Available online at www.sciencedirect.com
SciVerse ScienceDirect
Advances in Mathematics 234 (2013) 43–60
ADVANCES IN Mathematics
www.elsevier.com/locate/aim

A new family of semifields with 2 parameters

Yue Zhou[a,b], Alexander Pott[a,*]

[a] *Faculty of Mathematics, Otto-von-Guericke-University Magdeburg, 39106 Magdeburg, Germany*
[b] *Department of Mathematics and System Sciences, Science College, National University of Defense Technology, Changsha, 410073, PR China*

Received 17 December 2010; accepted 22 October 2012
Available online 17 November 2012

Communicated by Michel Van den Bergh

Abstract

A new family of commutative semifields with two parameters is presented. Its left and middle nucleus are both determined. Furthermore, we prove that for different pairs of parameters, these semifields are not isotopic. It is also shown that, for some special parameters, one semifield in this family can lead to two inequivalent planar functions. Finally, using a similar construction, new APN functions are given.

MSC: 12K10; 51A35; 51A40

Keywords: Commutative semifield; Isotopism; Planar function; Projective plane

1. Introduction

A *semifield* $\mathbb{S}$ is an algebraic structure satisfying all the axioms of a skewfield except (possibly) associativity. In other words, it satisfies the following axioms:

- $(\mathbb{S}, +)$ is a group, with identity element 0;
- $(\mathbb{S} \setminus \{0\}, *)$ is a quasigroup;
- $0 * a = a * 0 = 0$ for all a;

* Corresponding author.
E-mail addresses: yue.zhou@st.ovgu.de (Y. Zhou), alexander.pott@ovgu.de (A. Pott).

0001-8708/$ - see front matter
doi:10.1016/j.aim.2012.10.014

- The left and right distributive laws hold, namely for any $a, b, c \in \mathbb{S}$,

$$(a+b)*c = a*c + b*c,$$
$$a*(b+c) = a*b + a*c.$$

- There is an element $e \in \mathbb{S}$ such that $e*x = x*e = x$ for all $x \in \mathbb{S}$.

A finite field is a trivial example of a semifield. Furthermore, if $\mathbb{S}$ does not necessarily have a multiplicative identity, then it is called a *presemifield*. A semifield is not necessarily commutative or associative. However, by Wedderburn's Theorem [34], in the finite case, associativity implies commutativity. Therefore, a non-associative finite commutative semifield is the closest algebraic structure to a finite field.

In the earlier literature, semifields were also called *division rings* or *distributive quasifields*. The study of semifields was initiated by Dickson, see [22], shortly after the classification of finite fields. Semifields have become an attracting topic in many different areas of mathematics, such as difference sets, coding theory and finite geometry.

Dickson constructed the first non-trivial semifields in [22]. In [29], Knuth showed that the additive group of a semifield $\mathbb{S}$ is an elementary abelian group, and the additive order of the nonzero elements in $\mathbb{S}$ is called the characteristic of $\mathbb{S}$. Hence, any finite semifield can be represented by $(\mathbb{F}_{p^n}, +, *)$. Here $(\mathbb{F}_{p^n}, +)$ is the additive group of the finite field $\mathbb{F}_{p^n}$ and $x * y = \varphi(x, y)$, where φ is a mapping from $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$.

On the other hand, there is a well-known correspondence, via coordinatization, between semifields and projective planes of Lenz–Barlotti type V.1; see [28]. In [2], Albert showed that two semifields coordinatize isomorphic planes if and only if they are isotopic (isotopism can also be defined between presemifields):

Definition 1. Let $\mathbb{S}_1 = (\mathbb{F}_{p^n}, +, *)$ and $\mathbb{S}_2 = (\mathbb{F}_{p^n}, +, \star)$ be two presemifields. If there exist three bijective linear mapping $L, M, N : \mathbb{F}_p^n \to \mathbb{F}_p^n$ such that

$$M(x) \star N(y) = L(x * y)$$

for any $x, y \in \mathbb{F}_{p^n}$, then $\mathbb{S}_1$ and $\mathbb{S}_2$ are called *isotopic*, and the triple (M, N, L) is an *isotopism* between $\mathbb{S}_1$ and $\mathbb{S}_2$. Furthermore, if there exists an isotopism of the form (N, N, L) between $\mathbb{S}_1$ and $\mathbb{S}_2$, then $\mathbb{S}_1$ and $\mathbb{S}_2$ are *strongly isotopic*.

Let $\mathbb{P} = (\mathbb{F}_{p^n}, +, *)$ be a presemifield, and $a \in \mathbb{P}$. If we define a new multiplication $\star$ by the rule

$$(x * a) \star (a * y) = x * y,$$

we have $(a*a)\star(a*x) = a*x$ and $(x*a)\star(a*a) = x*a$, namely $(\mathbb{F}_{p^n}, +, \star)$ is a semifield with unit $a * a$. There are many semifields associated with a presemifield, but they are all isotopic.

Let $\mathbb{S} = (\mathbb{F}_{p^n}, +, *)$ be a semifield. The subsets

$$N_l(\mathbb{S}) = \{a \in \mathbb{S} : (a*x)*y = a*(x*y) \text{ for all } x, y \in \mathbb{S}\},$$
$$N_m(\mathbb{S}) = \{a \in \mathbb{S} : (x*a)*y = x*(a*y) \text{ for all } x, y \in \mathbb{S}\},$$
$$N_r(\mathbb{S}) = \{a \in \mathbb{S} : (x*y)*a = x*(y*a) \text{ for all } x, y \in \mathbb{S}\},$$

are called the *left, middle* and *right nucleus* of $\mathbb{S}$, respectively. It is easy to check that these sets are finite fields. The subset $N(\mathbb{S}) = N_l(\mathbb{S}) \cap N_m(\mathbb{S}) \cap N_r(\mathbb{S})$ is called the *nucleus* of $\mathbb{S}$. In some papers, not $N(\mathbb{S})$ but $N_m(\mathbb{S})$ is called the *nucleus* of $\mathbb{S}$. It is easy to see, if $\mathbb{S}$ is commutative,

then $N_l(\mathbb{S}) = N_r(\mathbb{S})$ and $N_l(\mathbb{S}) \subseteq N_m(\mathbb{S})$, therefore $N_l(\mathbb{S}) = N_r(\mathbb{S}) = N(\mathbb{S})$. In [28], a geometric interpretation of these nuclei is discussed.

Next, we give the definition of planar functions, which was introduced by Dembowski and Ostrom in [21] to describe affine planes possessing a collineation group with specific properties.

Definition 2. Let p be an odd prime. A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called a *planar function*, or *perfect nonlinear (PN)*, if for each $a \in \mathbb{F}_{p^n}^*$, $f(x+a) - f(x)$ is a bijection on $\mathbb{F}_{p^n}$.

For $p = 2$, if x_0 is a solution of $f(x+a) - f(x) = b$, then $x_0 + a$ is another one, hence there do not exist planar functions over $\mathbb{F}_{2^n}$.

Definition 3. A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *almost perfect nonlinear (APN)*, if for each $a, b \in \mathbb{F}_{p^n}, a \neq 0$, $f(x+a) - f(x) = b$ has at most 2 solutions.

For example, x^3 is an APN function over $\mathbb{F}_{2^n}$ for any integer $n > 0$. APN functions have important applications in cryptography, for recent surveys, see [13,25].

Note that $(\mathbb{F}_{p^n}, +)$ is also an n-dimensional vector space $\mathbb{F}_p^n$ over $\mathbb{F}_p$. Throughout this paper, we will use this identification of the field and the vector space. In particular, any linear mapping on $\mathbb{F}_p^n$ can be described by a polynomial of the form $\sum_{i=0}^{n-1} c_i x^{p^i}$, which is called *linearized polynomial*; see [31]. A *Dembowski–Ostrom* (DO) polynomial $D \in \mathbb{F}_{p^n}[x]$ is a polynomial

$$D(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i + p^j}.$$

Note that $D(0) = 0$ and

$$\begin{aligned} D(x+a) - D(x) - D(a) &= \sum_{i,j=0}^{n-1} a_{ij}(x^{p^i} a^{p^j} + a^{p^i} x^{p^j}) \\ &= \sum_{i=0}^{n-1} x^{p^i} \sum_{j=0}^{n-1} (a_{ij} + a_{ji}) a^{p^j}, \end{aligned}$$

which is a linearized polynomial. It can be proved that a planar DO polynomial is equivalent to a commutative presemifield with odd characteristic; see [17]. In fact, if $*$ is the presemifield product, then the corresponding planar function is $f(x) = x * x$; when the planar DO polynomial f is given, then the corresponding presemifield product can be defined as

$$x * y = \frac{1}{2}(f(x+y) - f(x) - f(y)). \tag{1}$$

Up until now, all the known planar functions are DO polynomials, except for the family found by Coulter and Matthews in [20], which defines planes of Lenz–Barlotti class II, but not semifield planes.

