New semifields, PN and APN functions

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

December 14, 2008

1 Introduction

In the theory of functions with extreme nonlinearity properties there is a sharp dichotomy between the characteristic 2 and the odd characteristic case. In characteristic 2 part of the motivation comes from the cryptographic theory of S-boxes. The relevant notion is as follows:

Definition 1. *Let $F = \mathbb{F}_{2^n}$. A function $f : F \longrightarrow F$ is* **almost perfectly nonlinear** *(APN) if for every $0 \neq a \in F$ the directional derivative $f(x + a) - f(x)$ is two-to-one.*

The notion goes back to K. Nyberg [17] and arose in the theory of S-boxes, the main objective being to guarantee protection agains linear attacks. In the odd characteristic case it is possible to obtain bijective directional derivatives:

Definition 2. *Let $F = \mathbb{F}_{p^n}$ 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 (defined as above) is bijective.*

The link to cryptography is lost in odd characteristic, but instead there are close connections to algebra and finite geometries. We may think of f as a polynomial with coefficients in F.

Definition 3. *Let $F = \mathbb{F}_{p^n}$ for an odd prime p. A function $f : F \longrightarrow F$ is a* **Dembowski-Ostrom** *(DO-)polynomial if all its monomials have p-weight ≤ 2 (the exponents are sums of two powers of p).*

The algebraic representation of a PN function arises from a simple change of perspective: choose f without restriction such that $f(0) = 0$ and interpret $f(x+a)-f(x)-f(a)$ as a product $a*x \in F$. Then $a*x = x*a$ and $a*x = 0$ if and only if either $a = 0$ or $x = 0$. If moreover f is a DO-polynomial, then $*$ is biadditive. This leads to the notions of a presemifield and a semifield.

Definition 4. *A* **presemifield** *is a set F with two binary relations, addition and $*$, such that*

- *F is a commutative group with respect to addition.*
- *F^* is a loop under multiplication.*
- *$0 * a = 0$ for all a.*
- *The distributive law holds.*

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

We saw that each planar DO-polynomial yields a commutative presemifield. The discovery that those concepts are equivalent is surprisingly new (Coulter-Henderson [10]):

Theorem 1. *The following concepts are equivalent:*

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

The translation mechanism is formally equivalent to the relation between quadratic forms and bilinear forms in odd characteristic, with the planar function in the role of the quadratic form. The corresponding presemifield product is described by

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

In the other direction define $f(x) = x * x$. Observe that in general the notions of commutative semifields and planar functions do not coincide. In characteristic 2 there are no planar functions. On the other hand there exist planar functions which are not DO-polynomials and therefore do not define semifields (see Coulter-Matthews [12]).

One way to turn a presemifield into a semifield is the following: choose your favorite element $e \in F$ which you want to play the role of the unit element and define the new multiplication $\circ$ by

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

With respect to the new multiplication $\circ$ we still have a presemifield, and the element $e * e$ is the unit element.

The geometric representation of a commutative semifield is a special type of a translation plane, which is also a dual translation plane.

In the present paper we introduce a large family of functions and a general method which can be used to prove that certain parametric subfamilies are APN (in the characteristic 2 case) respectively PN (see Section 2). Many of those subfamilies have been considered in earlier work. Historically the starting point was G. Kyureghyan's proof [16] that the Gold functions are the only crooked power functions. The method of proof finally led to our result [4] that crooked binomials must be quadratic. This motivated Y. Edel to conduct a computer search for crooked and APN functions. He found many examples, the smallest of which is a binomial defined on $\mathbb{F}_{2^{10}}$. It was proved in [14] that this sporadic example is not equivalent to a power function. The remaining crooked binomials produced by Edel obviously come in two families. The proof of the APN property for the corresponding infinite families of binomials was given in [6, 7, 8]. In [3] we obtain a greatly simplified proof for the APN property of the two families of binomials. The discovery that the first of those series can be generalized to obtain families of new planar functions is made in [18], thus obtaining the first provably new construction of commutative semifields in arbitrary odd characteristic after the classical work of Dickson [13] and Albert [1], see Kantor [15].

The general outline of the method of proof is given in Section 2, followed in Section 3 by illustrations of the proof method resulting in a family of APN trinomials (Theorem 2) and a simplified proof for the APN trinomials from [5]. The parametric family of binomial functions which is the main object of the paper is defined in Section 4. It comes in two subfamilies: the underlying field is represented either as a cubic extension (case $k = 3$) or as a biquadratic extension (case $k = 4$). In the characteristic 2 case a proof of the APN property using our method is in [3]. We concentrate therefore on the odd characteristic case. Section 4 contains a proof of a slight generalization of [18] as well as the main new construction of the present paper, the planar functions of Theorem 5.

