# New commutative semifields and their nuclei

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

August 4, 2009

**Abstract**

*Commutative semifields in odd characteristic can be equivalently described by planar functions (also known as PN functions). We describe a method to construct a semifield which is canonically associated to a planar function and use it to derive information on the nuclei directly from the planar function. This is used to determine the nuclei of a family of new commutative semifields of dimension* 12 *in arbitrary odd characteristic.*
**Key Words:** *PN functions, planar functions, presemifields, semifields, middle nucleus, kernel, Dembowski-Ostrom polynomial, isotopy, strong isotopy*

## 1 Introduction

Until recently the only known families of commutative semifields in arbitrary odd characteristic aside of the fields themselves were the classical constructions by Dickson [7] and Albert [1]. The first provably new such general constructions were given in Zha-Kyureghyan-Wang [11] and [2]. The families constructed in Budaghyan-Helleseth [3] may be new as well but this seems to remain unproved. The survey article of Kantor [9] gives more background information and comments on the scarcity of known commutative semifields in odd characteristic, in particular when the characteristic is $> 3$.

**Definition 1.** *A* **presemifield** *is a set $F$ with two binary relations, addition and $*$, such that*

- *$F$ is a commutative group with respect to addition, with identity* $0$.
- *$F^*$ is a loop under multiplication.*
- $0 * a = 0$ *for all $a$.*
- *The distributive laws hold.*

*If moreover there is an element $e \in F$ such that $e * x = x * e = x$ for all $x$ we speak of a* **semifield.**

**Definition 2.** *Let $F = \mathbb{F}_{p^r}$ for an odd prime $p$. A function $f : F \longrightarrow F$ is* **perfectly nonlinear** *(PN), also called a* **planar function,** *if for each $0 \neq a \in F$ the directional derivative $\delta_a$ defined as $\delta_a(x) = f(x+a) - f(x)$ is bijective.*

*Let $f : F \longrightarrow F$ and write it as a polynomial $f(x) = \sum_{i=0}^{r-1} a_i x^i$. Then $f$ is a* **Dembowski-Ostrom** *(DO-)polynomial if all its monomials have $p$-weight $\leq 2$ (the exponents are sums of two powers of $p$).*

In odd characteristic planar DO-polynomials are equivalent with commutative presemifields, see Coulter-Henderson [4]:

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

- *Commutative presemifields in odd characteristic.*
- *Dembowski-Ostrom polynomials which are PN functions.*

The relation between those concepts is identical to the equivalence between quadratic forms and bilinear forms in odd characteristic, with the planar function in the role of the quadratic form. If $*$ is the presemifield product, then the corresponding planar function is $f(x) = x * x$. When the planar function is given, the corresponding semifield product is

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

For an overview see also Section 9.3.2 of Horadam [8]. One way to construct a semifield from a commutative presemifield is the following: choose $0 \neq e \in F$ and define the new multiplication $\circ$ by

$$(x * e) \circ (y * e) = x * y.$$

Then $\circ$ describes a semifield with unit element $e * e$.

**Definition 3.** *Let $F = \mathbb{F}_p^r$ be the $r$-dimensional vector space over $\mathbb{F}_p$. Consider presemifields on $F$ whose additions coincide with that of $F$. Two such presemifield multiplications $*$ and $\circ$ on $F$ are* **isotopic** *if there exist $\alpha_1, \alpha_2, \beta \in GL(r,p)$ such that*

$$\beta(x \circ y) = \alpha_1(x) * \alpha_2(y)$$

*always holds. They are* **strongly isotopic** *if we can choose $\alpha_2 = \alpha_1$.*

This notion of equivalence is motivated by the fact that two presemifields are isotopic if and only if the corresponding projective planes are isomorphic. Let $F = \mathbb{F}_{p^r}$ be the field of order $p^r$. It is a commonly used method to replace a given commutative semifield of order $p^r$ by an isotopic copy which is defined on $F$ and shares the additive structure and the unit element 1 with $F$. The question is then to which degree the semifield structure can be made to coincide with the field structure. As associativity is the only field axiom that a commutative semifield does not satisfy it is natural that associativity will be in the center of interest.