A function from a finite field $\mathbb{F}_{p^n}$ to itself is *affine*, if it is defined by the sum of a constant and a linearized polynomial over $\mathbb{F}_{p^n}$. There are several equivalence relations of functions for which the *planar* property is invariant:

Definition 4. Two functions f and $g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are called

- *extended affine equivalent* (EA-equivalent), if $g = l_1 \circ f \circ l_2 + l_3$, where l_1, l_2 and l_3 are affine functions, and where l_1, l_2 are permutations of $\mathbb{F}_{p^n}$. Furthermore, if l_3 is the zero mapping,

then f and g are called *affine equivalent*; if l_1 and l_2 are both linearized, and l_3 is the zero mapping, then f and g are called *linear equivalent*;

- *Carlet–Charpin–Zinoviev equivalent* (CCZ-equivalent or graph equivalent), if there is some affine permutation L of $\mathbb{F}_p^{2n}$, such that $L(G_f) = G_g$, where $G_f = \{(x, f(x)) : x \in \mathbb{F}_{p^n}\}$ and $G_g = \{(x, g(x)) : x \in \mathbb{F}_{p^n}\}$.

Generally speaking, EA-equivalence implies CCZ-equivalence, but not vice versa, see [10]. However, if planar functions f and g are CCZ-equivalent, then they are also EA-equivalent [11,30]. Moreover, it is easy to prove the following (see also Corollary 3 in [11]):

Lemma 1. *Let f and g be both planar DO functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$. Then f and g are EA-equivalent if and only if f and g are linear equivalent.*

Proof. Since linear equivalence is a special case of EA-equivalence, we only need to prove the contrary statement. Now assume that f and g are EA-equivalent, i.e. there is affine functions l_1, l_2 and l_3 such that

$$g = l_1 \circ f \circ l_2 + l_3, \tag{2}$$

where l_1 and l_2 are both permutations. Notice that if f is a planar DO function, there exists a presemifield multiplication $*$ such that, $f(x) = x * x$. Let $l_i(x) = \bar{l}_i(x) + a_i$, where $\bar{l}_i(0) = 0$ for $i = 1, 2$. Then the right side of (2) becomes:

$$\begin{aligned} l_1 \circ f(\bar{l}_2(x) + a_2) + l_3 &= l_1\left(\bar{l}_2(x) * \bar{l}_2(x) + 2\bar{l}_2(x) * a_2 + a_2 * a_2\right) + l_3 \\ &= \bar{l}_1\left(\bar{l}_2(x) * \bar{l}_2(x)\right) + 2\bar{l}_1\left(\bar{l}_2(x) * a_2\right) + \bar{l}_1(a_2 * a_2) + a_1 + l_3. \end{aligned}$$

According to the distributivity of a presemifield, $\bar{l}_1(\bar{l}_2(x) * \bar{l}_2(x))$ is also a DO function, namely a quadratic form, and the rest part of the equation above is affine. However, as the right side of (2) is a planar DO function, we have

$$g(x) = \bar{l}_1\left(\bar{l}_2(x) * \bar{l}_2(x)\right) = \bar{l}_1 \circ f \circ \bar{l}_2(x),$$

which means that f and g are linear equivalent. □

Furthermore, because of the correspondence between commutative presemifields with odd characteristic and planar functions, as we mentioned above, the strong isotopism of two commutative presemifields is equivalent to the linear equivalence of the corresponding planar DO functions, which we call directly the *equivalence* of planar DO functions.

To end this section, we list all the commutative semifields of order p^n that are known. For any odd p, there are:

1. The finite fields.
2. Albert's commutative twisted fields [1].
3. Dickson's semifields [22].
4. The Budaghyan–Helleseth semifields [11], with n even (also discovered independently by Zha and Wang in [37]).
5. The Zha–Kyureghyan–Wang semifields [36], with $n = 3k$.
6. Bierbrauer's semifields [6], with $n = 4k$.

Remark 1. In [11], Budaghyan and Helleseth present two families of planar functions, but in [5], Bierbrauer proves that one of them belongs to the other. Therefore, we consider them as one family. There are more constructions [5], but it has been recently shown [32] that they are isotopic to Budaghyan–Helleseth semifields.

For $p = 3$, there are:

7. The Coulter–Matthews–Ding–Yuan semifields [20,23], with n odd.
8. The Cohen–Ganley semifields [15], with n odd.
9. Ganley's semifields [26], with n odd.

Sporadic examples (for Nos. 13, 14 and 15, we only give the corresponding planar functions):

10. The Coulter–Henderson–Kosick semifield [18], with $p = 3$ and $n = 8$.
11. The Penttila–Williams semifield [33], with $p = 3$ and $n = 10$.
12. $x^{90} + x^2$ on $\mathbb{F}_{3^5}$ [35].
13. $x^{162} + x^{108} - x^{84} + x^2$ on $\mathbb{F}_{3^5}$ [19,35].
14. $x^{50} + 3x^6$ on $\mathbb{F}_{5^5}$ [19,35].

2. Semifield family with two parameters

In [15], Cohen and Ganley made significant progress in the investigation of commutative semifields of rank 2 over their middle nucleus. Here "rank 2" means that if the size of semifield is p^{2m}, then its middle nucleus is of size p^m. Let $a, b, c, d \in \mathbb{F}_{p^m}$, $n = 2m$. Cohen and Ganley defined a binary mapping $*$ from $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ as follows:

$$(a, b) * (c, d) = (ac + \varphi_1(bd), ad + bc + \varphi_2(bd)), \tag{3}$$

where φ_1 and φ_2 are linearized polynomials. They considered under which condition $*$ defines the multiplication of a semifield. Some sufficient and necessary conditions were derived, see [3,15] for details. Finite fields, Dickson's semifields, the Cohen–Ganley semifields and the Penttila–Williams semifield are all of this form.

Observe that the multiplication of $\mathbb{F}_{p^m}$ is used in the multiplication $*$ defined by (3), which is basically a linear combination of ac, bd, ad and bc. Hence, one natural question arises: Is it possible to construct some semifields or presemifields, if we replace some of these finite field multiplications by semifield or presemifield multiplications? Our first candidate is naturally the multiplication of Albert's twisted fields, and it turns out to work quite well.

Theorem 1. *Let p be an odd prime, and let m, k be positive integers, such that $\frac{m}{\gcd(m,k)}$ is odd. Define $x \circ_k y = x^{p^k} y + y^{p^k} x$. For elements $(a, b), (c, d) \in \mathbb{F}_{p^m}^2$, define a binary operation $*$ as follows:*

$$(a, b) * (c, d) = (a \circ_k c + \alpha (b \circ_k d)^\sigma, ad + bc), \tag{4}$$

where α is a non-square element in $\mathbb{F}_{p^m}$ and σ is a field automorphism of $\mathbb{F}_{p^m}$. Then, $(\mathbb{F}_{p^{2m}}, +, *)$ is a presemifield, which we denote by $\mathbb{P}_{k,\sigma}$.

Proof. It is routine to check the distributive law of $\mathbb{P}_{k,\sigma}$. Hence, to prove $\mathbb{P}_{k,\sigma}$ is a presemifield, we only need to prove that

$$(a, b) * (c, d) = 0 \quad \text{if and only if} \quad a = b = 0 \quad \text{or} \quad c = d = 0.$$

Assume that $(a, b) * (c, d) = 0$, then we have

$$\begin{aligned} &a \circ_k c + \alpha (b \circ_k d)^\sigma = 0, \\ &ad + bc = 0. \end{aligned} \tag{5}$$

When $d = 0$, we have $a \circ_k c = 0$ and $bc = 0$, which means $c = 0$ or $a = b = 0$ since $\circ_k$ is Albert's presemifield multiplication on $\mathbb{F}_{p^m}$.