As a commutative semifield satisfies all the properties of a field with the exception of associativity it is natural to ask how far the semifield multiplication is from being associative. The additive group of a commutative semifield is elementary abelian. It is therefore useful to represent the semifield on the field F of the corresponding order, using the same additive group. Write the field multiplication of F as the ordinary multiplication, the semifield multiplication as $\circ$.

Definition 5. *The* **middle nucleus** *of a semifield* $(F, \circ)$ *is*

$$N_m = \{c \in F \mid (x \circ c) \circ y = x \circ (c \circ y) \text{ for all } x, y \in F\}$$

The **left nucleus** *or* **kernel** *is*

$$N_l = \{c \in F \mid (c \circ x) \circ y = c \circ (x \circ y) \text{ for all } x, y \in F\}$$

As mentioned in [11] the kernel of a commutative semifield is contained in the middle nucleus. Section 5 contains information on the kernel and the middle nucleus of our family. In the final Section 6 we study a subfamily of semifields F order p^{4s} where $s > 1$ is odd and $p \equiv 1 \pmod 4$. The main result is that those semifields are not isotopic to Dickson or Albert commutative semifields.

2 A family of functions

Let $q = p^s, K = \mathbb{F}_q \subset F = \mathbb{F}_{q^k}$ and $T : F \longrightarrow K$ the trace. Let $P(X_0, \ldots, X_{k-1}, Y_0, \ldots, Y_{k-1}) = P(X, Y)$ be a homogeneous quadratic polynomial with coefficients in F. Write

$$P(X, Y) = \sum_{0 \le i \le j \le k-1} \alpha_{ij} X_i X_j + \sum_{0 \le i \le j \le k-1} \beta_{ij} Y_i Y_j + \sum_{i,j=0}^{k-1} \gamma_{ij} X_i Y_j.$$

Let $q' = p^t$. Define the function $f : F \longrightarrow F$ by

$$f(x) = P(x, x^q, \ldots, x^{q^{k-1}}, x^{q'}, x^{q'q}, \ldots, x^{q'q^{k-1}}).$$

A large class of functions $f(x)$ constructed in this way are PN functions (in odd characteristic) respectively APN functions in characteristic 2. In each

case $k \leq 4$. Our main result is a family of new PN functions in arbitrary odd characteristic in the case when $k = 4$, see Theorem 5.

In the present section we describe the general method to establish the PN respectively the APN property. Let $\Delta_a(x) = f(x+a) - f(x) - f(a)$ where $0 \neq a \in F$. Then

$$\Delta_a(ax) = \sum_{0 \leq i \leq j \leq k-1} \alpha_{ij}^{q^i+q^j}(x^{q^i} + x^{q^j}) + \sum_{0 \leq i \leq j \leq k-1} \beta_{ij}^{q'(q^i+q^j)}(x^{q'q^i} + x^{q'q^j}) +$$

$$+ \sum_{i,j=0}^{k-1} \gamma_{ij}^{q^i+q'q^j}(x^{q^i} + x^{q'q^j}).$$

The function $f(x)$ is APN if $p = 2$ and $\Delta_a(ax)$ has a kernel of binary dimension 1 for all $a \neq 0$. It is PN if $p > 2$ and $\Delta_a(ax)$ is invertible for all $a \neq 0$. We assume $k \leq 4$. The method proceeds as follows:

1. **Separation:** For suitable $c \in F$ consider the equation $T(c\Delta_a(ax)) = 0$. Collect all terms involving q' in the exponent on the right side side. By elementary properties of the trace this equation can be written in the form $T(c_1 x) = T(c_2 x^{q'})$. Here the coefficients $c_1, c_2 \in F$ depend on c.

2. **The K-linear equations:** Find values of c such that either $c_1 = 0, c_2 \neq 0$ or vice versa. This leads to equations $T(c_2 x^{q'}) = 0$ in the first case, $T(c_1^{q'} x^{q'}) = 0$ in the second case.

3. **non-degeneracy:** Show that the two K-linear equations for the unknown $x^{q'}$ obtained in the preceding step are linearly independent.

4. **Reduction:** Show that $x \in K$ satisfies both equations in case $k = 3$. Show that $x \in L = \mathbb{F}_{q^2}$ satisfies both equations in case $k = 4$.

5. **Final step:** show that for arbitrary $a \neq 0$ and $x \in K$ (when $k = 3$) respectively $x \in L$ (for $k = 4$) the kernel of the linear mapping $\Delta_a(ax)$ has the required dimension over the prime field: 0 in odd characteristic, 1 in characteristic 2.

