\omega^2$ is a non-square in L. Write elements of F in the form

$x = a + b\omega$ with $a, b \in L$. If $l \in L \setminus \mathbb{F}_q$, define the Hughes-Kleinfeld semifield $(F, +, \underset{HK}{\circ})$ [10] by

$$(a + b\omega) \underset{HK}{\circ} (c + d\omega) = ac + lb^q d + (a^q d + bc)\omega.$$

If also $y = c + d\omega$, let $x *_1 y = ac + lb^q d$ and $x *_2 y = (a^q d + bc)\omega$ be the projections of $\underset{HK}{\circ}$ to L and $L\omega$, respectively. Define $\mathbb{F}_q$-linear invertible mappings $\alpha_i \colon F \to F$ by $\alpha_1(a + b\omega) = a + (l/n)b^q\omega$ and $\alpha_2(a + b\omega) = a^q + b\omega$. Let $x *_i' y = \alpha_i(x)y$. Then $*_1'$ is an $L\omega-$neighbor of $*_1$, and $*_2'$ is an $L-$neighbor of $*_2$. It follows that $\underset{HK}{\circ}$ can be described by Proposition 2.2 using as ingredients $x *_1' y$ and $x *_2' y$, both of which are isotopic to the field multiplication, since

$$x \underset{HK}{\circ} y = (1/2)T\big(\alpha_1(x)y\big) + (1/2n)T\big(\omega\alpha_2(x)y\big)\omega.$$

The Dickson semifields. Let $F = \mathbb{F}_{q^{2m}} \supset L = \mathbb{F}_{q^m}$ in odd characteristic and $\omega \in F$ with $\omega^2 = n$ a non-square in L. Let $\alpha(a + b\omega) = a + b^\sigma\omega$, where σ is a power of q. Then $(\omega\alpha(x)\alpha(y), L)$ is compatible with (xy, L), and the resulting product

$$x * y = (1/2)T(\alpha(x)\alpha(y)) + (1/2)T(xy/\omega)\omega$$

corresponds to a Dickson semifield [8].

Some Knuth semifields. Next we use Proposition 2.2 to construct one of Knuth's families of semifields $(F, *)$ using as ingredients multiplications isotopic to field multiplication. Let $L = \mathbb{F}_q \subset F = \mathbb{F}_{q^2}$; choose $f, g \in L$ and a power σ of q such that

$$t^{\sigma+1} + tg - f \neq 0 \text{ for all } t \in L. \tag{4.1}$$

If $1, \lambda$ is a basis of F over L with $N(\lambda) = -f$, then

$$(a + b\lambda) * (c + d\lambda) = (ac + b^{1/\sigma}df) + (bc + a^\sigma d + bdg)\lambda \tag{4.2}$$

(with $a, b, c, d \in L$) produces a semifield $(F, +, *)$ [15, Sec. 7.3].

Define three invertible L-linear maps $F \to F$ by $\alpha_1(a + b\lambda) = a + b^{1/\sigma}\lambda$, $\alpha_2(a + b\lambda) = a^\sigma + \lambda$ and $\beta_2(a + b\lambda) = a + b(g - T(\lambda)) + b\lambda$.

Proposition 4.3. *The pairs* $(\overline{\lambda}\alpha_1(x)y, L)$ *and* $(\alpha_2(x)\beta_2(y), L)$ *are compatible, and a semifield obtained via* Proposition 2.2 *is isotopic to* (4.2).

Proof. This is a routine calculation. We have $\lambda^2 = T(\lambda)\lambda + f$. If $x = a + g\lambda$ and $y = c + d\lambda$, then

$$\begin{aligned} \alpha_1(x)y &\in ac + b^{1/\sigma}df + L\lambda \\ a_2(x)\beta_2(y) &\in (a^\sigma d + bc + bd(g - T(\lambda)) + bdT(\lambda))\lambda + L. \end{aligned}$$

□

Thus, it is possible for the ingredients to be isotopic to commutative presemifields while the new presemifield is not isotopic to a commutative one.

5 The semifields $A(p, m, s, l, \mu)$

In this section we will define a family of examples obtained using Definition 2.1 and discuss its properties. In the next section we will describe variations and partial generalizations.

Let $L = \mathbb{F}_{p^m} \subset F = \mathbb{F}_{p^{2m}}$, $l \in L^*$, $\sigma = p^s$ with $1 < s < m$. Let the operation $x \underset{A}{\circ} y = xy^\sigma + lx^\sigma y$ on F imitate a twisted field (here the subscript A stands for Albert). Let $\mu \in F^*$. We apply Definition 2.1 with

$$A_1 = A_2 = L,\ \ x *_1 y = xy,\ x *_2 y = \mu(\overline{x} \underset{A}{\circ} y).$$

Thus, by (3.1) our binary operation is

$$x * y = T(\omega xy) + T\big(\omega\mu(\overline{x} \underset{A}{\circ} y)\big)\omega. \tag{5.1}$$

Theorem 5.2 (The semifields $A(p, m, s, l, \mu)$)**.** *The pairs (xy, L) and $(\mu(\overline{x} \underset{A}{\circ} y), L)$ are compatible if and only if*

- (i) $-l \notin L^{\sigma-1}$ *and*
- (ii) $\mu^{p^m-1} = \overline{\mu}/\mu$ *is not contained in the subgroup of* $\mathbb{F}^{*p^m+1}$ *of index* $\gcd(p^m + 1, \sigma + 1)$.

Proof. Let $x, y \neq 0$. Then $T(\omega xy) = 0 \iff xy \in L^* \iff y = a\overline{x} \neq 0$ for some $a \in L^*$, in which case

$$x *_2 y = \mu\big(\overline{x} \underset{A}{\circ} (a\overline{x})\big) = \mu\overline{x}^{\sigma+1}(a^\sigma + la).$$

The last factor is in L, and (i) is equivalent to this factor being nonzero for $a \neq 0$. Moreover, (ii) is equivalent to $\mu \notin L^*F^{*\sigma+1}$ and hence to $\mu\overline{x}^{\sigma+1} \notin L$ for all $x \in F^*$. □

We emphasize the elementary nature of this proof using a convenient factorization. Note that (i) is precisely the condition needed for $(L, \underset{A}{\circ})$ to be a twisted field, so that $(F, *)$ can be viewed as a "quadratic extension of a twisted field" (compare Lemma 5.5). The gcd in (ii) needs to be > 1. Hence, if $\sigma = 1$ then q must be odd; but in this case our presemifield is isotopic to a field.

There is a more general version of (5.1) using $x \underset{A}{\circ} y = x^{\sigma'} y^{\sigma} + l x^{\sigma} y^{\sigma'}$ with $\sigma' \in \mathrm{AutF}$, and $x * y = T(\omega\mu_1 xy) + T\big(\omega\mu_2(\overline{x} \underset{A}{\circ} y)\big)z$ for $\mu_i \in F^*$ such that $\mu_1^{\sigma-\sigma'} \in L$. We leave it to the reader to verify that this apparently more general product yields a presemifield isotopic to one of those in the theorem.

Corollary 5.3. *There is a semifield isotopic to $A(p, m, s, l, \mu)$ such that $\mathbb{F}_q$ is in the center while the field $\{z \mid z \in F,\ \overline{z} = z^{\sigma} = z^{1/\sigma}\}$ is in the middle nucleus.*

Proof. This follows from Corollary 3.7. □

Lemma 5.4. *Up to isotopy of $A(p, m, s, l, \mu)$, l can be replaced by an arbitrary member of the coset $lL^{*\sigma-1}$ and μ can be replaced by an arbitrary member of μL^*.*

Proof. Use $x' = \alpha x$, $y' = y/\alpha$ as new variables to map

$$l \to l/N(\alpha)^{\sigma-1},\ \mu \to \mu\alpha^{\sigma}/\overline{\alpha}.$$

The last statement corresponds to using $z' = kz$, $k \in L^*$. □

Lemma 5.5. *There is a presemifield $(F, \star)$ isotopic to $A(p, m, s, l, \mu)$ such that the subfield L of F is closed under $\star$ and $(L, +, \star)$ is isotopic to $(L, +, \underset{A}{\circ})$.*

Proof. An isotopic presemifield product is $x \star y = T(\omega\mu(x \underset{A}{\circ} y)) + T(\omega\overline{x}y)\omega$. If $x, y \in L$ then $x \star y = T(\omega\mu)(x \underset{A}{\circ} y)$, so that $(L, +, \star)$ and $(L, +, \underset{A}{\circ})$ are isotopic. □

It follows from the preceding lemma that $A(p, m, s, l, \mu)$ can be isotopic to a field only if the corresponding twisted field is. This is the case if and only if σ^2 is the identity on L. (In the latter case the twisted field $(L, +, \underset{A}{\circ})$ is isotopic to $(L, +, \circ')$, $x \circ' y := xy + l(xy)^{\sigma}$, and hence to a field.)

In Section 8 we will see that Corollary 5.3 and Lemma 5.5 provide information on the nuclei as the nuclei of twisted fields are known [2, Theorem 1]. The conditions in Theorem 5.2 can be met if and only if both $\gcd(q^m - 1, \sigma - 1)$ and $\gcd(q^m + 1, \sigma + 1)$ are not 1. These requirements always hold in odd characteristic, so the construction is more widely applicable in that case. If $p = 2$ then the conditions in Theorem 5.2 can be met if $\log_2 q^m$ is an odd integer divisible by $\log_2 s$.