When $d \neq 0$, we have $a = -\frac{bc}{d}$. If $b = 0$, then $a = 0$. If $b \neq 0$, then eliminating a in (5), we have

$$\alpha(b^{p^k} d + d^{p^k} b)^\sigma = c^{p^k+1} \left(\frac{b}{d} + \left(\frac{b}{d} \right)^{p^k} \right),$$

which means that

$$\alpha = (c^{p^k+1} (d^{-\sigma})^{p^k+1}) \left(\frac{b}{d} + \left(\frac{b}{d} \right)^{p^k} \right)^{1-\sigma}.$$

However, the equation cannot hold, since α is a non-square in $\mathbb{F}_{p^m}$. Therefore, we get $a = b = 0$. □

To analyze the properties of $\mathbb{P}_{k,\sigma}$, we need the following well-known results:

Proposition 1. *Let p be an odd prime, and let m, k be positive integers, such that $\frac{m}{\gcd(m,k)}$ is odd. Then*

1. $\gcd(p^m - 1, p^k + 1) = 2$, *which means that x^{p^k+1} is a 2–1 mapping on $\mathbb{F}_{p^m}$;*
2. $x^{p^k} + x$ *is a permutation on $\mathbb{F}_{p^m}$.*

It is easy to see that different α generate isotopic semifields, because

$$(a \circ_k c + \alpha(\beta b \circ_k \beta d)^\sigma, a(\beta d) + c(\beta b)) = (a \circ_k c + \alpha\beta^{(p^k+1)\sigma}(b \circ_k d)^\sigma, \beta(ad + bc)),$$

and the image set of $(\cdot)^{p^k+1}$ are all the squares in $\mathbb{F}_{p^m}$. In the remaining part, we assume that the non-square α is an element of $\mathbb{F}_{p^k} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^l}$, $l = \gcd(k, m)$. Furthermore, the planar function that corresponds to $\mathbb{P}_{k,\sigma}$ is

$$(x, y) \mapsto (2x^{p^k+1} + 2\alpha(y^{p^k+1})^\sigma, 2xy).$$

Dividing by 2, we have

$$(x, y) \mapsto (x^{p^k+1} + \alpha(y^{p^k+1})^\sigma, xy).$$

If there exists some u such that $p^k + 1 = p^u(p^s + 1) \bmod p^m - 1$, then $\mathbb{P}_{k,\sigma}$ is isotopic to $\mathbb{P}_{s,\sigma}$, since

$$(x, y) \mapsto (x^{p^k+1} + \alpha(y^{p^k+1})^\sigma, xy),$$

is equivalent with

$$(x, y) \mapsto ((x^{p^u})^{p^s+1} + \alpha((y^{p^u})^{p^s+1})^\sigma, (x^{p^u} y^{p^u})^{p^{-u}}),$$

which is also equivalent with

$$(x, y) \mapsto (x^{p^s+1} + \alpha(y^{p^s+1})^\sigma, xy).$$

For different σ but the same k, the same result can also be derived. Hence, in the rest of this paper, we always let $0 \leq k, r \leq \lfloor \frac{m}{2} \rfloor$ and $k \neq 0$, where $\sigma(x) = x^{p^r}$.

To get a semifield $\mathbb{S}_{k,\sigma}$ from our presemifield, we can define the multiplication $\star$ of $\mathbb{S}_{k,\sigma}$ as follows:

$$((a, b) * (1, 0)) \star ((c, d) * (1, 0)) := (a, b) * (c, d). \tag{6}$$

Let $L(a,b) = (a,b) * (1,0) = (a + a^{p^k}, b)$, which is a linearized mapping and a permutation on $\mathbb{F}_{p^{2m}}$ by Proposition 1. For convenience, when σ is the identity mapping on $\mathbb{F}_{p^m}$, we will denote our presemifield and semifield by $\mathbb{P}_k$ and $\mathbb{S}_k$.

If $L(\beta) = y \in \mathbb{F}_{p^{2m}}$ is in the middle nucleus of $\mathbb{S}_{k,\sigma}$, then for any $x, z \in \mathbb{F}_{p^{2m}}$ we have

$$(x \star L(\beta)) \star z = x \star (L(\beta) \star z).$$

Since L is a permutation, this is equivalent to

$$(L(x) \star L(\beta)) \star L(z) = L(x) \star (L(\beta) \star L(z)),$$

which is also

$$L^{-1}(x * \beta) * z = x * L^{-1}(\beta * z).$$

Furthermore, we can precisely determine the middle nucleus of $\mathbb{S}_{k,\sigma}$:

Theorem 2. *Let $\mathbb{S}_{k,\sigma}$ be the semifield with multiplication $\star$ defined on $\mathbb{F}_{p^{2m}}$ as in (6), with $\alpha \in \mathbb{F}_{p^l}$, $\alpha \neq 0$ and $l = \gcd(m,k)$.*

(a) *If σ is the identity mapping, then the middle nucleus $N_m(\mathbb{S}_k)$ is isomorphic to $\mathbb{F}_{p^{2l}}$.*
(b) *If σ is not trivial, then the middle nucleus $N_m(\mathbb{S}_{k,\sigma})$ is isomorphic to $\mathbb{F}_{p^l}$.*

Proof. Let $c, d \in \mathbb{F}_{p^m}$, such that $L(c,d) \in N_m(\mathbb{S}_{k,\sigma})$. Then we have

$$L^{-1}((a,b) * (c,d)) * (e,f) = (a,b) * L^{-1}((c,d) * (e,f)), \tag{7}$$

for any $(a,b), (e,f) \in \mathbb{F}_{p^m}^2$. For given $a, b \in \mathbb{F}_{p^m}$, there is a unique $u \in \mathbb{F}_{p^m}$ such that

$$u + u^{p^k} = a \circ_k c + \alpha(b \circ_k d)^\sigma, \tag{8}$$

since $x^{p^k} + x$ is a permutation on $\mathbb{F}_{p^m}$. We obtain

$$\begin{aligned} L^{-1}((a,b) * (c,d)) * (e,f) &= L^{-1}(a \circ_k c + \alpha(b \circ_k d)^\sigma, ad + bc) * (e,f) \\ &= L^{-1}(u + u^{p^k}, ad + bc) * (e,f) \\ &= (u, ad + bc) * (e,f) \quad \text{(using the definition of } L) \\ &= (u \circ_k e + \alpha(f \circ_k (ad + bc))^\sigma, uf + (ad + bc)e). \end{aligned} \tag{9}$$

Similarly, for given $e, f \in \mathbb{F}_{p^m}$ we define v by

$$v + v^{p^k} = c \circ_k e + \alpha(d \circ_k f)^\sigma, \tag{10}$$

and the right side of (7) is

$$(a,b) * L^{-1}((c,d) * (e,f)) = (a \circ_k v + \alpha(b \circ_k (cf + de))^\sigma, vb + a(cf + de)). \tag{11}$$

By comparing the second component of the two sides of (7), we have

$$uf + bce = vb + acf.$$

For $f = 0$ but $b \neq 0$, we have $ceb = vb$, which means that $v = ce$. Eliminate v in (10), we have

$$ce + (ce)^{p^k} = c^{p^k} e + ce^{p^k},$$

for any $e \in \mathbb{F}_{p^m}$. That means $c = c^{p^k}$, namely,

$$c \in \mathbb{F}_{p^l}. \tag{12}$$

Furthermore, for $f \neq 0$, we have

$$u + \frac{bce}{f} = \frac{b}{f} \cdot v + ac,$$

by eliminating u using (8) and (10), we have

$$\begin{aligned}
&(a^{p^k} + a)c + \alpha(b^{p^k} d + b d^{p^k})^\sigma + c\left(\frac{b}{f} \cdot e + \left(\frac{b}{f} \cdot e\right)^{p^k}\right) \\
&= \frac{b}{f} v + \left(\frac{b}{f}\right)^{p^k} (c \circ_k e + \alpha(d \circ_k f)^\sigma - v) + ac + (ac)^{p^k} \\
&= \frac{b}{f} v + \left(\frac{b}{f}\right)^{p^k} (c(e + e^{p^k}) + \alpha(d \circ_k f)^\sigma - v) + c(a + a^{p^k}).
\end{aligned}$$

By cancelling the same terms on both sides, we have

$$\alpha\left((b \circ_k d)^\sigma - (d \circ_k f)^\sigma \left(\frac{b}{f}\right)^{p^k}\right) + \left(\frac{b}{f} - \left(\frac{b}{f}\right)^{p^k}\right)(ce - v) = 0. \tag{13}$$

If σ is the identity mapping, then

$$\left(\frac{b}{f} - \left(\frac{b}{f}\right)^{p^k}\right)(\alpha f d^{p^k} + ce - v) = 0.$$

Since the equation above should hold for any b and $f \neq 0$, we have

$$v = \alpha f d^{p^k} + ce,$$

which means that

$$v + v^{p^k} = (e^{p^k} + e)c + \alpha(f^{p^k} d^{p^{2k}} + f d^{p^k}),$$

since $\alpha \in \mathbb{F}_{p^l} = \mathbb{F}_{p^k} \cap \mathbb{F}_{p^m}$. Together with (10), we have

$$d f^{p^k} + f d^{p^k} = f^{p^k} d^{p^{2k}} + f d^{p^k},$$

for any $f \neq 0$, which means that $d = d^{p^k}$. Therefore, if $(c, d) \in N_m(\mathbb{S}_k)$, then $c, d \in \mathbb{F}_{p^k} \cap \mathbb{F}_{p^m} (= \mathbb{F}_{p^l})$. Since the middle nucleus of a finite semifield is isomorphic to a finite field, $N_m(\mathbb{S}_k)$ is isomorphic to a subfield of $\mathbb{F}_{p^{2l}}$. Conversely, it is routine to check that $(c, d) \in N_m(\mathbb{S}_k)$, for $c, d \in \mathbb{F}_{p^l}$. Therefore we proved Claim 1.