**Definition 4.** *Let $F = \mathbb{F}_{p^r}$ and $(F, *)$ a commutative semifield with unit 1 whose additive structure agrees with that of the field F. Define*

$$\mathcal{S} = \{c \in F | c * x = cx \text{ for all } x \in F\}.$$

$$\mathcal{M} = \{c \in F | (x * c) * y = x * (c * y) \text{ for all } x, y \in F\}.$$

$$\mathcal{K} = \{c \in F | c * (x * y) = (c * x) * y \text{ for all } x, y \in F\}.$$

Here the dimensions of the **middle nucleus** $\mathcal{M}$ and of the **kernel** or **left nucleus** $\mathcal{K}$ of a commutative semifield are invariant under isotopy. The dimension of $\mathcal{S}$ depends on the embedding of the semifield in the field $F$. As mentioned in [5] we have $\mathcal{K} \subseteq \mathcal{M}$ (if $a * (x * y) = (a * x) * y$ for all $x, y$, then this also equals $(a * y) * x = (y * a) * x = (x * a) * y = x * (a * y)$). As $\mathcal{M}$ is closed under semifield multiplication and is associative it is a field. The semifield multiplication on $\mathcal{M}$ can therefore be made to coincide with field multiplication. The same is true of the vector space structure of $F$ over its subfield $\mathcal{M}$. It follows that we can find a suitable isotope such that

$$\mathcal{K} \subseteq \mathcal{M} \subseteq \mathcal{S}.$$

Here are the constructions from [11] and [2]:

**Theorem 2.** *Let $p$ be an odd prime, $q = p^s, q' = p^t, F = \mathbb{F}_{q^3}, s' = s/\gcd(s,t), t' = t/\gcd(s,t), s'$ odd. Let $f : F \longrightarrow F$ be defined by*

$$f(x) = x^{1+q'} - vx^{q^2+q'q} \text{ where } ord(v) = q^2+q+1.$$

*Then $f$ is a PN function in each of the following cases:*

- $s' + t' \equiv 0 \pmod 3$.
- $q \equiv q' \equiv 1 \pmod 3$

**Theorem 3.** *Let $p$ be an odd prime, $q = p^s, q' = p^t, K = \mathbb{F}_q \subset F = \mathbb{F}_{q^4}$ such that $2s/\gcd(2s,t)$ is odd, $q \equiv q' \equiv 1 \pmod 4$. Let $f : F \longrightarrow F$ be defined by*

$$f(x) = x^{1+q'} - vx^{q^3+q'q} \text{ where } ord(v) = q^3+q^2+q+1.$$

*Then $f$ is a PN function.*

The first family of Theorem 2 is constructed in [11], the second family of Theorem 2 and Theorem 3 are from [2]. In the generic case the first family of Theorem 2 is new as was shown in [11]. It was proved in [2] that the semifields of order $p^{4s}$ isotopic to the special case $t = 2, s > 1$ odd of Theorem 3 are not isotopic to Dickson or Albert semifields.

Let $f(x)$ be a Dembowski-Ostrom polynomial which is a PN function and $*$ the corresponding presemifield product $(x * y = (1/2)\{f(x+y) - f(x) - f(y)\})$. In the following section we decribe a canonical construction of a (commutative) semifield strongly isotopic to $(F, *)$ which allows to read off information on the nuclei directly from $f(x)$. In the last section we continue studying low-dimensional subfamilies of the planar functions of Theorems 2,3. In particular we describe 12-dimensional semifields with middle nucleus of dimension 2 and kernel $\mathbb{F}_p$ as well as a new family of 9-dimensional semifields. In the sequel $p$ always denotes an odd prime.

This is a corrected version of what appeared in the proceedings of AAECC-18 (Tarragona, 2009). In the earlier version we used the interpretation given in [4] of a result of Menichetti [10]. It is stated in [4]: *Menichetti showed that a commutative semifield which is three-dimensional over its middle nucleus is necessarily Albert's commutative twisted field.* This statement is not correct. In the earlier version of the present paper this erroneous statement was used in two occasions. In the proof of Theorem 6 it is in fact not needed and the statement of the theorem remains unchanged. Theorem 7 in contrast is affected. We no longer claim that the middle nucleus is the prime field. It may as well be 3-dimensional.