Characteristic 2. We briefly consider $A(2, m, s, l, \mu)$ in Theorem 5.2. If $Q = 2^m$ then $F = \mathbb{F}_{Q^2} \supset L = \mathbb{F}_Q$. Let $m = 2u$ for odd u and choose $\sigma = 4$. Then $\gcd(Q - 1, \sigma - 1) = 3$ and our requirement on l is that $l \in L \setminus L^3$. It follows from Lemma 5.4 that the choice of l does not affect the isotopy class. As u is odd we have $\gcd(Q + 1, \sigma + 1) = 5$. It follows from Lemma 5.4 that we may assume that μ has norm 1 and is not a fifth power in the norm 1 group. Observe that $\mathbb{F}_{16} \subset F$ and 25 does not divide $Q^2 - 1$ unless $u = 5 \bmod 10$. If u is not 5 mod 10 we can choose μ as an element of order 5.

The smallest case, $A(2, 2, 2, \omega, \mu)$ of order 16, is a field. Here ω is an element of order 3, the field $\mathbb{F}_{16}$ has been constructed as $\mathbb{F}_2(\alpha)$ where $\alpha^4 = \alpha + 1$ and $\mu = \alpha^3, \omega = \alpha^5$. The presemifield multiplication can be chosen as $x * y = T(\mu(\overline{xy} + \omega xy)) + T(xy)\mu$ where $T \colon \mathbb{F}_{16} \to \mathbb{F}_4$ is the trace. Proposition 3.5 shows that this is a field.

The smallest interesting case is $A(2, 6, 2, l, \mu)$, of order 2^{12}, where $\mu = \alpha^3 \in \mathbb{F}_{16}$ as before and $l \in L = \mathbb{F}_{64}$ has order 9 and $l^3 = \omega$. The presemifield product is

$$(x, y) = T(\mu(\overline{x}y^4 + l\overline{x}^4 y)) + T(xy)\mu.$$

Proposition 3.5 applies. The corresponding semifield has left and right nucleus $\mathbb{F}_4$ and middle nucleus $\mathbb{F}_{16}$. We do not know whether $A(2, 6, 2, l, \mu)$ is isotopic to a twisted field.

6 The semifields $B(p, m, s, l, n, N)$ and $C(p, m, s, l, R)$

For odd p we now rewrite the product (5.1) entirely in terms of L. This will allow us to generalize the presemifields $A(p, m, s, l, \mu)$.

Let F and L be as usual with p odd. Let $T(\omega) = 0 \neq \omega$, so that $n := \omega^2$ is a nonsquare in L^*, and $u \in F$ satisfies $T(\omega u) = 0$ if and only if $u \in L$. Identify F with L^2 via $(a,b) = a + b\omega$ and

$$(a,b)(c,d) = (ac + nbd, ad + bc) \tag{6.1}$$

whenever $a,b,c,d \in L$. Then $\overline{(a,b)} = (a,-b)$. For $x = a + b\omega = (a,b)$ we also write $a = \pi_{\mathfrak{R}}(x), b = \pi_{\mathfrak{I}}(x)$ (we think of these as the "real" and "imaginary" parts of x). If $\sigma = p^s$ then $(a,b)^\sigma = (a+b\omega)^\sigma = (a^\sigma, Nb^\sigma)$ where $N := \omega^{\sigma-1} \in L$.

Motivation. Let $x = (a,b), y = (c,d)$. Up to a constant factor, the presemifield multiplication in Theorem 5.2 is

$$x \star y = \big(\pi_{\mathfrak{I}}\big(\mu(\overline{x} \underset{A}{\circ} y), \pi_{\mathfrak{I}}(xy)\big).$$

By Theorem 5.2(ii), $\bar{\mu} \neq \mu$ and hence $\mu \notin L$. Then we may assume that $\mu = (nv, 1)$ by the second part of Lemma 5.4.

A straightforward calculation shows that the product is

$$(a,b) \star (c,d) = (h(a,b,c,d), ad + bc), \tag{6.2}$$

where

$$\begin{aligned} h(a,b,c,d) := \{[ac^\sigma - nNbd^\sigma] \,+\, l[a^\sigma c - nNb^\sigma d]\} \\ + nv\{[Nad^\sigma - bc^\sigma] \,\,+\, l[a^\sigma d - Nb^\sigma c]\}. \end{aligned} \tag{6.3}$$

This presemifield multiplication can be generalized:

Theorem 6.4. *Let $L = \mathbb{F}_{p^m}$ with p odd, $\sigma = p^s$ with $0 < s < m$, and $l, n, N \in L^*$, $v \in L$. Then (6.2) and (6.3) define a presemifield $X(p,m,s,v,l,n,N)$ if and only if*

(i) *$-l \notin L^{\sigma-1}$ and*

(ii) *the polynomial $t^{\sigma+1} - vt^\sigma - (v/N)t + 1/nN$ has no root $t \in L$.*

Proof. Assume (i), (ii), and that $(a,b)\star(c,d) = 0$ with $(a,b),(c,d) \neq 0$. If $a = 0$, then $bc = -ad = 0$ and $bd \neq 0$, in which case $nNbd^\sigma + lnNb^\sigma d = 0$ is impossible, by hypothesis.

If $a \neq 0$ then we may assume that $a = 1$ by homogeneity. Since $d = -bc$, we obtain $c \neq 0$ and

$$\begin{aligned} \{[c^\sigma - nNb(-bc)^\sigma] \,+\, l[c - nNb^\sigma(-bc)]\} \\ +nv\{[N(-bc)^\sigma - \, bc^\sigma] \,\,+\, l[(-bc) - Nb^\sigma c]\} = 0. \end{aligned}$$

This simplifies to $(c^\sigma + lc)\big(b^{\sigma+1} - vb^\sigma - (v/N)b + 1/nN\big) = 0$, which contradicts our hypotheses. The preceding argument reverses. $\square$

Notation. Denote by $K_1 = \mathbb{F}_{p^{\gcd(m,s)}} = \mathbb{F}_q \subseteq K_2 = \mathbb{F}_{p^{\gcd(m,2s)}}$ the fixed fields of σ and σ^2 in L.

Remark 6.5. *Let $K \subset L$ be a field extension in odd characteristic. We will repeatedly use the elementary fact that a non-square in K is a non-square in L provided $[L:K]$ is odd.*

Lemma 6.6. *If $k_b, k_c \in L^*$ then the presemifields $X(p,m,s,v,l,n,N)$ and $X(p,m,s,v/k_b, l/k_c^{\sigma-1}, nk_b^2, Nk_b^{\sigma-1})$ are isotopic; and both are isotopic to $X(p,m,m-s,v/N,1/l,nN^2,1/N)$.*

Proof. The first statement follows from the substitution

$$a' = a,\ b' = bk_b,\ c' = ck_c,\ d' = dk_d$$

$$l' = l/k_c^{\sigma-1},\ v' = v/k_b,\ n' = nk_b^2,\ N' = Nk_b^{\sigma-1}$$

where $k_d = k_b k_c$, giving the product $(h_{lvnN}(a',b',c',d'), a'd'+b'c') = (k_c^\sigma h_{l'v'n'N'}(a,b,c,d), k_b k_c(ad+bc))$. (N. B.–The condition in Theorem 6.4(ii) is unchanged: substitute $t \mapsto k_b t$ and divide by $k_b^{\sigma+1}$.)

Let $t = m - s, \tau = p^t$ and use the substitution

$$a' = a^\tau,\ b' = b^\tau,\ c' = c^\tau,\ d' = d^\tau,$$

$$v' = v/N,\ l' = 1/l,\ n' = nN^2,\ N' = 1/N.$$

Then

$$(h_{lvnN}(a',b',c',d'), a'd'+b'c') = (lh_{l'v'n'N'}, (ad+bc)^\sigma).$$

This proved the second claim. (This time the substitution $t \mapsto t^\tau$ shows that condition in Theorem 6.4(ii) again is unchanged.) □

The special case $k_b = 1$ shows in particular that l can be replaced by an arbitrary element of $lL^{*\sigma-1}$ without changing the isotopy type. Lemma 6.6 shows that all of the presemifields $X(p,m,s,v,l,n,N)$ in Theorem 6.4 are already isotopic to members of a significantly smaller subset:

Corollary 6.7. *Every presemifield $X(p,m,s,v,l,n,N)$ is isotopic to one of the following:*

(i) $B(p,m,s,l,n,N) = X(p,m,s,1,l,n,N)$, *where $0 < s < m$, $-l \notin L^{\sigma-1}$ and*

$$x^{\sigma+1} + (1-1/N)x + (1/n-1)/N \neq 0 \quad \text{for} \quad x \in L; \qquad (6.8)$$

or

(ii) $C(p,m,s,l,R) = X(p,m,s,0,l,n,N)$, *where* $0 < s < m, -l \notin L^{\sigma-1}, R = -nN \notin L^{\sigma+1}$.

Proof. These follow from the lemma; in Theorem 6.4(ii) we have substituted $t = x+1$ in order to obtain the polynomial in (6.8). □

Proposition 6.9. *$C(p,m,s,l,R)$ is isotopic to $C(p,m,s,l',R')$ for any $l' \in lL^{*\sigma-1}$, $R' \in RL^{*\sigma+1}$.*

$C(p,m,s,l,R)$ is isotopic to $C(p,m,m-s,1/l,R)$.

$B(p,m,s,l,n,N)$ is isotopic to $B(p,m,m-s,1/l,n,1/N^{1/\sigma})$, and l can be replaced by an arbitrary element of $lL^{*\sigma-1}$.

Proof. These follow from Lemma 6.6. □

Remark 6.10. There is a curious similarity between the polynomials in (6.8) and (4.1), with $g = 1-1/N$ and $f = (n-1)/nN$. However, the present presemifields depend on more parameters in L than Knuth's semifields.

7 The commutative case

Recall that all commutative presemifields are isotopic to commutative ones by (3.2) or (3.4).