If σ is not trivial, then it is also routine to check that $(c, 0) \in N_m(\mathbb{S}_{k,\sigma})$, for $c \in \mathbb{F}_{p^l}$, namely $\mathbb{F}_{p^l}$ is a subfield of $N_m(\mathbb{S}_{k,\sigma})$. Next, we prove $d = 0$. We separate this proof into two steps, first let us prove that $d \in \mathbb{F}_{p^l}$. Let $L(c, d) \in N_m(\mathbb{S}_{k,\sigma})$, which means that $c \in \mathbb{F}_{p^l}$, see (12), and

$$L(c, d) \star L(c, d) = (c, d) * (c, d) = (2c^2 + 2\alpha d^{\sigma(p^k+1)}, 2cd).$$

Notice that the middle nucleus is a finite field in the semifield, hence we have $c^2 + \alpha d^{\sigma(p^k+1)} \in \mathbb{F}_{p^l}$, which means that $d^{p^k+1} \in \mathbb{F}_{p^l}$. Since $l = \gcd(m, k)$, we have $d^{p^k+1} = d^{p^{2k}+p^k}$, hence $d \in \mathbb{F}_{p^k} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^l}$. This shows that $N_m(\mathbb{S}_{k,\sigma})$ is isomorphic to a subfield of $\mathbb{F}_{p^{2l}}$.

Now we show that $d = 1$ is impossible. The case of $d \neq 0, 1$ is similar and left to the reader. Assume that $d = f = 1$ and $e = 0$. Then (10) shows that $v = \alpha$, and (13) becomes

$$\alpha((b^{p^k} + b)^\sigma - 2b^{p^k}) - \alpha(b - b^{p^k}) = 0,$$

which means that

$$(b^{p^k} + b)^\sigma = (b^{p^k} + b),$$

holds for all $b \in \mathbb{F}_{p^m}$. Thus $x^\sigma = x$ for all $x \in \mathbb{F}_{p^n}$, and so σ is trivial, contradicting the $\sigma \neq \mathrm{id}$ assumption. Hence d has to be 0. □

Noticing that $N_l(\mathbb{S}_{k,\sigma}) = N_r(\mathbb{S}_{k,\sigma}) = N(\mathbb{S}_{k,\sigma})$, since $\mathbb{S}_{k,\sigma}$ is commutative, the nucleus of $\mathbb{S}_{k,\sigma}$ can also be derived:

Theorem 3. *Let $\mathbb{S}_{k,\sigma}$ be the semifield with multiplication $\star$ defined as in (6) on $\mathbb{F}_{p^{2m}}$, then its (left, right) nucleus $N(\mathbb{S}_{k,\sigma})$ is isomorphic to $\mathbb{F}_{p^t}$, where $x^\sigma = x^{p^s}$ and $t = \gcd(m, k, s)$.*

Proof. By using the same notations as in the proof of Theorem 2, assume that (a, b) is an element in $N(\mathbb{S}_{k,\sigma})$. Since $N(\mathbb{S}_{k,\sigma}) \subseteq N_m(\mathbb{S}_{k,\sigma})$, by Theorem 2, we have $a \in \mathbb{F}_{p^l} = \mathbb{F}_{p^k} \cap \mathbb{F}_{p^m}$ and $b = 0$. Moreover, by (9) and (11), we have

$$L^{-1}((a, b) * (c, d)) * (e, f) = (u \circ_k e + \alpha(f \circ_k (ad))^\sigma, uf + ade),$$

and

$$(a, b) * L^{-1}((c, d) * (e, f)) = (a \circ_k v, a(cf + de)).$$

Since $u + u^{p^k} = a \circ_k c + \alpha(b \circ_k d)^\sigma = a(c + c^{p^k})$, we have $u = ac$ and

$$L^{-1}((a, b) * (c, d)) * (e, f) = (a(c \circ_k e) + \alpha a^\sigma (f \circ_k d)^\sigma, acf + ade),$$
$$(a, b) * L^{-1}((c, d) * (e, f)) = (a(v + v^{p^k}), a(cf + de)).$$

By the definition of v, it follows that:

$$L^{-1}((a, b) * (c, d)) * (e, f) = (a, b) * L^{-1}((c, d) * (e, f)) \quad \text{if and only if} \quad a^\sigma = a.$$

Since $N(\mathbb{S}_{k,\sigma}) \subseteq N_m(\mathbb{S}_{k,\sigma})$, when σ is non-trivial, from Theorem 2(2), we know that $N_m(\mathbb{S}_{k,\sigma}) = \{(a, 0) | a \in \mathbb{F}_{p^l}, l = \gcd(m, k)\}$. Therefore, we have $N(\mathbb{S}_{k,\sigma}) \simeq \mathbb{F}_{p^t}$.

When σ is the identity mapping, let $a, b \in \mathbb{F}_{p^l}, b \neq 0$ and $d = f = 0$. Assume that $(a, b) \in N(\mathbb{S}_{k,\sigma})$, then by comparing the second components of (9) and (11), we have $v = ce$, which means that

$$v + v^{p^k} = ce + c^{p^k} e^{p^k}.$$

However, by (10), we have

$$v + v^{p^k} = c \circ_k e.$$

Hence,

$$(c - c^{p^k})(e - e^{p^k}) = 0,$$

which cannot hold for $c, e \in \mathbb{F}_{p^m} \setminus \mathbb{F}_{p^k}$. Hence, $N(\mathbb{S}_{k,\sigma})$ is a proper subset of $N_m(\mathbb{S}_{k,\sigma})$.

Furthermore, since $N(\mathbb{S}_{k,\sigma})$ is a subfield in the finite field $N_m(\mathbb{S}_{k,\sigma}) \cong \mathbb{F}_{p^{2l}}$, and it is routine to show that $\mathbb{F}_{p^l} \subseteq N(\mathbb{S}_{k,\sigma})$, finally we have $N(\mathbb{S}_{k,\sigma}) \cong \mathbb{F}_{p^l}$ and $l = t = \gcd(m, k, 0)$. □

Remark 2. If we let $k = 0$, then $\mathbb{S}_{k,\sigma}$ is a Dickson semifield. It is easy to see that Theorems 2 and 3 also hold for Dickson semifields.

3. The isotopism between $\mathbb{S}_{k,\sigma}$

It is natural to ask that whether (4) defines isotopic presemifields for the same m but different k and σ. As we mentioned after Theorem 1, if there exists some u such that $p^k + 1 = p^u(p^s + 1) \bmod p^m$, then $\mathbb{P}_{k,\sigma}$ is isotopic to $\mathbb{P}_{s,\sigma}$; for different σ but same k, the same result can also be derived. Furthermore, we can prove the following:

Theorem 4. *Let $\mathbb{P}_{k,\sigma}$ be the presemifield with the multiplication $*$ defined as in (4) on $\mathbb{F}_{p^{2m}}$. Let $0 < k, s \le \lfloor \frac{m}{2} \rfloor$ and $0 \le r, t \le \lfloor \frac{m}{2} \rfloor$, where $\sigma(x) = x^{p^r}$ and $\tau(x) = x^{p^t}$. If $(k, \sigma) \ne (s, \tau)$, then $\mathbb{P}_{k,\sigma}$ and $\mathbb{P}_{s,\tau}$ are not strongly isotopic.*

Proof. Let l be a linearized polynomial over $\mathbb{F}_{p^{2m}}$. Since every element $z \in \mathbb{F}_{p^{2m}}$ can be viewed as a vector $(x, y) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ by choosing a basis of $\mathbb{F}_{p^{2m}}$ over $\mathbb{F}_{p^m}$, $l(z)$ can be written as a polynomial $L(x, y) \in \mathbb{F}_{p^{2m}}[x, y]$ whose terms are x^{p^i} and y^{p^i} with $i = 0, \ldots, m-1$.