## 2 From commutative presemifields to semifields in odd characteristic

**Definition 5.** *Let $f(X)$ be a DO-polynomial defined on $F = \mathbb{F}_{p^r}$ for odd $p$. Let $G = Gal(F|\mathbb{F}_p) = \{g_0 = id, g_1, \ldots, g_{r-1}\}$ be the Galois group where $g_i(x) = x^{p^i}$. Write*

$$f(X) = \sum_{i=0}^{r-1} a_i g_i(X^2) + \sum_{j<k} b_{jk} g_j(X) g_k(X)$$

*where $a_i, b_{jk} \in F$. If $f(X)$ is also a planar function, then the presemifield product defined by $f(X)$ is*

$$x * y = \sum_i a_i g_i(xy) + \sum_{j<k} (b_{jk}/2)(g_j(x)g_k(y) + g_k(x)g_j(y))$$

*Let $t_i(X) = X^{p^i} - X$.*

**Lemma 1.** *$t_{mu}(X)$ is a polynomial in $t_m(X)$.*

*Proof.* Let $Q = p^m$. Then $t_{mu}(X) = t_m(X)^{Q^{u-1}} + t_m(X)^{Q^{u-2}} + \cdots + t_m(X) = g_{(u-1)m}(t_m(X)) + \cdots + t_m(X)$. □

**Proposition 1.** *Let $p$ odd, $F = \mathbb{F}_{p^r}$ and $(F, *)$ a commutative presemifield. Let $\alpha \in GL(r, p)$ and define a product $\circ$ by*

$$\alpha(1) * \alpha(x \circ y) = \alpha(x) * \alpha(y).$$

*Then $(F, \circ)$ is a commutative semifield with unit $1$. It is strongly isotopic to $(F, *)$.*

*Proof.* Obviously $(F, \circ)$ is a commutative presemifield. It is related to $(F, *)$ by the strong isotopy $\beta(x \circ y) = \alpha(x) * \alpha(y)$ where $\beta(x) = \alpha(1) * \alpha(x)$. Choosing $y = 1$ shows $\alpha(1) * \alpha(x \circ 1) = \alpha(x) * \alpha(1)$. It follows $x \circ 1 = x$. □

In case $\alpha = id$ we obtain $1 * (x \circ y) = x * y$. This is made explicit in the following definition and theorem.

**Definition 6.** *Let $F = \mathbb{F}_{p^r}$ for odd $p$ and $f(x)$ a planar DO-polynomial on $F$. The* **associated semifield function** *is $B(f(x))$ where $B \in GL(r, p)$ is the inverse of $A(x) = x * 1$. The* **associated semifield product** *is the product $\circ$ defined by $B(f(x))$.*

**Theorem 4.** *Let $f(X) = \sum_{i=0}^{r-1} a_i g_i(X^2) + \sum_{j<k} b_{jk} g_j(X) g_k(X)$ be a planar function on $F = \mathbb{F}_{p^r}$ for odd $p$, with presemifield product $*$ and associated semifield product $\circ$ (see Definition 6). Let $m$ be the greatest common divisor of $r$ and the numbers $k-j$ where $j<k$ is such that $b_{jk} \neq 0$. Then $\mathbb{F}_{p^m} \subseteq \mathcal{M}(F, \circ) \cap \mathcal{S}(F, \circ)$.*

*Proof.* Let $x * y$ be the presemifield product defined by $f(X)$. We have

$$A(x) = x * 1 = \sum a_i g_i(x) + \sum_{j<k} (b_{jk}/2)(g_j(x) + g_k(x))$$

and

$$f(x) = A(x^2) + \sum_{j<k} (b_{jk}/2)(2g_j(x)g_k(x) - g_j(x^2) - g_k(x^2)).$$

The expression in parenthesis is

$$2g_j(x)g_k(x) - g_j(x^2) - g_k(x^2) = -(g_k(x) - g_j(x))^2 = -g_j(t_{k-j}(x)^2).$$