7.1 The commutative C-family

Theorem 7.1. *$C(p,m,s,l,R)$ (where $-l \notin L^{\sigma-1}, R \notin L^{\sigma+1}$) is isotopic to a commutative semifield if and only if $l^{\sigma+1}R^{\sigma-1} \in L^{\sigma^2-1}$.*

Proof. Assume first that $l^{\sigma+1}R^{\sigma-1} \in L^{\sigma^2-1}$. Up to isotopy we may assume that $l^{\sigma+1}R^{\sigma-1} = 1$. (For, if $l^{\sigma+1}R^{\sigma-1} = z^{-(\sigma^2-1)}$ then we can use Proposition 6.9 to replace l by $lz^{\sigma-1}$, where $(lz^{\sigma-1})^{\sigma+1}R^{\sigma-1} = 1$.) Let $k = lR$. Then $k^\sigma = R/l$, and the substitution $a \mapsto kb$, $b \mapsto a$ transforms the presemifield multiplication of $C(p,m,s,l,R)$ in Corollary 6.7(ii) and (6.2) into $(h(kb,a,c,d), ac+kbd)$, where

$$h(kb,a,c,d) = Rad^\sigma + lRa^\sigma d + lRbc^\sigma + Rb^\sigma c.$$

Conversely, assume that $C(p,m,s,l,R)$ is isotopic to a commutative semifield. Recall the presemifield multiplication for $C(p,m,s,l,R)$:

$$(a,b)*(c,d) = (\underbrace{ac^\sigma + Rbd^\sigma + l[a^\sigma c + Rb^\sigma d]}_{h(a,b,c,d)}, ad+bc).$$

We use Corollary 3.9 with $v = (v_0, v_1)$. As $x * 1 = (a + la^\sigma, b)$, we have $\alpha(x) = (a', b)$ where $a' + la'^\sigma = a$. Further $v * x = (h(v_0, v_1, a, b), v_0 b + v_1 a)$ and $\alpha(v * x) = (h'(v_0, v_1, a, b), v_0 b + v_1 a)$, where h' is defined by

$$h'(a, b, c, d) + lh'(a, b, c, d)^\sigma = h(a, b, c, d) \tag{7.2}$$

The commutativity condition in Corollary 3.9 therefore becomes the two requirements

$$h(h'(v_0, v_1, a, b), v_0 b + v_1 a, c, d) = h(h'(v_0, v_1, c, d), v_0 d + v_1 c, a, b) \tag{7.3}$$
$$h'(v_0, v_1, a, b)d + v_0 bc + v_1 ac = h'(v_0, v_1, c, d)b + v_0 ad + v_1 ac. \tag{7.4}$$

Consider (7.4) as a function of c, d alone. Then $h'(v_0, v_1, c, d)$ has the form $h'(v_0, v_1, c, d) = f_{v_0,v_1} d + g_{v_0,v_1} c$, where we write $f_{v_0,v_1} = h'(v_0, v_1, a, b)/b - v_0 a/b)$ and $g_{v_0,v_1} = v_0$. Abbreviate this to $h'(c, d) = fd + g$ and use it in (7.2):

$$\begin{aligned} h'(c, d) + lh'(c, d)^\sigma &= lf^\sigma d^\sigma + fd + g + lg^\sigma \\ &= h = Rv_1 d^\sigma + lRv_1^\sigma d + v_0 c^\sigma + lv_0^\sigma c. \end{aligned}$$

Comparing coefficients of d and d^σ : $Rv_1 = lf^\sigma$, $lRv_1^\sigma = f$, which in case $v_1 \neq 0$ combine to $l^{\sigma+1} R^{\sigma-1} = 1/v_1^{\sigma^2-1}$, as desired. Assume $v_1 = 0$. Then $v_0 \neq 0, f = 0, h'(v_0, 0, c, d) = v_0 c$. Then (7.4) is satisfied, and (7.3) reads $h(v_0 a, v_0 b, c, d) = h(v_0 c, v_0 d, a, b)$ for all a, b, c, d, which is satisfied if and only if $l = 1/v_0^{\sigma-1}$. In this case we may assume that $l = 1$. The condition $-1 \notin L^{\sigma-1}$ implies $(p^m - 1)/(p^{\gcd(m,s)} - 1)$ odd, equivalently $m/\gcd(s, m)$ odd and therefore $L^{\sigma-1} = L^{\sigma^2-1}$. It follows $l^{\sigma+1} R^{\sigma-1} = R^{\sigma-1} \in L^{\sigma^2-1}$ as claimed. □

In particular, the C-family contains many semifields not isotopic to commutative ones. A small example occurs with $p = 3, m = 4$ and $l = R$ of order 16.

Notation. Denote by $v_2(n)$ the highest power of 2 dividing the integer n. The following is elementary:

Lemma 7.5. *For odd p we have $\gcd(p^m + 1, p^s + 1) = 2$ if $v_2(s) \neq v_2(m)$, whereas $\gcd(p^m + 1, p^s + 1) = p^{\gcd(m,s)} + 1$ if $v_2(s) = v_2(m)$.*

Lemma 7.6. *Let p be odd, $d = \gcd(s, m)$.*

(i) *If $v_2(d) = v_2(m)$, then $\gcd(2s, m) = d$, $\gcd(p^m - 1, p^s + 1) = 2$ and $L^{\sigma-1} \cap L^{\sigma+1} = L^{\sigma^2-1}$.*

(i) *If* $v_2(d) < v_2(m)$, *then* $\gcd(2s,m) = 2d$, $\gcd(p^m-1,p^s+1) = p^d+1$ *and* L^{σ^2-1} *has index* 2 *in* $L^{\sigma-1} \cap L^{\sigma+1}$.

Proof. The statements concerning $\gcd(2s,m)$ are obvious. Let $g = \gcd(p^m-1,p^s+1)$. Then g divides $\gcd(p^m-1,p^{2s}-1) = p^{\gcd(2s,m)}-1$. If $v_2(d) = v_2(m)$, then $\gcd(2s,m) = d$ and $g|p^d-1|p^s-1$. As g also divides p^s+1 it follows $g = 2$. Let $v_2(d) < v_2(m)$. Then $v_2(d) = v_2(s)$ and $g|(p^{2d}-1)$, which divides p^m-1. It follows $g = \gcd(p^{2d}-1,p^s+1)$. Lemma 7.5 shows $p^d+1|g$. Further $\gcd(p^d-1,p^s+1) = 2$ as $v_2(d) = v_2(s)$. This shows $g = p^d+1$.

Clearly $L^{\sigma^2-1} \leq L^{\sigma-1} \cap L^{\sigma+1}$. Let $a \in L^{\sigma-1} \cap L^{\sigma+1}$. Then $a^{\sigma+1} \in L^{\sigma^2-1}$ and $a^{\sigma-1} \in L^{\sigma^2-1}$. It follows $a^2 \in L^{\sigma^2-1}$. This shows $i = [L^{\sigma-1} \cap L^{\sigma+1} : L^{\sigma^2-1}] \leq 2$. Use the familiar formula $|L^{\sigma-1}| = (p^m-1)/\gcd(p^s-1,p^m-1)$ and analogous formulas for the other cyclic goups involved. We see that $i = 2$ if and only if both of $v_2(\gcd(p^m-1,p^s-1))$ and $v_2(\gcd(p^m-1,p^s+1))$ are smaller than $v_2(\gcd(p^m-1,p^{2s}-1))$. By what we saw above this is satisfied if and only if $v_2(d) < v_2(m)$. □

Lemma 7.7. *Let* $L = \mathbb{F}_{p^m}$ *with* p *odd,* $n \in L$ *a non-square,* $\sigma = p^s$, $0 \leq s < m$ *and* $d = \gcd(s,m)$. *Then*

(i) $-n^{(\sigma-1)/2} \in L^{\sigma-1}$ *if and only if* s/d *and* m/d *odd; and*

(ii) $n^{(\sigma-1)/2} \in L^{\sigma-1}$ *if and only if* s/d *even (*m/d *is then necessarily odd).*

Proof. (i) The first statement means that there is an element $x \in L$ such that $(n/x^2)^{(\sigma-1)/2} = -1$, or equivalently that there is a non-square $n' \in L$ such that $n'^{(\sigma-1)/2} = -1$. This is equivalent to $v_2(p^s-1) = v_2(p^m-1)$ and to both s/d and m/d being odd.

(ii) The proof is similar: an equivalent condition is $v_2(\sigma-1) > v_2(p^m-1)$, which is equivalent to

$$v_2(p^d-1) = v_2(p^m-1),\ v_2(p^d-1) < v_2(\sigma-1);$$

and these are equivalent to m/d odd and s/d even, respectively. □

Proposition 7.8. *Let* $d = \gcd(s,m)$. *The* C*-family of commutative presemifields in* Theorem 7.1 *splits into two subfamilies*:

(i) m/d *is odd,* $l = 1$ *and* R *is a non-square in* $K_1 = \mathbb{F}_{p^d}$, *and*

(ii) m/d *is even and the presemifield is* $C(p,m,s,1/\omega^{s-1},\omega^{s+1})$ *with* $s \leq m/2$.