Denote f and g as the corresponding planar functions from $\mathbb{P}_{k,\sigma}$ and $\mathbb{P}_{s,\tau}$. Since strong isotopism between $\mathbb{P}_{k,\sigma}$ and $\mathbb{P}_{s,\tau}$ is equivalent to the linear equivalence between f and g, we assume that there exist linearized polynomials $l_1, l_2 : \mathbb{F}_{p^{2m}} \to \mathbb{F}_{p^m}$ which can be written as $L_1(x, y)$, $L_2(x, y)$ respectively, and linearized polynomial $l(z) = L(x, y)$ where both $L(x, y)$ and $(L_1(x, y), L_2(x, y))$ invertible, such that

$$\begin{aligned} &L\left(L_1(x,y)^{p^k+1} + \alpha(L_2(x,y)^{p^k+1})^\sigma, L_1(x,y)L_2(x,y)\right) \\ &\quad = (x^{p^s+1} + \alpha(y^{p^s+1})^\tau, xy). \end{aligned} \tag{14}$$

For convenience, we denote $L_i(x, 0)$ and $L_i(0, y)$ by $L_i(x)$ and $L'_i(y)$ respectively. We first prove the following:

Claim 1. *If (14) holds, then $s = k$ and $L_i(x)$ and $L'_i(y)$ are monomials or zero, for $i = 1, 2$.*

Here we only prove the result for $L_i(x)$. By symmetry, a similar proof can be derived for $L'_i(y)$. Let $y = 0$, we have,

$$\begin{aligned} \left(L_1(x)^{p^k+1} + \alpha(L_2(x)^{p^k+1})^\sigma, L_1(x)L_2(x)\right) &= L^{-1}(x^{p^s+1}, 0) \\ &= (\varphi_1(x^{p^s+1}), \varphi_2(x^{p^s+1})), \end{aligned}$$

where $L_1(x) = \sum_{i=0}^{m-1} a_i x^{p^i}$, $L_2(x) = \sum_{i=0}^{m-1} b_i x^{p^i}$, $\varphi_1(x) = \sum_{i=0}^{m-1} c_i x^{p^i}$ and $\varphi_2(x) = \sum_{i=0}^{m-1} d_i x^{p^i}$ are linearized polynomials. We divide the following proof into two cases:

1. Neither $L_1(x)$ nor $L_2(x)$ equals 0;
2. $L_1(x)$ or $L_2(x)$ equals 0.

Case (1): Since $L_1(x)L_2(x) = \varphi_2(x^{p^s+1})$ and $s > 0$, we have

$$\begin{cases} (a_i b_{i+s} + a_{i+s} b_i) = d_i, & \text{for any } i; \\ a_i b_j + a_j b_i = 0, & j \ne i \pm s. \end{cases}$$

Assume that $d_u \ne 0$, then noticing that $a_i b_i = 0$ for any $0 \le i \le m-1$, we have $d_u = a_u b_{u+s}$ or $a_{u+s} b_u$.

(a) If $a_u \neq 0$, then $b_u = 0$ and for any $j \neq u \pm s$, we have

$$a_u b_j + a_j b_u = 0,$$

which means that $b_j = 0$, and $L_2(x) = b_{u-s}x^{p^{u-s}} + b_{u+s}x^{p^{u+s}}$. If $b_{u\pm s} \neq 0$, then we can also use a similar argument to prove that $L_1(x) = a_u x^{p^u}$. Furthermore, we have

$$\varphi_1(x^{p^s+1}) = a_u^{p^k+1}(x^{p^k+1})^{p^u} + \alpha(b_{u-s}x^{p^{u-s}} + b_{u+s}x^{p^{u+s}})^{(p^k+1)\sigma}. \tag{15}$$

The right side of (15) is

$$\begin{aligned}&\left(a_u^{p^k+1}x^{(p^k+1)p^u} + \alpha b_{u-s}^{(p^k+1)\sigma}x^{(p^k+1)\sigma p^{u-s}} + \alpha b_{u+s}^{(p^k+1)\sigma}x^{(p^k+1)\sigma p^{u+s}}\right)\\ &\quad + \alpha\left(b_{u-s}^{p^k}b_{u+s}x^{(p^{k-s}+p^s)p^u} + b_{u-s}b_{u+s}^{p^k}x^{(p^{-s}+p^{s+k})p^u}\right)^{\sigma}\end{aligned}$$

which means that (15) does not hold, since $x^{(p^{k-s}+p^s)}$ and $x^{(p^{-s}+p^{s+k})}$ cannot be simultaneously written in the form $x^{(p^s+1)p^i}$ for some i respectively. Therefore, one of b_{u-s} and b_{u+s} must be 0.

If $b_{u-s} = 0$, then we can derive that $L_1(x) = a_u x^{p^u} + a_{u+2s}x^{p^{u+2s}}$. By symmetry it can also be proved that $a_{u+2s} = 0$. These arguments show that $L_1(x)$ and $L_2(x)$ are both monomials, and we have that

$$\varphi_1(x^{p^s+1}) = a_u^{p^k+1}(x^{p^k+1})^{p^u} + \alpha(b_{u+s}x^{p^{u+s}})^{(p^k+1)\sigma}. \tag{16}$$

When $s \neq k$, then (16) also cannot hold, otherwise that means the presemifields on $\mathbb{F}_{p^m}$ defined by x^{p^s+1} and x^{p^k+1} are isotopic.

If $b_{u+s} \neq 0$, then by symmetry we can get $L_1(x) = a_{u+s}x^{p^{u+s}}$ and $L_2(x) = b_u x^{p^u}$ and $s = k$.

(b) Similarly as in (a), if $b_u \neq 0$, by the symmetry of L_1 and L_2 in $L_1(x)L_2(x) = \varphi_2(x^{p^s+1})$, we can prove that $s = k$ and both $L_1(x)$ and $L_2(x)$ are monomials.

Case (2): Assume that $L_1(x) \neq 0$ and $L_2(x) = 0$, without loss of generality, we have $L_1(x)^{p^k+1} = \varphi_1(x^{p^s+1})$. It cannot hold for $s \neq k$, since two generalized twisted fields are not isotopic. When $s = k$, according to Theorem 5.2 in [8], we know that $L_1(x)$ and $\varphi_1(x)$ are both linearized monomials.

Therefore, we have proved Claim 1.

Now, for $k = s$, we know that $L_1(x, y)$ and $L_2(x, y)$ are both linearized binomials or monomials. Assume that the possible degrees of x in L_1 and L_2 are p^u and p^{u+k}, those of y are p^v and p^{v+k}, then there are four possible combinations of them to form L_1 and L_2:

(a) $L_1 : (x^{p^u}, y^{p^v})$, $L_2 : (x^{p^{u+k}}, y^{p^{v+k}})$;
(b) $L_1 : (x^{p^u}, y^{p^{v+k}})$, $L_2 : (x^{p^{u+k}}, y^{p^v})$;
(c) $L_1 : (x^{p^{u+k}}, y^{p^v})$, $L_2 : (x^{p^u}, y^{p^{v+k}})$;
(d) $L_1 : (x^{p^{u+k}}, y^{p^{v+k}})$, $L_2 : (x^{p^u}, y^{p^v})$.

First, let us assume that L_1 and L_2 are both binomials. In fact, noticing that there is only xy on the right side of (14), both (a) and (d) are not feasible, and there must be $u = v$ for (b) and (c). Now we consider case (b): $L_1(x, y) = a_u x^{p^u} + a'_{u+k}y^{p^{u+k}}$ and $L_2(x, y) = b_{u+k}x^{p^{u+k}} + b'_u y^{p^u}$. Let

$$L^{-1} = \begin{pmatrix}\varphi_1 & \varphi_3\\ \varphi_2 & \varphi_4\end{pmatrix},$$

then by expanding the first component of (14), we have

$$L_1(x,y)^{p^k+1} + \alpha(L_2(x,y)^{p^k+1})^\sigma = \varphi_1(x^{p^k+1} + \alpha(y^{p^k+1})^\tau) + \varphi_3(xy).$$

The terms are $a_u x^{p^u} a'^{p^k}_{u+k} y^{p^{u+2k}}$ and $(b^{p^k}_{u+k} x^{p^{u+2k}} b'_u y^{p^u})^\sigma$ occur on the left side, but they are impossible to appear on the right side. That means $L_1(x)$ and $L_2(x)$ are both monomials with the same degree.

First, if $a'_{u+k} = b_{u+k} = 0$ then we have

$$(a_u x^{p^u})^{p^k+1} + \alpha((b'_u y^{p^u})^{p^k+1})^\sigma = \varphi_1(x^{p^k+1} + \alpha(y^{p^k+1})^\tau) + \varphi_3(xy).$$

We can easily derive that φ_1 is a monomial, $\varphi_3 = 0$ and hence $\sigma = \tau$.

Second, if $a'_u = b_u = 0$ and $w = u + k$, then we have that $L_1(x,y) = a'_w y^{p^w}$, $L_2(x,y) = b_w x^{p^w}$, and

$$(a'_w y^{p^w})^{p^k+1} + \alpha((b_w x^{p^w})^{p^k+1})^\sigma = \varphi_1(x^{p^k+1} + \alpha(y^{p^k+1})^\tau) + \varphi_3(xy).$$

It is also easy to see that $\varphi_1(x)$ is a monomial and $\varphi_3(x) = 0$. Therefore $\sigma = \tau$ and σ^2 is identity.

For case (c), we can derive the same result as case (b). Hence, this completes the proof. □

To investigate the isotopism between $\mathbb{S}_{k,\sigma}$ and $\mathbb{S}_{s,\tau}$ further, we need the following result from [17]:

Theorem 5 (*Coulter and Henderson*). *Let $F_1 = (\mathbb{F}_q, +, \star)$ and $F_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative semifields. Then every isotopism (M, N, K) between F_1 and F_2 satisfies either*

1. *$M = N$, or*
2. *$M(x) \equiv \gamma \star N(x) \bmod (x^q - x)$, where $\gamma \in N_m(F_1)$, $\gamma \neq 0$.*

Next, we are going to show the non-isotopism between $\mathbb{S}_{k,\sigma}$ and $\mathbb{S}_{s,\tau}$.