This yields the associated semifield function

$$B(f(x)) = x^2 - B(\sum_{j<k} (b_{jk}/2) g_j(t_{k-j}(x)^2))$$

and the associated semifield product

$$x \circ y = xy - B(\sum_{j<k} (b_{jk}/2) g_j(t_{k-j}(x) t_{k-j}(y)).$$

This follows from the linearity of Equation 1 and the fact that a term $x^2$ in the planar function turns into $xy$ in the presemifield product. Observe that $t_{mu}(X)$ is a polynomial in $t_m(X)$ by Lemma 1. Let $c \in \mathbb{F}_{p^m}$. Then $c \circ x = cx$ as $t_m(c) = 0$. This shows $\mathbb{F}_{p^m} \subseteq \mathcal{S}(F, \circ)$. In order to show $\mathbb{F}_{p^m} \subseteq \mathcal{M}(F, \circ)$ it remains to be shown $(cx) \circ y = x \circ (cy)$ for all $x, y$. This also follows directly from the fact that $t_{k-j}(cx) = c t_{k-j}(x)$ for all $k, j$ such that $b_{jk} \neq 0$. □

**Theorem 5.** *In the situation of Theorem 4 let $l$ be the greatest common divisor of $r$ and the numbers $i, j, k$ where $a_i \neq 0$ and $j < k$ such that $b_{jk} \neq 0$. Then the associated semifield has $\mathbb{F}_{p^l}$ in its left nucleus.*

*Proof.* Let $c \in \mathbb{F}_{p^l}$. We have to show $(cx) \circ y = c(x * y)$. This follows from the form of $B(f(x))$ as given in the proof of Theorem 4 and the fact that $A(x)$ and its inverse $B(x)$ are linear over $\mathbb{F}_{p^l}$. □

## 3 Some semifields and their nuclei

**Theorem 6.** *The semifields of order $p^{12}$ associated to the presemifields in case $s = 3, t = 2$ of Theorem 3 have middle nucleus $\mathbb{F}_{p^2}$ and kernel $\mathbb{F}_p$.*

*Proof.* We have $p \equiv 1 \pmod 4), F = \mathbb{F}_{p^{12}}$ and $ord(v) = p^9 + p^6 + p^3 + 1$. The planar function is

$$f(x) = x^{1+p^2} - vx^{p^5+p^9}.$$

It follows from Theorem 4 that the middle nucleus $\mathcal{M}$ of the associated semifield $(F, \circ)$ has even dimension. It was shown in [2] that $dim(\mathcal{M})$ is not a multiple of 6. It follows from Lemma 8 of [2] that $dim(\mathcal{M})$ is not a multiple of 4 either. It follows $\mathcal{M} = \mathbb{F}_{p^2}$. We have

$$x \circ y = xy - (1/2)B(t_2(x)t_2(y)) + (1/2)B(vg_5(t_4(x)t_4(y)))$$

(see the proof of Theorem 4) and $t_4(X) = t_2(X) + g_2(t_2(X))$. Let $K(X, Y)$ be the polynomial such that $x \circ y = xy + K(t_2(x), t_2(y))$. Then

$$K(X, Y) = -(1/2)B(XY - vg_5((X + X^{p^2})(Y + Y^{p^2})) =$$

$$= -(1/2)B(XY - v(XY)^{p^5} - v(XY)^{p^7} - vX^{p^5}Y^{p^7} - vX^{p^7}Y^{p^5}).$$

Assume $dim(\mathcal{K}) > 1$. Then $\mathcal{K} = \mathcal{M} = \mathbb{F}_{p^2}$. It has been proven in [5], Theorem 4.2, that this is equivalent with $K(X, Y)$ being a polynomial in $X^{p^2}$ and $Y^{p^2}$. Although we do not know $B$ explicitly it is obvious that this condition cannot be satisfied. In fact, let $B(x) = \sum_{i=0}^{11} \beta_i g_i(x)$. The absence of monomials $X^{p^i}Y^{p^{i+2}}$ for odd $i$ shows $\beta_0 = \beta_2 = \cdots = \beta_{10} = 0$. As $(XY)^{p^i}$ is absent for odd $i$ we have $0 = \beta_i - g_{i-5}(v)\beta_{i-5} - g_{i-7}(v)\beta_{i-7} = \beta_i$. This yields the contradiction $B \equiv 0$. □

We turn to Theorem 2. The smallest dimension for which new planar functions may result is $r = 9$ for the second subfamily. Here $t$ should not be a multiple of 3 as otherwise a field or an Albert twisted field is obtained. Up to obvious isotopy equivalences there are three cases, $f(x) = x^{1+p} - vx^{p^4+p^6}$, $f(x) = x^{1+p} - vx^{p^3+p^7}$, $f(x) = x^{1+p^2} - vx^{p^3+p^8}$. We show that those yield new semifields:

**Theorem 7.** *Let $p \equiv 1$ (mod 3), $q = p^3, K = \mathbb{F}_q \subset F = \mathbb{F}_{p^9}$ and $ord(v) = q^2 + q + 1$. The semifields of order $p^9$ associated to the planar functions*

$$f(x) = x^{1+p} - vx^{p^4+p^6}, \; f(x) = x^{1+p} - vx^{p^3+p^7} \text{ or } f(x) = x^{1+p^2} - vx^{p^3+p^8}$$

*are not isotopic to a commutative Albert semifield.*

*Proof.* There are four cases to consider. Corresponding presemifields are described by the monomial planar functions $X^{1+p^s}$ where $s \in \{1,2,3,4\}$. Here case $s=3$ corresponds to the uniquely determined Albert semifield with nucleus of dimension 3, the remaining values of $s$ are representatives of the three isotopism classes of commutative Albert presemifields whose corresponding semifields have nucleus of dimension 1. Assume we have isotopy with one of those commutative Albert presemifields. It follows from Coulter-Henderson [4], Corollary 2.8 that there is a strong isotopy. There exist invertible linear mappings

$$\alpha(x)=\sum_{i=0}^{8} a_i g_i(x),\ \ \beta(x)=\sum_{i=0}^{8} b_i g_i(x)$$

such that

$$\alpha(x)^{1+p^s}=\beta(f(x)).$$

We complete the proof for the first type $f(x)$. The proofs in the remaining cases are analogous. Observe that in the exponents modular distances (in the circle of length 9) $d=0, d=3, d=4$ do not occur. In the case of distance $d=0$ this yields $a_i a_{i+s}=0$ for all $i$. The equations for $d=3$ and $d=4$ are the following:

$$a_i g_s(a_{i+3-s})+a_{i+3} g_s(a_{i-s})=0.$$

$$a_i g_s(a_{i+4-s})+a_{i+4} g_s(a_{i-s})=0.$$

Without restriction $a_0 \neq 0$. It follows $a_s=a_{-s}=0$. Evaluating the $d=3$ equation for $i \in \{0,-3,s,s-3\}$ and the $d=4$ equation for $i \in \{0,-4,s,s-4\}$ shows $a_i=0$ for $i \in \pm\{s, s-3, s-4, s+3, s+4\}$. For $s=3$ or $s=4$ this yields the contradiction $a_0=0$. For $s=1$ or $s=2$ the contradiction $a_i=0$ for all $i \neq 0$ is obtained. □

# References


[1] Albert, A.A.: On nonassociative division algebras, Transactions of the American Mathematical Society, vol. 72, pp. 296–309 (1952)

[2] Bierbrauer, J.: New semifields, PN and APN functions, *Designs, Codes and Cryptography,* to appear.

[3] Budaghyan, L. and Helleseth, T.: New perfect nonlinear multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime $p$, LNCS, vol. 5203, SETA, pp. 403-414 (2008)

[4] Coulter, R.S. and Henderson, M.: Commutative presemifields and semifields, Advances in Mathematics, vol. 217, pp. 282–304 (2008)

[5] Coulter, R.S., Henderson, M., Kosick, P.: Planar polynomials for commutative semifields with specified nuclei, Designs, Codes and Cryptography, vol. 44, pp. 275–286 (2007)

[6] Coulter, R.S. and Matthews, R.W.: Planar functions and planes of Lenz-Barlotti class II, Designs, Codes and Cryptography, vol 10, pp. 167–184 (1997)

[7] Dickson, L.E.: On commutative linear algebras in which division is always uniquely possible, Transactions of the American Mathematical Society, vol. 7, pp. 514–522 (1906)

[8] Horadam, K. J.: Hadamard matrices and their applications, Princeton University Press (2007).

[9] Kantor, W. M.: Commutative semifields and symplectic spreads, Journal of Algebra, vol. 270, pp. 96–114 (2003)

[10] Menichetti, G.: On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field, Journal of Algebra, vol. 47, pp. 400–410 (1977)

[11] Zha, Z., Kyureghyan, G. M., Wang, X.: Perfect nonlinear binomials and their semifields, Finite Fields and Their Applications, vol. 15, pp. 125-133 (2009).