Proof. As mentioned in the proof of Theorem 7.1, it may be assumed that $l^{\sigma+1}R^{\sigma-1}=1$. Let $Z=\{(l,R)|u(l,R):=l^{\sigma+1}=1/R^{\sigma-1},-l\notin L^{\sigma-1},R\notin L^{\sigma+1}\}$. Then $u(l,R)\in L^{\sigma-1}\cap L^{\sigma+1}$. Recall from Proposition 6.9 that l may be replaced by an arbitrary member of $lL^{*\sigma-1}$, and R may be replaced by an arbitrary element of $RL^{*\sigma+1}$ without changing the isotopy type. Concretely, if $(l,R)\in Z$, then $(lx^{\sigma-1},R/x^{\sigma+1})\in Z$ for arbitrary $0\neq x\in L$, $u(lx^{\sigma-1},R/x^{\sigma+1})=u(l,R)x^{\sigma^2-1}$ and $C(p,m,s,lx^{\sigma-1},R/x^{\sigma+1})$ is isotopic to $C(p,m,s,l,R)$. It follows that $u(l,R)\in L^{\sigma-1}\cap L^{\sigma+1}$ can be chosen arbitrarily in its coset mod L^{σ^2-1}. Now use Lemma 7.6.

If $v_2(d)=v_2(m)$ there is only one such coset and we may assume $u=1$. Then $l^{\sigma+1}=1$, and l is in the subgroup of order $\gcd(p^m-1,\sigma+1)=2$. As $l\neq -1$ it follows $l=1$. The condition $-1\notin L^{\sigma-1}$ translates as $m/\gcd(s,m)$ odd, and this implies that non-squares of K_1 are non-squares of L. As $R^{\sigma-1}=1$, it follows $R\in K_1$. The second condition on R is $R\notin L^{\sigma+1}$. By Lemma 7.6 we have $|L^{\sigma+1}|=(p^m-1)/\gcd(p^m-1,\sigma+1)=(p^m-1)/2$, which means that R is a non-square. Both conditions on R taken together are equivalent to R being a non-square in K_1. The choice of this non-square R is irrelevant up to isotopy.

Now consider the case $v_2(d)<v_2(m)$. There are two cosets of L^{σ^2-1} in $L^{\sigma-1}\cap L^{\sigma+1}$, see Lemma 7.6. Assume first that $u(l,R)=1$; we will see that this cannot occur. This time l is in the group of order $\gcd(p^m-1,\sigma+1)=p^d+1$. We have $\gcd(p^m-1,p^{2s}-1)=p^{2d}-1$. We can replace l by $l'=lx^{\sigma-1}$ provided $x^{\sigma^2-1}=1$. This means x is in the group of order $p^{2d}-1$ and $x^{\sigma-1}$ in the group of order p^d+1. We may therefore assume $l=1$, which forces $-1\notin L^{*\sigma-1}$, equivalently m/d odd, a contradiction to the current assumption.

It follows that $u=u(l,R)$ is a representative of the nontrivial coset of $L^{*\sigma^2-1}$ in $L^{*\sigma-1}\cap L^{*\sigma+1}$. We claim that $u=1/\omega^{\sigma^2-1}$ is a representative. In fact, clearly $u\in L^{*\sigma-1}\cap L^{*\sigma+1}$ and $u^2\in L^{\sigma^2-1}$. Assume $u\in L^{\sigma^2-1}$. As $n=\omega^2$ is a non-square in L, Lemma 7.7 implies m/d odd which contradicts our current assumption.

We have $u=1/\omega^{\sigma^2-1}$. As $l^{\sigma+1}=u$ it follows $l=x/\omega^{\sigma-1}$, where $x^{\sigma+1}=1$. As $\gcd(p^m-1,\sigma+1)=p^d+1$ there are p^d+1 choices for x. Up to isotopy we can replace l by ly where $y\in L^{\sigma-1}$ and $y^{\sigma+1}=1$. There are p^d+1 choices for y. It follows that we may assume $x=1$, equivalently $l=1/\omega^{\sigma-1}$. The necessary condition $-l\notin L^{\sigma-1}$ is equivalent to $m/d,s/d$ not both being odd. This is satisfied as $v_2(d)<v_2(m)$ (see Lemma 7.7). Similarly $R^{\sigma-1}=1/u=\omega^{\sigma^2-1}$ shows

$R = \omega^{\sigma+1}x$ where $x \in K_1$. Observe that $K_1 \subseteq L^{*\sigma+1}$ as follows from Lemma 7.6. Those choices for x therefore yield isotopic presemifields. We may choose $R = \omega^{\sigma+1}$. Assume the condition $\omega^{\sigma+1} \notin L^{\sigma+1}$ is not satisfied: $(\omega^2/x^2)^{(\sigma+1)/2} = 1$ for some $x \in L$. This means there is a non-square $\nu = \omega^2/x^2 \in L$ such that $\nu^{(\sigma+1)/2} = 1$ and therefore $v_2(\sigma+1) > v_2(p^m-1)$. However $\gcd(p^m-1, \sigma+1) = p^d+1$ by Lemma 7.6. It follows $v_2(p^d+1) = v_2(p^m-1)$ which is not true as $p^{2d}-1$ divides p^m-1. We have the uniquely determined semifields $C(p, m, s, 1/\omega^{\sigma-1}, \omega^{\sigma+1})$ where $s \leq m/2$, $v_2(d) < v_2(m)$. □

Notation. Denote the commutative semifields of Proposition 7.8 by $C_{p,m,s}$. There are $\lfloor m/2 \rfloor$ of them of order p^{2m}.

Proposition 7.9. *The first family of commutative semifields from* [5] *coincides with the family of semifields $C_{p,m,s}$ of* Proposition 7.8 *satisfying the additional condition that $p \equiv 1 \bmod 4$ if m/d is odd and s/m is even.*

We note that the latter additional condition is not needed for the existence of these semifields.

Proof. In [5] it is shown that $(bx)^{\sigma+1} - \overline{(bx)^{\sigma+1}} + \sum_{i=0}^{m-1} c_i(x\bar{x})^{p^i}$ is a planar function on $F = \mathbb{F}_{p^{2m}}$, where $b \in F^*, c_i \in L$, $y \rightarrow \sum_i c_i y^{p^i}$ describes an invertible linear mapping $L \rightarrow L$ and

$$(i)\ \gcd(m+s, 2m) = \gcd(m+s, m).$$
$$(ii)\ \gcd(p^s+1, p^m+1) \neq \gcd(p^s+1, (p^m+1)/2).$$

The substitution $x \mapsto x/b$ shows that it can be assumed that $b = 1$. Observe that $x^{\sigma+1} - \overline{x^{\sigma+1}} \in L\omega$, whereas $\sum_i c_i(x\bar{x})^{p^i} \in L$. Applying the identity to $L\omega$ and the inverse of the linear mapping to L, we obtain the planar function $x^{\sigma+1} - \overline{x^{\sigma+1}} + N(x)$ where $N\colon F \rightarrow L$ is the norm $N(x) = x\bar{x}$. After polarization the commutative presemifield multiplication can therefore be chosen as $x \circ y - \overline{x \circ y} + T(\overline{x}y)$, where $x \circ y = xy^\sigma + x^\sigma y$. This is based on the compatibility of $(\overline{x}y, L\omega)$ and $(x \circ y, L)$. In L-coordinates the presemifield multiplication is

$$(Nad^\sigma + bc^\sigma + a^\sigma d + Nb^\sigma c, ac - nbd)$$

where $n = \omega^2, N = n^{(\sigma-1)/2}$.

Condition (i) is equivalent to $v_2(s) \neq v_2(m)$, again equivalently: either m/d is even or s/d is even, and $\gcd(\sigma+1, p^m+1) \neq \gcd(\sigma+1, (p^m+1)/2)$ is equivalent to $v_2(\sigma+1) \geq v_2(p^m+1)$.

In terms of L-equations perform the substitution $a \mapsto b \mapsto -a/n$ and multiply the real part by $-n$. The multiplication which results is

$$(ac^\sigma - nNbd^\sigma + (N/n^{\sigma-1})a^\sigma c - nb^\sigma d, ad + bc).$$

This is precisely the multiplication in $C(p, m, s, 1/\omega^{\sigma-1}, -\omega^{\sigma+1}) = C_{p,m,s}$. For any s either itself or $m - s$ satisfies conditions (i) and (ii). If m/d is even, (ii) is automatically satisfied; if m/d odd and s/d even that condition is satisfied if and only if $p \equiv 1 \bmod 4$. □

The smallest member of the commutative C-family that is not contained in the first family of [5] has order 3^6. It is $C_{3,3,2} = C(3, 3, 2, 1, -1)$ with presemifield multiplication

$$(a, b) * (c, d) = (ad^9 + a^9d + bc^9 + b^9c, ac - bd).$$

Proposition 7.10. *The family from* [3, Theorem 1] *coincides with the set of* $C_{p,km',2k}$ *with* $m' > 1$ *odd.*

Proof. Let $\mathbb{F}_q \subset L = \mathbb{F}_{q^{m'}} \subset F = \mathbb{F}_{q^{2m'}}$ for odd q, $m' > 1$. The family from [3, Theorem 1] relies on the compatibility of $(xy, L\omega)$ and $(x \circ_A y, L)$, using $\sigma = q^2$. The presemifield product therefore uses $\pi_{\mathfrak{I}}(x \circ_A y)$ and $\pi_{\mathfrak{R}}(xy)$, hence can be written as

$$x * y = (Nad^\sigma + bc^\sigma + a^\sigma d + Nb^\sigma c, ac + nbd)$$

where $n = \omega^2, N = \omega^{\sigma-1}$ and $\omega \in \mathbb{F}_{q^2}$. The substitution $a \mapsto b, b \mapsto a/n$, followed by multiplying the real part by n transforms this into

$$(ac^\sigma + nNbd^\sigma + (1/N)(a^\sigma c + nNb^\sigma d), ad + bc)$$

which is the product of $C(p, km', 2k, 1/N, R)$ where $\sigma = q^2 = p^{2k}$, $N = \omega^{\sigma-1}$ and $R = nN = \omega^{\sigma+1}$. The condition $v_2(s) \neq v_2(m)$ is satisfied as $s = 2k$ and $m = km'$ and m' odd. The second condition $\omega^{\sigma+1} \notin L^{\sigma+1}$ is equivalent to $v_2(\sigma+1) \leq v_2(p^{km'} - 1)$. This is satisfied as $v_2(\sigma + 1) = 2$. We have $C(p, m'k, 2k, 1/N, R)$ where $m' > 1$ is odd and $N = \omega^{\sigma-1}, R$ a non-square. □

It had been shown in [17] that the family from [3, Theorem 1] is isotopic to a subfamily of [5].