Theorem 6. *Let $\mathbb{S}_{k,\sigma}$ be the presemifield with the multiplication $*$ defined as in (6) on $\mathbb{F}_{p^{2m}}$. Let $0 < k, s \leq \lfloor \frac{m}{2} \rfloor$ and $0 \leq r, t \leq \lfloor \frac{m}{2} \rfloor$, where $\sigma(x) = x^{p^r}$ and $\tau(x) = x^{p^t}$. If $(k,\sigma) \neq (s,\tau)$, then $\mathbb{S}_{k,\sigma}$ and $\mathbb{S}_{s,\tau}$ are not isotopic.*

Furthermore, if $\sigma = \mathrm{id}$, then for every k, the semifield $\mathbb{S}_k$ defines two inequivalent planar functions over $\mathbb{F}_{p^{2m}}$.

Proof. Now let $\star$ and $\diamond$ be the multiplication of $\mathbb{S}_{k,\sigma}$ and $\mathbb{S}_{s,\tau}$ respectively defined by (6), where $(k,\sigma) \neq (s,\tau)$. To show that they are not isotopic, by Theorem 5 we need to show that it is impossible to find linearized polynomials N, K and $\gamma \in N_m(\mathbb{S}_{k,\sigma})$ such that

$$(r \star N(x)) \star N(y) = K(x \diamond y),$$

which is

$$(r \star x') \star y' = K(N^{-1}(x') \diamond N^{-1}(y')),$$

by replacing $N(x)$ with x' and $N(y)$ with y'. Define $x \star_\gamma y := (\gamma \star x) \star y$, and let $*$ be the multiplication of $\mathbb{P}_{k,\sigma}$. By (6), we have

$$\begin{aligned} x \star_\gamma y &= (\gamma \star x) \star y \\ &= L^{-1}(L^{-1}(\gamma) * L^{-1}(x)) * L^{-1}(y), \end{aligned}$$

which is strongly isotopic to

$$x \otimes_\gamma y := L^{-1}(L^{-1}(\gamma) * x) * y. \tag{17}$$

Hence we only need to prove that for any nonzero γ the semifield defined by $\otimes_\gamma$ and $\mathbb{S}_{s,\tau}$ are not strongly isotopic. We divide the proof into two cases: $\sigma \neq \mathrm{id}$ and $\sigma = \mathrm{id}$.

When σ is non-trivial, we know that $N_m(\mathbb{S}_{k,\sigma}) = \mathbb{F}_{p^m} \cap \mathbb{F}_{p^k} = \{(c, 0) \mid c \in \mathbb{F}_{p^l}\}$ with $l = \gcd(k, m)$ by Theorem 2, hence $L(c, 0) = (c + c^{p^k}, 0) = (2c, 0)$. Write γ as $(2c, 0)$ where $c \neq 0$, and write x as (a, b), then

$$L^{-1}(\gamma) * x = L^{-1}((c, 0) * (a, b)) = L^{-1}(a \circ_k c, bc) = (ac, bc).$$

Take $y = (e, f)$, then (17) becomes

$$\begin{aligned}(a, b) \otimes_\gamma (e, f) &= L^{-1}((c, 0) * (a, b)) * (e, f)\\ &= \left((a \circ_k e)c + \alpha c^\sigma (b \circ_k f)^\sigma, c(af + be)\right).\end{aligned}$$

The corresponding planar function of $\otimes_\gamma$ can be written as

$$(x, y) \mapsto 2 \cdot (cx^{p^k+1} + \alpha c^\sigma (y^{p^k+1})^\sigma, cxy),$$

which is equivalent to the one defined by $\mathbb{S}_{k,\sigma}$. That means if the presemifield defined by $\otimes_\gamma$ is strongly isotopic to $\mathbb{S}_{s,\tau}$, then $\mathbb{S}_{k,\sigma}$ is also strongly isotopic to $\mathbb{S}_{s,\tau}$, which contradicts Theorem 4. Hence $\mathbb{S}_{k,\sigma}$ is not isotopic to $\mathbb{S}_{s,\tau}$.

For the case that σ is trivial, as proved in Theorem 2, $N_m(\mathbb{S}_{k,\sigma}) = \mathbb{F}_{p^{2l}} = \{(c, d) \mid c, d \in \mathbb{F}_{p^l}\}$ with $l = \gcd(k, m)$. Hence $L(c, d) = (c + c^{p^k}, d) = (2c, d)$. Write γ as $(2c, d)$ where $cd \neq 0$, and write x as (a, b), then

$$\begin{aligned}L^{-1}\left(L^{-1}(\gamma) * x\right) &= L^{-1}((c, d) * (a, b))\\ &= L^{-1}\left(c(a + a^{p^k}) + \alpha d(b + b^{p^k}), ad + bc\right)\\ &= (ac + \alpha bd, ad + bc).\end{aligned}$$

Take $y = (e, f)$, then (17) becomes

$$\begin{aligned}(a, b) \otimes_\gamma (e, f) &= ((ac + \alpha bd) \circ_k e + \alpha((ad + bc) \circ_k f), (ad + bc)e + (ac + \alpha bd) f)\\ &= (c(a \circ_k e + b \circ_k f\alpha) + \alpha d(b \circ_k e + a \circ_k f), c(af + be)\\ &\quad + d(ae + bf\alpha)).\end{aligned}$$

If $c \neq 0$ but $d = 0$, then it is easy to check that the semifield defined by $\otimes_\gamma$ is strongly isotopic to $\mathbb{S}_k$. By Theorem 4, $\mathbb{S}_k$ is not strongly isotopic to $\mathbb{S}_s$, therefore the semifield defined by $\otimes_\gamma$ is also not strongly isotopic to $\mathbb{S}_s$.

If $d \neq 0$, then without loss of generality, we assume that $d = 1$. Then $(a, b) \otimes_\gamma (e, f)$ becomes

$$(c(a \circ_k e + b \circ_k f\alpha) + \alpha(b \circ_k e + a \circ_k f), c(af + be) + (ae + bf\alpha)), \tag{18}$$

and the corresponding planar function is

$$(x, y) \mapsto (2c(x^{p^k+1} + \alpha y^{p^k+1}) + 2\alpha x \circ_k y, 2cxy + x^2 + \alpha y^2),$$

which is equivalent to

$$(x, y) \mapsto (2cxy + x^2 + \alpha y^2, c(x^{p^k+1} + \alpha y^{p^k+1}) + \alpha x \circ_k y). \tag{19}$$

Now, we need a claim:

Claim. *If $c^2-\alpha$ is a non-square in $\mathbb{F}_{p^l}$, where $l=\gcd(m,k)$, then the presemifield defined by $\otimes_\gamma$ in (18) is not strongly isotopic with $\mathbb{S}_s$, for any $s>0$.*

Let us first assume that this claim holds. It is well-known that there always exist some $c\in\mathbb{F}_{p^l}$ such that $c^2-\alpha$ is a non-square in $\mathbb{F}_{p^l}$, where $l=\gcd(m,k)$ and $\alpha\in\mathbb{F}_{p^l}$ is also a non-square. Therefore for any γ, the presemifield defined by $\otimes_\gamma$ and $\mathbb{S}_s$ are not strongly isotopic. Hence $\mathbb{S}_k$ and $\mathbb{S}_s$ are also not isotopic. Furthermore, we also see that for every k, the semifield $\mathbb{S}_k$ defines two inequivalent planar functions over $\mathbb{F}_{p^{2m}}$.