3 Some APN-trinomials

As a first illustration of the method described in Section 2 we prove the following

Theorem 2. *Let s be odd, t even such that $t < 2s, \gcd(t,s) = 1$. Let $q = 2^s, q' = 2^t, F = \mathbb{F}_{q^2}, v \in F \setminus \mathbb{F}_q$ and $v \notin (F^*)^3$. Then*

$$f(x) = ux^{1+qq'} + u^q x^{q+q'} + vx^{q'(1+q)}$$

is an APN function.

Proof. In the terminology of Section 2 we have $p = 2, k = 2, K = \mathbb{F}_q$. The underlying quadratic polynomial is $P(X_0, X_1, Y_0, Y_1) = uX_0Y_1 + u^qX_1Y_0 + vY_0Y_1$. For $0 \neq a \in F$ consider

$$\Delta_a(ax) = ua^{1+q'q}(x + x^{q'q}) + u^q a^{q'+q}(x^q + x^{q'}) + va^{q'(1+q)}(x^{q'} + x^{q'q}).$$

As $k = 2$ we need only one K-linear equation. The result of the separation step (with $c = 1$) is

$$T((v + v^q)a^{q'+q'q}x^{q'}) = 0$$

This is non-trivial as $v \notin K$. It follows $x \in K$. The original equation simplifies:

$$\Delta_a(ax) = (ua^{1+q'q} + u^q a^{q'+q})(x + x^{q'}) = 0.$$

As $\gcd(t,s) = 1$ we have $x + x^{q'} = 0$ only for $x \in \mathbb{F}_2$. It remains to be shown that $ua^{1+qq'} \notin K$. This follows from the fact that $a^{1+qq'}$ and the elements of K are third powers while u is not. □

Next we give a construction of the APN-trinomials from [5] with the method of Section 2.

Theorem 3. *Let s, t be coprime to 3, $s+t$ divisible by 3 and $t < 3s, \gcd(t,s) = 1$. Let $q = 2^s, q' = 2^t, F = \mathbb{F}_{q^3}, v \in \mathbb{F}_q$ and $u \in F \setminus (F^*)^7$. Then*

$$f(x) = ux^{q^2+qq'} + u^q x^{1+q'} + vx^{q'(1+q)}$$

is an APN function.

Proof. In the language of Section 2 we have $p = 2, k = 3$ and $P(X,Y) = uX_2Y_1 + u^qX_0Y_0 + vY_0Y_1$. Then

$$\Delta_a(ax) = ua^{q^2+q'q}(x^{q^2} + x^{q'q}) + u^q a^{1+q'}(x + x^{q'}) + va^{q'+q'q}(x^{q'} + x^{q'q}).$$

The equation $T(c\Delta_a(ax)) = 0$ (separation step) yields

$$T((c^q u^q a^{1+q'q^2} + cu^q a^{1+q'})x_0) = T((c^{q^2} u^{q^2} a^{q'+q} + cu^q a^{1+q'} + cva^{q'+q'q} + c^{q^2} va^{q'+q'q^2})x^{q'})$$

The choice $c = a^{q'q^2}$ annihilates the left side. On the right side the terms containing v cancel. With $\alpha = u^q a^{1+q'+q'q^2}$ the first K-linear condition is

$$T((\alpha + \alpha^q)x^{q'}) = 0.$$

The factor on the right side vanishes with the choice $c = u^{q^2}a^q + va^{q'q^2}$. Let $\beta = u^{1+q}a^{1+q^2+q'q^2}$. The second K-linear condition is

$$T((\beta + \beta^q)^{q'}x^{q'}) = 0.$$

Let $\phi = u^q a^{1+q'q^2} + u^{q^2}a^{q+q'q}$. Then

$$\alpha + \alpha^q = a^{q'}\phi,\ \beta + \beta^q = u^q a\phi^q.$$

The conditions on s, t guarantee $\alpha, \beta \notin K$ and $K^* \subseteq (F^*)^7$. In particular $\phi \neq 0$. Assume the K-linear conditions are dependent, equivalently $(\beta + \beta^q)^{q'}/(\alpha + \alpha^q) = u^{q'q}\phi^{qq'-1} \in K$. It follows $u \in (F^*)^7$, contradiction. As the K-linear conditions are linearly independent we have shown $x \in K$. Equation $\Delta_a(ax) = 0$ simplifies to

$$(ua^{q^2+q'q} + u^q a^{1+q'})(x + x^{q'}) = 0.$$

As $\gcd(t, s) = 1$ the second factor vanishes only when $x \in \mathbb{F}_2$. Assume the first factor vanishes. This is equivalent with $u^{q-1} = a^{(q-1)(q'+q+1)}$ which is not true as the right side is in $(F^*)^7$ and $u \notin (F^*)^7$. □

4 A family of PN-functions

In this section we consider the family corresponding to case $P(X, Y) = X_0Y_0 - vX_{k-1}Y_1$ of Section 2 where $k = 3$ or $k = 4$. The characteristic 2 cases are the objective of [6, 7, 8, 3]. Case $k = 3$ in odd characteristic corresponds to the main result of [18]. Our new result (Theorem 5) is obtained in the subcase when $k = 4$ in odd characteristic. At first consider general k.