7.2 Commutative B-families

Theorem 7.11. *$B(p, m, s, l, n, N)$ is isotopic to a commutative semifield if and only if there is $v = (v_0, v_1) \neq 0$ such that the following equations hold using $f = nv_0 + lnv_0^\sigma - lnNv_1^\sigma$:*

$$\begin{aligned} lf^\sigma &= nNv_0 + lnNv_0^\sigma - nNv_1 \\ v_0 &= lv_0^\sigma + nv_1 - lnNv_1^\sigma. \end{aligned}$$

In particular, these hold when either

(i) $N^2 = n^{\sigma-1}$, $l \in (1/N)L^{\sigma-1}$, *or*

(ii) $N = n^{\sigma-1}$, $l \in L^{\sigma-1}$.

Proof. We use Corollary 3.9. Here

$$x * 1 = (h(a, b, 1, 0), b) = (a + la^\sigma - n(b + lNb^\sigma), b).$$

Then $\alpha(x) = (a', b)$, where

$$a' + la'^\sigma = a + n(b + lNb^\sigma).$$

We have $v * x = (h(v_0, v_1, a, b), v_0b + v_1a)$ and

$$\alpha(v * x) = (h'(a, b), v_0b + v_1a),$$

where

$$h'(a, b) + lh'(a, b)^\sigma = h(a, b) + n(v_0b + v_1a + lN(v_0b + v_1a)^\sigma). \quad (7.12)$$

The left side of the condition in Corollary 3.9 is $\alpha(v * x) * y = (h(h'(a, b), v_0b + v_1a, c, d), h'(a, b)d + (v_0b + v_1a)c)$. The right side is obtained by switching the roles of x and y. This leads to the following two conditions:

$$h(h'(a, b), v_0b + v_1a, c, d) = h(h'(c, d), v_0d + v_1c, a, b) \quad (7.13)$$

$$h'(a, b)d + v_0bc = h'(c, d)b + v_0ad. \quad (7.14)$$

View the last equation as a function of d alone. This shows

$$h'(c, d) = (h'(a, b)/b - v_0a/b)d + v_0c.$$

Here $f = f_{v_0,v_1} = h'(a, b)/b - v_0a/b$ is a constant, depending only on v_0, v_1. Write $h'(c, d) = fd + v_0c, h'(a, b) = fb + v_0a$ and use 7.12:

$$(fd+v_0c)+l(fd+v_0c)^\sigma = h(v_0, v_1, c, d)+n(v_0d+v_1c+lN(v_0d+v_1c)^\sigma).$$

Comparing coefficients of d, d^σ, c, c^σ produces 3 equations, the coefficients of c, c^σ yielding the same equation. These are the relations given in the statement of the theorem. Assume that they are satisfied. Equation 7.14 is then satisfied. Equation 7.14 reads

$$h(fb + v_0a, v_0b + v_1a, c, d) = h(fd + v_0c, v_0d + v_1c, a, b)$$

Comparing coefficients this leads to 8 equations, all of which are automatically satisfied.

Let $v_0 = 0, v_1 \neq 0$. Then $f = -nv_1, v_1^{\sigma-1} = 1/(lN)$ (in particular $lN \in L^{\sigma-1}$). Comparison with lf^σ gives $N^2 = n^{\sigma-1}$.

In case $v_1 = 0$ the condition is $N = n^{\sigma-1}$ and $l = 1/v_0^{\sigma-1}$. □

Corollary 7.15. *The exceptional cases of* Theorem 7.11 *lead to the following families of commutative semifields:*

(1) $B(p, m, s, 1/\omega^{\sigma-1}, n, n^{(\sigma-1)/2})$, *where* $n \in L$ *a non-square and either* $m/\gcd(s, m)$ *or* $s/\gcd(s, m)$ *even.*

(2) $B(p, m, s, -1/\omega^{\sigma-1}, n, -n^{(\sigma-1)/2})$, *where* $n \in L$ *a non-square,* $s/\gcd(s, m)$ *odd.*

(3) $B(p, m, s, 1, v^2, v^{\sigma-1})$ *where* $0 \neq v \in L, m/\gcd(s, m)$ *odd.*

(4) $B(p, m, s, 1, n, n^{\sigma-1})$, *where* $m/\gcd(s, m)$ *odd.*

Proof. The first three cases subdivide Theorem 7.11(i). Observe that the variant when n is a square and $N = -n^{(\sigma-1)/2}$ does not occur as in this case $-l \in L^{\sigma-1}$. Recall that l may be replaced by an arbitrary member of its coset $lL^{*\sigma-1}$ (Proposition 6.9), so that we may choose $l = 1/N$ in the first three cases, $l = 1$ in the last. In the first case we may also choose $l = 1/\omega^{\sigma-1}$ or $l = \omega^{\sigma-1}$, in the second $l = -1/\omega^{\sigma-1}$ or $l = -\omega^{\sigma-1}$, and $l = 1$ in the last two cases. The conditions on $m/\gcd(s, m), s/\gcd(s, m)$ are equivalent to the condition $-l \notin L^{\sigma-1}$ from Corollary 6.7, see Lemma 7.7. □

Recall also that the members of the B-family need to satisfy the polynomial condition in Corollary 6.7. Whenever $m/\gcd(s, m)$ is odd we can choose the non-square $\omega^2 \in K_1$ and then $\omega^{\sigma-1} = -1$ (see the remark preceding Lemma 6.6). In the cases when $N^2 = n^{\sigma-1}, l = 1/N$, a commutative presemifield is obtained by the substitution $a \mapsto -nb, b \mapsto a$, which transforms the product to $\big(h(-nb, a, c, d), ac - nbd\big)$, where

$$-h(-nb, a, c, d) =$$
$$[nNad^\sigma + na^\sigma d + nbc^\sigma + nNb^\sigma c] + n\{ac^\sigma + a^\sigma c + nNbd^\sigma + nNb^\sigma d\}.$$

Proposition 7.16. *The second family of commutative semifields from* [5] *is contained in the union of the first family and the family from* Corollary 7.15(1).

Proof. The PN function constructed in [5] is

$$\beta x^{\sigma+1} + \overline{\beta x^{\sigma+1}} + \gamma N(x) + \sum_{i=0}^{m-1} r_i N(x)^{p^i},$$

where $\beta \in F$ is a non-square, $\gamma \notin L$, $r_i \in L$ and $\gcd(m+s, 2m) = \gcd(m+s, m)$. Up to isotopy we can choose $\gamma = \omega$. Apply the inverse of the linear mapping $a + b\omega \mapsto a + b\omega + \sum_i r_i b^{p^i}$. This produces the presemifield operation $\beta(x \circ y) + \overline{\beta(x \circ y)} + \omega T(\overline{x}y)$. This relies on the compatibility of $(\overline{x}y, L\omega)$ and $(\beta(x \circ y), L\omega)$, or equivalently, $(\omega xy, L)$ and $(\omega\beta(\overline{x} \circ y), L)$. Here $x \circ y = xy^\sigma + x^\sigma y$. The substitution $x \mapsto x/\omega$ produces $A(p, m, s, 1/\omega^{\sigma-1}, \beta)$ (see Theorem 5.2). The condition $\gcd(m+s, 2m) = \gcd(m+s, m)$ is equivalent to $v_2(s) \neq v_2(m)$, equivalently either $s/\gcd(s,m)$ or $m/\gcd(s,m)$ even and again equivalently $-1/\omega^{\sigma-1} \notin L^{\sigma-1}$ (see Lemma 7.7). This verifies the first condition of Theorem 5.2. The second condition is satisfied as β is a non-square. Because of isotopy we can write $\beta = vn + \omega$ for some $v \in L$, and our semifield is $X(p, m, s, v, 1/\omega^{\sigma-1}, \omega^2, \omega^{\sigma-1})$. The case $v = 0$ leads to the first family as considered in Proposition 7.9. Let $v \neq 0$. By Lemma 6.6, $X(p, m, s, v, 1/\omega^{\sigma-1}, \omega^2, \omega^{\sigma-1})$ is isotopic to

$$X(p, m, s, 1, 1/\omega^{\sigma-1}, \omega^2 v^2, \omega^{\sigma-1} v^{\sigma-1}) = B(p, m, s, 1/\omega^{\sigma-1}, \omega^2 v^2, \omega^{\sigma-1} v^{\sigma-1}).$$

□

In particular, we obtain a parametric description of the second family from [5]. In order to describe such a semifield of order p^{2m} the following have to be chosen:

- A representative s from $\{s, -s\}$ such that either m/d or s/d is even, where $d = \gcd(s, m)$. Let $\sigma = p^s$.
- An element $0 \neq v \in L = \mathbb{F}_{p^m}$ such that $\beta = v\omega^2 + \omega \in F$ is a non-square, equivalently: $N(\beta) = v^2\omega^4 - \omega^2 \in L$ is a non-square.
- The semifield is $X(p, m, s, v, 1/\omega^{\sigma-1}, \omega^2, \omega^{\sigma-1})$, which is isotopic to $B(p, m, s, 1/\omega^{\sigma-1}, \omega^2 v^2, \omega^{\sigma-1} v^{\sigma-1})$.