Finally, we are going to prove this claim. Assume that the presemifield defined by $\otimes_\gamma$ in (18) is not strongly isotopic with $\mathbb{S}_s$, then, similarly as in the proof of Theorem 4, we have linearized polynomials $L_1(x,y)$, $L_2(x,y)$ and $L(x,y)$, where $L(x,y)$ is a permutation such that

$$L\circ\begin{pmatrix}2cL_1(x,y)L_2(x,y)+L_1(x,y)^2+\alpha L_2(x,y)^2\\ c(L_1(x,y)^{p^k+1}+\alpha L_2(x,y)^{p^k+1})+\alpha L_1(x,y)\circ_k L_2(x,y)\end{pmatrix}^T = (x^{p^s+1}+\alpha y^{p^s+1},xy).$$

Let $y=0$, and we denote $L_i(x,0)$ by $L_i(x)$, for convenience. We get,

$$\begin{pmatrix}2cL_1(x)L_2(x)+L_1(x)^2+\alpha L_2(x)^2\\ c(L_1(x)^{p^k+1}+\alpha L_2(x)^{p^k+1})+\alpha L_1(x)\circ_k L_2(x)\end{pmatrix}^T = L^{-1}(x^{p^s+1},0)=(\varphi_1(x^{p^s+1}),\varphi_2(x^{p^s+1})),$$

where $\varphi_1(x),\varphi_2(x)$ are linearized polynomials. Let $L_1(x)=\sum_{i=0}^{m-1}a_ix^{p^i}$, $L_2(x)=\sum_{i=0}^{m-1}b_ix^{p^i}$ and $\varphi_1(x)=\sum_{i=0}^{m-1}c_ix^{p^i}$, then

$$L_1(x)^2+\alpha L_2(x)^2+2cL_1(x)L_2(x) = \sum_{i>j}2(a_ia_j+\alpha b_ib_j+ca_ib_j+ca_jb_i)x^{p^i+p^j}+\sum_{i=0}^{m-1}(a_i^2+\alpha b_i^2+2ca_ib_i)x^{2p^i}.$$

Since $s\neq 0$, by comparing the equation above with $\varphi_1(x^{p^s+1})$, we have that

$$a_i^2+\alpha b_i^2+2ca_ib_i=0,\quad \text{for any } 0\le i\le m-1,$$

which can also be written as,

$$(a_i+cb_i)^2+(\alpha-c^2)b_i^2=0,\quad \text{for any } 0\le i\le m-1.$$

If $c^2-\alpha$ is a non-square in $\mathbb{F}_{p^l}$, then it is also a non-square in $\mathbb{F}_{p^m}$, since $\frac{m}{l}$ is odd. Hence the equation above has no solution. Therefore, the claim is proved, and we also finish the proof of this theorem. □

The total number of non-isotopic semifields and inequivalent planar functions defined by $\mathbb{S}_{k,\sigma}$ can also be counted:

Corollary 1. *Let $\mathbb{S}_{k,\sigma}$ be the semifield with the multiplication $\star$ defined as in (6) on $\mathbb{F}_{p^{2m}}$, where $m=2^e\mu$ with $\gcd(\mu,2)=1$, then $\mathbb{S}_{k,\sigma}$ defines*

1. $\lfloor\frac{\mu}{2}\rfloor\cdot\lceil\frac{m}{2}\rceil$ *non-isotopic semifields; and*
2. $\lfloor\frac{\mu}{2}\rfloor\cdot(\lceil\frac{m}{2}\rceil+1)$ *inequivalent planar functions.*

4. $\mathbb{S}_{k,\sigma}$ is a new family

In the previous sections, we showed that our new family looks like a combination of Dickson semifields and generalized twisted fields, and $\mathbb{S}_k$ behaves quite different from $\mathbb{S}_{k,\sigma}$ with nontrivial σ. Therefore, we suggest to divide it into two families, according to whether σ is trivial, as the case of finite fields and Dickson semifields.

When we take them as two families, then one natural question is:

Do $\mathbb{S}_k$ and $\mathbb{S}_{k,\sigma}$ contain new semifields compared with the other known families?

In fact, for some cases, we can prove that $\mathbb{S}_k$ is contained in the family discovered by Budaghyan and Helleseth [11,12], which can be rewritten in the following form:

Theorem 7 (*Kyureghyan and Bierbrauer [7]*)**.** *Let p be an odd prime number, $q = p^m$, $n = 2m$ and integers i, j such that $s = i - j$. Then the mapping $M_s : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by*

$$M_s(x) = x^{p^m+1} + \omega \mathrm{tr}_{q^2/q}(\beta x^{p^i+p^j}), \quad i \geq j \geq 0,$$

is planar if and only if all the following conditions are fulfilled:

1. *$s = 0$ or $\nu(s) \neq \nu(m)$,*
2. *$\omega \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$,*
3. *β is a non-square in $\mathbb{F}_{q^2}$,*

where $\nu(s)$ is defined by $s = 2^{\nu(s)}s_1$ with s_1 an odd integer.

Since $u^{p^m+1} \in \mathbb{F}_{p^m}$, for any $u \in \mathbb{F}_{p^{2m}}$, different choices of ω give equivalent planar functions. Furthermore, it is easy to see that different (i, j) with the same s also lead to equivalent M_s, so we redefine $M_s(x)$ as follows:

$$M_s(x) = x^{p^m+1} + \omega \mathrm{tr}_{q^2/q}(\beta x^{p^s+1}), \tag{20}$$

where $s = 0$ or $\nu(s) \neq \nu(m)$, and β and ω are the same as in Theorem 7.

The following lemma can be found in [16,24,27]:

Lemma 2. *For an odd prime p,*

$$\gcd(p^j + 1, p^n - 1) = \begin{cases} p^{\gcd(j,n)} + 1, & \text{if } \nu(j) < \nu(n); \\ 2, & \text{otherwise.} \end{cases}$$

When m is odd, there exist $\omega \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, such that $\omega + \omega^{p^m} = 0$ and $u \in \mathbb{F}_{p^{2m}}$ can be written as $a + b\omega$, where $a, b \in \mathbb{F}_{p^m}$. Furthermore, by Lemma 2, since m is odd and $\nu(s) \neq \nu(m)$, we have $\gcd(p^s + 1, p^{2m} - 1) = 2$, so different non-square β lead to equivalent $M_s(x)$ and we assume that $\beta = \omega^{-1}$. Then we denote $\odot$ to be the multiplication defined by (20), denote $u, v \in \mathbb{F}_{p^{2m}}$ respectively by $a + b\omega$ and $c + d\omega$, and we have

$$\begin{aligned} u \odot v &= (a + b\omega) \odot (c + d\omega) \\ &= (a + b\omega^{p^m})(c + d\omega) + (a + b\omega)(c + d\omega^{p^m}) + \omega \mathrm{tr}_{q^2/q}(\omega^{-1} x \circ_s Y) \\ &= 2ac - 2bd\omega^2 + ((a + b\omega) \circ_s (c + d\omega) - (a - b\omega) \circ_s (c - d\omega)) \\ &= 2(ac - bd\omega^2) + 2(a \circ_s (d\omega) + (b\omega) \circ_s c) \\ &= 2(ac - bd\omega^2) + 2(a \circ_s d + b \circ_s c)\omega. \end{aligned}$$

The last equality sign holds, because $\omega^{p^s-1} = 1$, since that s must be even. Moreover, the corresponding planar function is equivalent to

$$M_s(x, y) = (x^{p^s} y + x y^{p^s}, x^2 - \omega^2 y^2),$$

which is equivalent to (19) with $c = 0$, when -1 is a square in $\mathbb{F}_{p^m}$.

However, on the other hand, since we showed above that when m is odd and -1 is a square, the Budaghyan–Helleseth semifield is isotopic to $\mathbb{S}_k$, it cannot be isotopic to $\mathbb{S}_{k,\sigma}$ with non-trivial σ by Theorem 6. Furthermore, by the middle and left nucleus of $\mathbb{S}_{k,\sigma}$, we know that it is not isotopic with Albert's and Dickson's semifields. Moreover, since $\mathbb{S}_{k,\sigma}$ is defined over p^{2m} for any odd p, it must cover some new semifields.

Theorem 8. *When $m \geq 5$ is odd and -1 is a square, $\mathbb{S}_{k,\sigma}$ with non-trivial σ contains semifields which are not isotopic with any known ones.*

5. APN functions with the similar form

In [11,36], it is independently shown for the first time that some planar functions can be derived from quadratic APN functions. Similar constructions for planar function can also be found in [4,6,37]. One natural question is the following: Is it possible to get some new APN functions from known planar ones?

In fact, from our new presemifields family, we can derive a similar family of APN functions on $\mathbb{F}_{2^{2m}}$:

Theorem 9. *Let $m \geq 2$ be even integer, and k be a integer such that $\gcd(k, m) = 1$. Define a function f on $\mathbb{F}_{2^{2m}}$ as follows,*

$$f(x, y) = (x^{2^k+1} + \alpha y^{(2^k+1)\sigma}, xy),$$

where $\alpha \in \mathbb{F}_{2^m}, \alpha \neq 0$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{2^m})$. Then f is an APN function, if and only if, α cannot be written as $a^{2^k+1}(t^{2^k} + t)^{1-\sigma}$, where $a, t \in \mathbb{F}_{2^m}$.

Proof. Since f is quadratic, we only have to prove that for each $(a, b) \neq 0$, the equations

$$\begin{cases} x \circ_k a + \alpha(y \circ_k b)^\sigma = 0 \\ ay + bx = 0 \end{cases}$$

have at most two roots, where $x \circ_k y = x^{p^k} y + y^{p^k} x$.

If $b = 0$, then we have $x \circ_k a = 0$ and $ay = 0$, which means $y = 0$, $x = 0$ or a, since x^{p^k+1} is APN function on $\mathbb{F}_{2^m}$ and $a \neq 0$.