If m/d is odd, we can choose ω^2 as a non-square in $\mathbb{F}_{p^d}$ and obtain $\omega^{\sigma-1} = -1$.

We have not yet encountered an isotopy between semifields in different cases in Corollary 7.15. We therefore expect commutative semifields of types 2, 3 and 4 to be non-isotopic to members of the families from [5].

The semifield in Corollary 7.15(2) can be parametrized as $B(p, m, s, -1/\omega^{\sigma-1}, v^2\omega^2, -v^{\sigma-1}\omega^{s-1})$. The polynomial condition (6.8) reads

$$t^{\sigma+1} + (v^\sigma + v/\omega^{\sigma-1})t + v^2/\omega^{\sigma-1} - 1/\omega^{\sigma+1} \neq 0 \text{ for } t \in L.$$

Proposition 7.17. *Suppose that $m/\gcd(s, m)$ and $s/\gcd(s, m)$ are odd, $\omega^2 \in K_1$ is non-square and $v \in K_1$ is such that $v^2 - 1/\omega^2$ is a non-square. Then the presemifield $B(p, m, s, 1, (v\omega)^2, 1)$ is defined and is isotopic to a commutative semifield.*

Proof. This is contained in the family from Corollary 7.15(2). We have $\omega^2 \in K_1$ and therefore $\omega^{\sigma-1} = -1$. The polynomial condition simplifies to $v^2 - 1/\omega^2 \notin L^{\sigma+1}$. As $\gcd(p^m - 1, p^s + 1) = 2$ (see Lemma 7.6) this is satisfied. □

Consider Corollary 7.15(3) where $n = v^2$ is a square. The polynomial condition (6.8) reads

$$t^{\sigma+1} + (v^\sigma - v)t + 1 - v^2 \neq 0 \text{ for } t \in L.$$

Computer experiments suggest that there are many values of v which satisfy it. An easy way to obtain examples is to choose $v \in K_1$. The polynomial condition simplifies then to $v^2 - 1 \notin L^{\sigma+1}$. It follows from Lemma 7.6 that $\gcd(p^m-1, p^s+1) = 2$. The condition on v is therefore: $v^2 - 1$ is a non-square in K_1.

A similar procedure leads to the following parametric form of Corollary 7.15(4):

Theorem 7.18. *Let m/d odd and $0 \neq n \in L$ such that*

$$t^{\sigma+1} + (n^\sigma - n)t + n - n^2 \neq 0 \textit{ for } t \in L.$$

Then $B(p, m, s, 1, n, n^{\sigma-1})$ exists and is isotopic to a commutative semifield. The above polynomial condition is satisfied in particular when $n \in K_1$ and $1 - 1/n \in K_1$ is a non-square.

8 The nuclei of $B(p, m, s, l, n, N)$ and $C(p, m, s, l, R)$

First we handle a special case.

8.1 The semifields $C(p, 2k, k, l, R)$

The semifields $C(p, 2k, k, l, R)$ and $B(p, 2k, k, l, n, N)$ of order q^4 (where $q = p^k$) have $\sigma^2 = 1$ on L. Here we give a very explicit description of the presemifields $C(p, 2k, k, l, R)$, and use this to prove the

Proposition 8.1. *$\mathbb{N}_l = \mathbb{N}_r = \mathbb{F}_q$ and $\mathbb{N}_m = L = \mathbb{F}_{q^2}$ for $C(p, 2k, k, l, R)$.*

Proof. The conditions of Theorem 6.4 are: $N(l) := l^{q+1} \neq 1$ and $R \notin \mathbb{F}_q$. Write $\bar{a} = a^\sigma = a^q$ for $a \in L$. By (6.3),

$$h(a, b, c, d) = [a\bar{c} + Rb\bar{d}] + l[\bar{a}c + R\bar{b}d].$$

Let $x = (a, b), y = (c, d), z = (e, f)$. Then $1 * x = (\bar{a} + la, b), x * 1 = (a + l\bar{a}, b)$ and $\gamma(a, b) = (\bar{a}, b)$. A direct calculation, using the fact that the inverse of $\bar{x} + lx$ on L is $(\bar{x} - \bar{l}x)/(1 - N(l))$, leads to the explicit *semifield* multiplication

$$x \circ y = (ac + R_1\bar{b}d + R_2b\bar{d}, \bar{a}d + bc)$$

with $R_1 := \frac{\bar{R} - N(l)R}{1 - N(l)}$, $R_2 := \frac{\bar{l}(\bar{R} - R)}{1 - N(l)}$. Then

$$\begin{aligned} x \circ (y \circ z) &= \big(ace + R_1a\bar{d}f + R_2ad\bar{f} + R_1\bar{b}(\bar{c}f + de) + R_2b(c\bar{f} + \bar{d}\bar{e}), \\ &\qquad \bar{a}(\bar{c}f + de) + b(ce + R_1\bar{d}f + R_2d\bar{f})\big) \\ (x \circ y) \circ z &= \big(ac + R_1\bar{b}d + R_2b\bar{d})e + R_1(a\bar{d} + \bar{b}\bar{c})f + R_2(\bar{a}d + bc)\bar{f}, \\ &\qquad (\bar{a}\bar{c} + \bar{R}_1b\bar{d} + \bar{R}_2\bar{b}d)f + (\bar{a}d + bc)e\big). \end{aligned}$$

Therefore $x \circ (y \circ z) = x \circ y) \circ z$ is equivalent to

$$(a - \bar{a})d\bar{f} = b\bar{d}(e - \bar{e}) \text{ and } (R_1 - \bar{R}_1)b\bar{d}f = \bar{R}_2\bar{b}df - R_2bd\bar{f}.$$

It follows easily that the nuclei are as stated. □

Applying a suitable Knuth operation [15, Sec. 4] to $C(p, 2k, k, l, R)$ produces a semifield with left nucleus of order q^2 that is a lifting of a Desarguesian plane [6, (8)].

8.2 The generic case: preliminaries

In odd characteristic, define $(a,b)*(c,d)$ by (6.2) and (6.3). This describes $B(p,m,s,l,n,N)$ (case $v=1$) and $C(p,m,s,l,R)$ (case $v=0$, where $R=-nN$). We wish to determine the nuclei. Recall that $\sigma \neq 1$ on L.

Let $x=(a,b), y=(c,d), z=(e,f)$. We use the formulas

$$\begin{aligned} 1*x &= (h(1,0,a,b),b) = (a^\sigma + la + nv(Nb^\sigma + lb), b) \\ x*1 &= (h(a,b,1,0),b) = (a + la^\sigma - nv(b + lNb^\sigma), b) \end{aligned}$$

in order to calculate the functions β, γ given in (3.3). Proposition 3.5 provides the semifield product $x \circ y = \beta(\gamma(x)*y)$, where $\gamma(x)=(V,b)$ with

$$V + lV^\sigma - nv(b + lNb^\sigma) = a^\sigma + la + nv(Nb^\sigma + lb) \tag{8.2}$$

and $\beta(x)=(V',b)$ with

$$V'^\sigma + lV' + nv(Nb^\sigma + lb) = a. \tag{8.3}$$

Also $\gamma(y)=(W,d)$ with

$$W + lW^\sigma - nv(d + lNd^\sigma) = c^\sigma + lc + nv(Nd^\sigma + ld). \tag{8.4}$$

Lastly, define k and M by

$$\begin{aligned} k + lk^\sigma - nv(Vd + bc + lN(Vd+bc)^\sigma) &= h(V,b,c,d) \qquad (8.5) \\ M^\sigma + lM + nv(N(Wf+de)^\sigma + l(Wf+de)) &= h(W,d,e,f). \qquad (8.6) \end{aligned}$$

Note that all of the definitions (8.2)–(8.6) use the fact that $x \to x + lx^\sigma$ is bijective on L by Theorem 6.4(i). In terms of the notation (8.2)–(8.6) we have the following

Lemma 8.7. *The equation $x \circ (y \circ z) = (x \circ y) \circ z$ is equivalent to the following system*:

$$\begin{aligned} bM &= bce + (k - VW)f \qquad (8.8) \\ h(k, Vd + bc, e, f) &= h(V, b, M, Wf + de). \qquad (8.9) \end{aligned}$$

Proof. By (3.4), $x \circ (y \circ z) = (x \circ y) \circ z$ is equivalent to

$$\gamma(x \circ y) * z = \gamma(x) * (y \circ z). \tag{8.10}$$

Since

$$\gamma(x) * y = (V,b)*(c,d) = (h(V,b,c,d), Vd + bc)$$

we have $x \circ y = (m, Vd + bc)$, where $m^\sigma + lm + nv(N(Vd + bc)^\sigma + l(Vd + bc)) = h(V, b, c, d)$. Then $\gamma(x \circ y) = (k, Vd + bc)$ by (8.5).

Also $\gamma(y) * z = (W, d) * (e, f) = (h(W, d, e, f), Wf + de)$, so that $y \circ z = (M, Wf + de)$ by (8.6).

Now (8.10) becomes $(k, Vd + bc) * (e, f) = (V, b) * (M, Wf + de)$, and comparison of coordinates completes the proof. □

Corollary 8.11. *If $x \circ (y \circ z) = (x \circ y) \circ z$ for some $x = (a, b),\ b \neq 0$, some y and all z, then*

$$\begin{aligned} W &= c^\sigma + nv(d + Nd^\sigma) \\ W^\sigma &= c \ \ + nv(d + Nd^\sigma) \end{aligned} \tag{8.12}$$

$$\begin{aligned} k &= VW + nvb(c - c^\sigma) - nNbd^\sigma \\ k^\sigma &= (VW)^\sigma + nvNb^\sigma(c^\sigma - c) - nNb^\sigma d. \end{aligned} \tag{8.13}$$

In particular,

$$c^\sigma - c = W - W^\sigma \tag{8.14}$$

$$c - c^{\sigma^2} = (nv(d + Nd^\sigma))^\sigma - nv(d + Nd^\sigma) \tag{8.15}$$

$$(nv)^\sigma(c - c^\sigma)^\sigma + nvN(c - c^\sigma) = (nN)^\sigma d^{\sigma^2} - nNd. \tag{8.16}$$

Proof. As $b \neq 0$, (8.8) yields $M = ce + ((k - VW)/b)f$. By definition, V, W, k depend only on a, b, c, d not e or f. Then (8.6) yields (8.12)–(8.13) by comparing coefficients of e, e^σ, f, f^σ and using the facts that $e, f \in L$ are arbitrary and $\sigma \neq 1$ on L. Now (8.14)–(8.16) are immediate by (8.12)–(8.13). □

Later we will need the identities

$$\begin{aligned} &h(ea, eb, c, d) - eh(a, b, c, d) \\ &\qquad = l(e^\sigma - e)\{(a^\sigma c - nNb^\sigma d) + nv(a^\sigma d - Nb^\sigma c)\} \end{aligned} \tag{8.17}$$

$$\begin{aligned} &h(a, b, ec, ed) - eh(a, b, c, d) \\ &\qquad = (e^\sigma - e)\{(ac^\sigma - nNbd^\sigma) + nv(Nad^\sigma - bc^\sigma)\}. \end{aligned} \tag{8.18}$$

8.3 Left and right nuclei

By (6.3), $(a, 0) * (c, 0) = (ac^\sigma + la^\sigma c, 0)$, so there is a twisted field induced on $(L, 0)$. *We identify the set $(L, 0)$ with L.* By (3.3) and (3.4), $(L, +, \circ)$ is a semifield associated with this twisted field.

Let $K_1 = \mathbb{F}_q$ and K_2 denote the respective fixed fields of σ and σ^2 in L. We frequently identify these with $(K_1, 0)$ and $(K_2, 0)$, respectively. These will be significant for calculating the nuclei. First we note the

Lemma 8.19. *K_1 is in the center of $(F,+,\circ)$.*

Proof. Apply Proposition 3.5(i). $\square$

We will need the nuclei of the twisted field L [2, Theorem 1]:

$$\begin{array}{l}\textit{If } \sigma^2 \neq 1 \textit{ on } L \textit{ then } K_2 \textit{ is the middle nucleus of } (L,+,\circ) \\ \textit{while } K_1 \textit{ is both the left and right nucleus.} \\ \textit{If } \sigma^2 = 1 \textit{ on } L \textit{ then } (L,+,\circ) \textit{ is a field.}\end{array} \tag{8.20}$$

Theorem 8.21. *The semifields $B(p,m,s,l,n,N)$ and $C(p,m,s,l,R)$ have left and right nucleus $K_1 \subset L$.*

Proof. By Lemma 8.19, K_1 is in both of these nuclei.

Case $\sigma^2 = 1$ on L. We need only consider $B(p,2k,k,l,n,N)$ in view of Proposition 8.1. Recall $q = p^k$. Let $(a,b) \in \mathbb{N}_l$

First suppose that $b \neq 0$. Then (8.15) yields $n(d+Nd^q) = (n(d+Nd^q))^q$ for all d, and hence $N = n^{q-1}$. Then $N = 1$ by (8.16), which contradicts Theorem 6.4(ii). Thus $\mathbb{N}_l \subseteq L$.

Similarly, $\mathbb{N}_r \subseteq L$.

Assume that $(a,0) \in \mathbb{N}_l$. Then (8.8) gives $k = VW$, while (8.2) gives $V = a^q$ since $-l \notin L^{\sigma-1}$. Rewrite (8.6) and (8.9):

$$V(M^q + lM) = Vh(W,d,e,f) - Vn\{N(Wf+de)^q + l(Wf+de)\}$$
$$VM^q + lV^qM = h(VW,Vd,e,f) - n\{NV(Wf+de)^q + lV^q(Wf+de)\}.$$

We claim that $V^q = V$ and hence $a^q = a$. For if not, subtract, use (8.17), factor out $l(V - V^q)$, and then use (8.6) again to get

$$\begin{aligned} M &= \{W^q - n(d+Nd^q)\}e - n\{(W-W^q) + Nd^q\}f \\ M^q &= \{W - n(d+Nd^q)\}e^q - nN\{(W^q - W) + d\}f^q. \end{aligned}$$

Compare these: the coefficient of e^q shows $N = n^{q-1}$, and the coefficient of f^q yields $n \in K_1 = \mathbb{F}_q$. Then $N = 1$, which again contradicts Theorem 6.4(ii).

Finally, assume that $(e,0) \in \mathbb{N}_r$. *We claim that $e^q = e$.* For otherwise, (8.8) shows $M = ce$. Comparison with (8.6) shows

$$We^q + lW^qe = (ce)^q + lce + n\{de^q + N(de)^q + lde + lNd^qe\}.$$

Comparison with (8.4) produces(8.12). This implies that $N = n^{q-1}$. Rewrite (8.5) and (8.9) as

$$\begin{aligned} ek + elk^q &= eh(V,b,c,d) + en\{(Vd+bc) + lN(Vd+bc)^q\} \\ ke^q + lk^qe &= h(V,b,ce,de) + n\{(Vd+bc)e^q + lN(Vd+bc)^qe\}. \end{aligned}$$

Subtract, use (8.18) and divide by $e^q - e$:

$$k = Vc^q - nNbd^q + n(NVd^q + Vd - bc^q + bc).$$

Then (8.5) implies that

$$k^q = V^q c - nNb^q d + n(V^q d - Nb^q c + N(Vd + bc)^q\}.$$

Comparison yields the usual contradiction $N = n^{q-1} = 1$, which finally proves our claim.

Case $\sigma^2 \neq 1$ **on** L. By Lemma 8.19 and (8.20), $\mathbb{N}_l \cap L = \mathbb{N}_r \cap L = K_1$. We must show that $\mathbb{N}_l$ and $\mathbb{N}_r$ are in L.

Assume that $(a, b) \in \mathbb{N}_l$ with $b \neq 0$. Choosing $d = 0$ in (8.15) shows that $c \in K_2$. Since c is arbitrary, we have $K_2 = L$ and hence $\sigma^2 = 1$ on L, which is not the case. Thus, $\mathbb{N}_l \subseteq (L, 0)$, as required.

Assume that $(e, f) \in \mathbb{N}_r$ with $f \neq 0$. Since $\gamma(x) = (V, b)$, $c, d, b, V \in L$ are arbitrary. Then (8.8) yields $k = VW + \big((M - ce)/f\big)b$. As in the proof of Lemma 8.11, comparison of the coefficients of V, V^σ, b and b^σ in (8.5) yields four equations. Two of these are (8.12), which we compare and choose $d = 0$ in order to deduce that $\sigma^2 = 1$ on L, which is not the case. □

8.4 Middle nucleus

Our results for the middle nucleus are not as satisfactory as for the left and right nuclei. We start by identifying the middle nucleus in terms of field equations.

Lemma 8.22. *$(c, d) \in \mathbb{N}_m$ if and only if (8.15) and (8.16) hold.*

Proof. Let $(c, d) \in \mathbb{N}_m$. Choosing $b \neq 0$ yields (8.12)–(8.16).

Conversely, assume that (8.15) and (8.16) hold. If $\tilde{W} := c^\sigma + nv(d + Nd^\sigma)$, then (8.15) implies that both parts of (8.12) hold with W replaced by $\tilde{W}$. Then (8.4) holds with W replaced by $\tilde{W}$, so the uniqueness of W in the definition (8.4) implies that $\tilde{W} = W$: (8.12) holds. The same reasoning yields (8.13).

In order to show that $(c, d) \in \mathbb{N}_m$ we need to prove that (8.8) and (8.9) are satisfied for all V, b, e, f.

Assume at first $b \neq 0$. Let $\tilde{M} := ce + \big((k - VW)/b\big)f = ce + \big(nv(c - c^\sigma) - nNd^\sigma\big)f$ (using (8.13)). Then (8.6) holds with $\tilde{M}$ in place of M, and hence $\tilde{M} = M$ and (8.8) is satisfied. We now have $W, W^\sigma, k, k^\sigma, M$, and a calculation produces (8.9). (In fact, $h(k, Vd+$

$bc, e, f) - h(V, b, M, Wf + de)$ is a linear combination of e, e^σ, f, f^σ with coefficients depending only on V, b, c, d, and a straightforward calculation shows that all four coefficients vanish.)

Finally, let $b = 0$. Then $k = VW$ by (8.4), so that (8.8) holds. As above, $M = ce + \big(nv(c - c^\sigma) - nNd^\sigma\big)f$ follows from (8.6), and then (8.9) follows easily. □

Theorem 8.23. (i) *For $C(p, m, s, l, R)$, $\mathbb{N}_m$ is K_2 if $R \notin K_1^* L^{*\sigma+1}$, and a quadratic extension of K_2 otherwise.*

(ii) *For $B(p, m, s, l, n, n^{\sigma-1})$, $\mathbb{N}_m$ is K_2 if $1 - 1/n \notin K_1^* L^{*\sigma+1}$ and a quadratic extension of K_2 otherwise.*

(iii) *For $B(p, m, s, l, n, N)$ with $N \neq n^{\sigma-1}$, $\mathbb{N}_m \cap L = K_1$.*

(iv) *For $B(p, 2k, k, l, n, N)$ with $N \neq n^{\sigma-1} = n^{q-1}$, $\mathbb{N}_m$ is a quadratic extension of $K_1 = \mathbb{F}_q$.*

Proof. (i) Here $v = 0$, $R = -nN \notin L^{\sigma+1}$ by Corollary 6.7(ii). Then (8.15) yields $c \in K_2$, hence $\mathbb{N}_m \cap L \subseteq K_2$.