If $b \neq 0$, then $x = \frac{ay}{b} = t \cdot a$, where $t := \frac{y}{b}$. Hence, we have

$$(at) \circ_k a + \alpha((bt) \circ_k b)^\sigma = 0,$$

namely,

$$(t^{2^k} + t)a^{2^k+1} + \alpha(t^{2^k} + t)^\sigma b^{(2^k+1)\sigma} = 0.$$

If $t^{2^k} + t = 0$, then $x = y = 0$ or $y = b$, $x = a$; If $t^{2^k} + t \neq 0$, then we have

$$\alpha = \left(\frac{a}{b^\sigma}\right)^{2^k+1} (t^{2^k} + t)^{1-\sigma},$$

from which we prove the claim. □

Let us further consider the condition of Theorem 9. For even m, when $\gcd(k, m) = 1$, we have $\gcd(2^k + 1, 2^m - 1) = 3$ and $\gcd(2^i - 1, 2^m - 1) = 2^{\gcd(i,m)} - 1$. Hence, if i is seven and $\sigma(x) = x^{2^i}$, then $a^{2^k+1}(t^{2^k} + t)^{1-\sigma}$ is a cube. Therefore, if α is not a cube, then the condition in Theorem 9 holds.

Corollary 2. *Let $m \geq 2$ be even integer, and k be a integer such that $\gcd(k, m) = 1$. Define a function f on $\mathbb{F}_{2^{2m}}$ as follows:*

$$f(x, y) = (x^{2^k+1} + \alpha y^{(2^k+1)2^i}, xy),$$

where the nonzero $\alpha \in \mathbb{F}_{2^m}$ is a non-cubic and i is even. Then f is an APN function.

Let $m = 4$, $k = 1$ and α be a primitive element of $\mathbb{F}_{2^4}$. By Corollary 2, we can choose $i = 0$ or 2 to get two APN functions. By using MAGMA [9], it can be computed that, when $i = 0$, the APN function is equivalent to the function No 2.1 in Table 10 in [25]. However, when $i = 2$, the Γ-rank of the APN function is 13642, which does not occur in the list of known APN functions in [25] (see [25] for the Γ-rank). More concretely, the function

$$f(x, y) = (x^3 + \alpha y^{12}, xy)$$

is a new APN function on $\mathbb{F}_{2^8}$.

Remark 3. In [14], Carlet presents some interesting constructions of APN functions, which include a similar result to Theorem 9 with $\sigma = \mathrm{id}$.

Acknowledgments

Yue Zhou is partially supported by Natural Science Foundation of China (No. 61070215) and China Scholarship Council.

We would like to thank Juergen Bierbrauer, Lilya Budaghyan and the anonymous referees for their valuable comments and suggestions on the manuscript.

References

[1] A. Albert, On nonassociative division algebras, Trans. Amer. Math. Soc. 72 (1952) 292–309.
[2] A. Albert, Finite division algebras and finite planes, in: Combinatorial Analysis: Proceedings of the 10th Symposium in Applied Mathematics, Symposia in Appl. Math., vol. 10, American Mathematical Society, Providence, RI, 1960, pp. 53–70.
[3] S. Ball, M. Lavrauw, Commutative semifields of rank 2 over their middle nucleus, in: Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer-Verlag, Berlin, New York, 2002, pp. 1–21.
[4] J. Bierbrauer, New commutative semifields and their nuclei, in: M. Bras-Amorós, T. Høholdt (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, in: Lecture Notes in Computer Science, vol. 5527, Springer, Berlin, Heidelberg, Tarragona, Spain, 2009, pp. 179–185.
[5] J. Bierbrauer, Commutative semifields from projection mappings, Des. Codes Cryptogr. 61 (2010) 187–196.
[6] J. Bierbrauer, New semifields, PN and APN functions, Des. Codes Cryptogr. 54 (2010) 189–200.
[7] J. Bierbrauer, G.M. Kyureghyan, On the projection construction of planar and APN mappings, Talk presented at YACC 2010, Porquerolles Island, France, 2010.
[8] M. Biliotti, V. Jha, N.L. Johnson, The collineation groups of generalized twisted field planes, Geom. Dedicata 76 (1999) 97–126. http://dx.doi.org/10.1023/A:1005089016092.
[9] W. Bosma, J. Cannon, C. Playoust, The MAGMA algebra system I: the user language, J. Symbolic. Comput. 24 (1997) 235–265.
[10] L. Budaghyan, C. Carlet, A. Pott, New classes of almost bent and almost perfect nonlinear polynomials, IEEE Trans. Inform. Theory 52 (2006) 1141–1152.

[11] L. Budaghyan, T. Helleseth, New perfect nonlinear multinomials over $F_{p^{2k}}$ for any odd prime p, in: SETA'08: Proceedings of the 5th International Conference on Sequences and their Applications, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 403–414.
[12] L. Budaghyan, T. Helleseth, New commutative semifields defined by new PN multinomials, Cryptogr. Commun. 3 (2011) 1–16.
[13] C. Carlet, Boolean Models and Methods in Mathematics, Computer Science, and Engineering, in: Encyclopedia of Mathematics and its Applications, vol. 134, Cambridge University Press, 2010, pp. 398–471.
[14] C. Carlet, Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions, Des. Codes Cryptogr. 59 (2011) 89–109.
[15] S. Cohen, M. Ganley, Commutative semifields, two-dimensional over their middle nuclei, J. Algebra 75 (1982) 373–385.
[16] R.S. Coulter, Explicit evaluations of some Weil sums, Acta Arith. 83 (1998) 241–251.
[17] R.S. Coulter, M. Henderson, Commutative presemifields and semifields, Adv. Math. 217 (2008) 282–304.
[18] R.S. Coulter, M. Henderson, P. Kosick, Planar polynomials for commutative semifields with specified nuclei, Des. Codes Cryptogr. 44 (2007) 275–286.
[19] R.S. Coulter, P. Kosick, Commutative semifields of order 243 and 3125, in: Finite Fields: Theory and Applications, in: Contemp. Math., vol. 518, Amer. Math. Soc., Providence, RI, 2010, pp. 129–136.
[20] R.S. Coulter, R.W. Matthews, Planar functions and planes of Lenz-Barlotti class II, Des. Codes Cryptogr. 10 (1997) 167–184.
[21] P. Dembowski, T. Ostrom, Planes of order n with collineation groups of order n^2, Math. Z. 103 (1968) 239–258.
[22] L. Dickson, On commutative linear algebras in which division is always uniquely possible, Trans. Amer. Math. Soc. 7 (1906) 514–522.
[23] C. Ding, J. Yuan, A family of skew hadamard difference sets, J. Combin. Theory Ser. A 113 (2006) 1526–1535.
[24] S. Draper, X. Hou, Explicit evaluation of certain exponential sums of quadratic functions over $\mathbb{F}_{p^n}$, p odd, 2007. arXiv:0708.3619v1.
[25] Y. Edel, A. Pott, A new almost perfect nonlinear function which is not quadratic, Adv. Math. Commun. 3 (2009) 59–81.
[26] M. Ganley, Central weak nucleus semifields, European J. Combin. 2 (1981) 339–347.
[27] T. Helleseth, A. Kholosha, On the dual of monomial quadratic p-ary bent functions, in: S. Golomb, G. Gong, T. Helleseth, H.Y. Song (Eds.), Sequences, Subsequences, and Consequences, in: Lecture Notes in Computer Science, vol. 4893, Springer, Berlin, Heidelberg, 2007, pp. 50–61.
[28] D. Hughes, F. Piper (Eds.), Projective Planes, Springer, Berlin, 1973.
[29] D. Knuth, Finite semifields and projective planes, Ph.D. Thesis, California Institute of Technology, Pasadena, California, 1963.
[30] G.M. Kyureghyan, A. Pott, Some theorems on planar mappings, in: WAIFI'08: Proceedings of the 2nd International Workshop on Arithmetic of Finite Fields, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 117–122.
[31] R. Lidl, H. Niederreiter, Finite Fields, second ed., Cambridge University Press, Cambridge, New York, 1997.
[32] G. Marino, O. Polverino, On isotopisms and strong isotopisms of commutative presemifields, J. Algebraic Combin. 36 (2012) 247–261.
[33] T. Penttila, B. Williams, Ovoids of parabolic spaces, Geom. Dedicata 82 (2004) 1–19.
[34] J.H.M. Wedderburn, A theorem on finite algebras, Trans. Amer. Math. Soc. 6 (1905) 349–352.
[35] G. Weng, X. Zeng, Further results on planar DO functions and commutative semifields, Des. Codes Cryptogr. 63 (2012) 413–423.
[36] Z. Zha, G.M. Kyureghyan, X. Wang, Perfect nonlinear binomials and their semifields, Finite Fields Appl. 15 (2009) 125–133.
[37] Z. Zha, X. Wang, New families of perfect nonlinear polynomial functions, J. Algebra 322 (2009) 3912–3918.