Assume that $d \neq 0$. Then (8.16) yields $d^{\sigma^2-1} = 1/(nN)^{\sigma-1} = 1/R^{\sigma-1}$, or equivalently $d^{\sigma+1}R \in K_1^*$. There is a solution $d \in L^*$ if and only if $R \in K_1^* L^{*\sigma+1}$. Any two solutions d_1, d_2 satisfy $(d_1/d_2)^{\sigma^2-1} = 1$ and hence $d_1/d_2 \in K_2$. Thus, $|\mathbb{N}_m| = |K_2|^2$ and $\mathbb{N}_m$ has basis $\{(1, 0), (0, d_0)\}$ over K_2, where d_0 is such that $R \in d_0^{\sigma+1} K_1$.

(ii) Let $v = 1, nN = n^\sigma$. If $d = 0$, then (8.15) yields $c \in K_2$ and (8.16) implies $\mathbb{N}_m \cap L = K_2$.

Suppose that $d \neq 0$. Then (8.15) simplifies to $c - c^{\sigma^2} = (nd)^{\sigma^2} - nd$, equivalently $c = -nd + t$ where $t \in K_2 \subseteq \mathbb{N}_m$. We may thus assume that $c = -nd$. Now (8.16) states that $n^\sigma(c - c^\sigma) = (nd)^{\sigma^2} - n^\sigma d$. Using $c = -nd \neq 0$, this simplifies to $(dn)^{\sigma^2-1} = (1 - 1/n)^{1-\sigma}$, or equivalently $(dn)^{\sigma+1}(1 - 1/n) \in K_1$. A solution $d \in L^*$ exists if and only if $1 - 1/n \in K_1^* L^{*\sigma+1}$, and any two solutions d_1, d_2 satisfy $d_1/d_2 \in K_2$. Once again this implies that $\mathbb{N}_m$ is a quadratic extension of K_2.

(iii) Use Lemma 8.22 with $d = 0$.

(iv) Let $(c, d) \in \mathbb{N}_m$. Write $\bar{a} = a^\sigma = a^q$ for $a \in L$. Conditions (8.15) and (8.16) state that $n(d + N\bar{d}) \in \mathbb{F}_q$ and $\bar{n}(\bar{c} - c) + nN(c - \bar{c}) = \bar{n}\bar{N}d - nNd$. If $d = 0$ then $c \in \mathbb{F}_q$.

Suppose that $d \neq 0$. Then $\bar{d}/d = (\bar{n} - nN)^{q-1}$, hence $d = (\bar{n} - nN)t, t \in K_1$. Also, $\bar{c} - c = (\bar{n}\bar{N} - nN)t$ and $c = nNs, s \in K_1$. It follows that $\mathbb{N}_m$ is 2-dimensional over K_1, with basis $\{(1, 0), (nN, \bar{n} - nN)\}$. □

We now assume that $\sigma^2 \neq 1$ on L and, until Proposition 8.29, also that $n^{\sigma-1} \neq N^2$. Let $\mathbb{W}$ denote the kernel of the K_1-linear map $t \to (1+n\alpha_0)t + (1+n\alpha_1+nN\alpha_0^\sigma)t^\sigma + (n\alpha_2+nN\alpha_1^\sigma)t^{\sigma^2} + nN\alpha_2^\sigma t^{\sigma^3}$, where

$$\begin{aligned} \alpha_0 &= \frac{n^\sigma - n^2N^2}{n(nN^2-n^\sigma)} \\ \alpha_1 &= \frac{n^\sigma + n^2N^2 - nN - n^{\sigma+1}N}{n(nN^2-n^\sigma)} \\ \alpha_2 &= \frac{nN(n^\sigma-1)}{n(nN^2-n^\sigma)}. \end{aligned} \tag{8.24}$$

Theorem 8.25. $\dim_{K_1}\mathbb{N}_m = 1 + \dim_{K_1}\mathbb{W} \leq 4$ *if* $n^{\sigma-1} \neq N, N^2$ *and* $\sigma^2 \neq 1$.

Proof. First note that (8.15) is equivalent to $c+c^\sigma+n(d+Nd^\sigma) \in K_1$. For, if $\alpha := n(d+Nd^\sigma)$ then $\alpha^\sigma - \alpha = c - c^{\sigma^2}$ and hence $\alpha^{\sigma^2} - \alpha = (c-c^\sigma) - (c-c^\sigma)^{\sigma^2}$. Then $e := \alpha + c + c^\sigma \in K_2$. Substituting $\alpha = -c - c^\sigma + e$ in (8.15) yields $e \in K_1$.

Since $\mathbb{N}_m \cap L = (K_1, 0)$ by Lemma 8.19 and (8.20) (as $\sigma^2 \neq 1$ on L), we may assume that $e = 0$. Thus, we are left to consider the K_1-space $\mathbb{M}$ of pairs $(c,d) \in L^2$ satisfying

$$d^\sigma = -d/N - (c+c^\sigma)/(nN) \tag{8.26}$$

$$(nN)^\sigma d^{\sigma^2} = nNd + n^\sigma(c-c^\sigma)^\sigma + nN(c-c^\sigma). \tag{8.27}$$

It is easy to check that $\mathbb{M} \cap (K_1, 0) = 0$, so that $\dim \mathbb{N}_m = \dim \mathbb{M} + 1$. Therefore, *it remains to prove that* $\dim_{K_1}\mathbb{M} = \dim_{K_1}\mathbb{W}$.

If (8.26) holds then (8.27) is equivalent to

$$\begin{aligned} n(nN^2-n^\sigma)d = {} & \big(n^\sigma - n^2N^2\big)c \\ & +(n^\sigma + n^2N^2 - nN - n^{\sigma+1}N)c^\sigma + nN(n^\sigma-1)c^{\sigma^2}. \end{aligned} \tag{8.28}$$

Then $d = \alpha_0 c + \alpha_1 c^\sigma + \alpha_2 c^{\sigma^2}$ with α_i in (8.24). Substituting this into (8.26) shows that $c \in \mathbb{M}$ whenever $(c,d) \in \mathbb{W}$, and this argument reverses. □

Note that we could have allowed $n^{s-1} = N$ in the above argument, but that case was already handled in Theorem 8.23(ii).

Proposition 8.29. *If* $n^{\sigma-1} = N^2$ *and* $\sigma^2 \neq 1$, *then* $1 \leq \dim_{K_1}\mathbb{N}_m \leq 3$.

Proof. This time the left side of (8.28) is 0, so that (8.28) describes a space of solutions c of K_1-dimension at most 2. For each c there are 0 or $|K_1|$ possible d in (8.26). Hence, even allowing d to be 0, the number of possible (c, d) is at most $|K_1|^3$. □

Recall from the Motivation at the start of Section 6 that $N = n^{(\sigma-1)/2}$ was one of the assumptions in Theorem 5.2.

References

[1] A. A. Albert, Finite division algebras and finite planes, pp. 53–70 in: AMS Proc. Symp. Appl. Math. 10 (1960).

[2] A. A. Albert: *Generalized twisted fields, Pacific Journal of Mathematics* **11** (1961) 1–8.

[3] J. Bierbrauer: *Commutative semifields from projection mappings, Des. Codes Cryptogr.* **61** (2011) 187-196.

[4] L. Budaghyan and C. Carlet: *Classes of quadratic APN trinomials and hexanomials and related structures, IEEE IT Transactions* **54** (2008) 2354–2357.

[5] L. Budaghyan and T. Helleseth: *New commutative semifields defined by new PN multinomials, Cryptogr. Commun.* **3** (2011), 1-16.

[6] I. Cardinali, O. Polverino and R. Trombetti: *Semifield planes of order q^4 with kernel $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$, European Journal of Combinatorics* **27** (2006) 940–961.

[7] P. Dembowski, Finite Geometries. Springer, Berlin–Heidelberg–NY 1968.

[8] L. E. Dickson, On finite algebras. Göttinger Nachrichten (1905) 358–393.

[9] M. J. Ganley, Polarities in translation planes. Geom. Ded. 1 (1972) 103–116.

[10] D. R. Hughes and E. Kleinfeld, Seminuclear extensions of Galois fields. Amer. J. Math. 82 (1960) 389–392.

[11] D. R. Hughes and F. C. Piper, Projective planes. Springer, New York-Berlin 1973.

[12] W. M. Kantor, Commutative semifields and symplectic spreads. J. Algebra 270 (2003) 96–114.

[13] W. M. Kantor, Finite semifields, pp. 103–114 in: Finite Geometries, Groups, and Computation (Proc. of Conf. at Pingree Park, CO Sept. 2005), de Gruyter, Berlin-New York 2006.

[14] I. Kaplansky, Infinite-dimensional quadratic forms admitting composition. PAMS 4 (1953) 956–960.

[15] D. E. Knuth: *Finite semifields and projective planes, J. Algebra* **2** (1965) 182-217.

[16] G. Lunardon, G. Marino, O. Polverino and R. Trombetti: *Symplectic semifield spreads of $PG(5, q)$ and the Veronese surface,* Ric. Mat. 60 (2011) 125–142.

[17] G. Marino and O. Polverino: *On isotopisms and strong isotopisms of commutative presemifields,* to appear in J. Alg. Comb.

[18] O. Veblen and J. H. Maclagan-Wedderburn, Non-desarguesian and non-pascalian geometries. TAMS 8 (1907) 379–388.

[19] Z. Zha and X. Wang: *New families of perfect nonlinear polynomial functions, J. Algebra* 322 (2009) 3912–3918.