Definition 6. *Let p be an odd prime, $q = p^s, q' = p^t, K = \mathbb{F}_q \subset F = \mathbb{F}_{q^k}$ and $T : F \longrightarrow K$ the trace. Let $P(X_0, \ldots, X_{k-1}, Y_0, \ldots, Y_{k-1}) = X_0Y_0 - vX_{k-1}Y_1$ where $v \in (F^*)^{q-1}$ and $f : F \longrightarrow F$ defined by*

$$f(x) = P(x, x^q, \ldots, x^{q^{k-1}}, x^{q'}, \ldots, x^{q'q^{k-1}}).$$

The following lemma is obvious from the results of Section 2.

Lemma 1. *Under the assumptions of Definition 6 we have*

$$\Delta_a(ax)/a^{1+q'} = (x + x^{q'}) - u(x^{q^{k-1}} + x^{q'q}),$$

where $u = va^m = w^{q-1} \in (F^*)^{q-1}$, $m = q^{k-1} + qq' - q' - 1 = (q-1)(q' + q^{k-2} + \cdots + 1)$.

Lemma 2. *Under the assumptions of Definition 6 equation* $\Delta_a(ax) = 0$ *implies the following:*

$$T((1/w^{q^{k-1}} - 1/w^q)x^{q'}) = 0$$

$$T((w^{q'} - w^{q'q^2})x^{q'}) = 0.$$

Those conditions are satisfied for $x \in K$ *when* $k = 3$ *and for* $x \in L = \mathbb{F}_{q^2}$ *in case* $k = 4$.

Proof. The equation $T(c\Delta_a(ax)/a^{1+q'}) = 0$ (the separation step) yields

$$T((c - c^q u^q)x) = T((c^{q^{k-1}} u^{q^{k-1}} - c)x^{q'}).$$

The choices $c = 1/w^q$ and $c = w$ make one of the sides vanish. The K-linear equations follow. □

In order to verify non-degeneracy the following criterion is instrumental:

Lemma 3. *The two* $\mathbb{F}_q$*-linear conditions on* $x^{q'}$ *in Lemma 2 are linearly dependent over* K *if and only if*

$$1/u^{q+q'} = (1 - u^{1+q^{k-1}})^{(q-1)(qq'-1)}.$$

Proof. Assume they are linearly dependent. Write $a \sim b$ if $a/b \in \mathbb{F}_q$. We have

$$1/w^{q^{k-1}} - 1/w^q \sim (w - w^{q^2})^{p^i}.$$

Factor out $1/w$ on the left and w^{p^i} on the right, use $w^{q^{k-1}}/w = 1/u^{q^{k-1}}$:

$$(u^{1+q^{k-1}} - 1)/(wu) \sim w^{p^i}(1 - u^{1+q})^{p^i}.$$

Raising to power $q - 1$ yields the claim. □

Lemma 4. *Let* $d' = |(F^*)^{q-1}/(F^*)^m|$. *Then* $d' = \gcd(q^{k-1}+\cdots+1, q^{k-1}-q')$ *divides* $p^{\gcd(ks,(k-1)s-t)} - 1$.

Proof. By definition $d' = \gcd(q^{k-1}+\cdots+1, q'+q^{k-2}+\cdots+1)$. □

At first we prove a slight generalization of the main result of [18]:

Theorem 4. *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:*

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

Proof. We are in the situation of Definition 6. Let $P = p^{\gcd(s,t)}$.

Lemma 5. d' *is divisible by* P^2+P+1 *if* $s'+t' \equiv 0 \pmod 3$. *We have* $d' = 3$ *if* $s'+t' \not\equiv 0 \pmod 3, q \equiv q' \equiv 1 \pmod 3$ *and* $d' = 1$ *in all other cases.*

Proof. In the first case we have $\gcd(3s, 2s-t) = 3 \times \gcd(s,t)$ and the claim is obviously true. Let $s'+t' \not\equiv 0 \pmod 3$, equivalently $\gcd(3s, 2s-t) = \gcd(s,t)$. Then d' divides q^2+q+1 and also $q-1$ and therefore $d' \mid \gcd(q^2+q+1, q-1) = \gcd(q-1, 3)$. The claim follows. □

Consider $\Delta_a(ax) = 0$. Assume the two K-linear equations of Lemma 2 are dependent. Use the equation of Lemma 3. In the first case of Theorem 4 the exponent $qq'-1 = P^{s'+t'}-1$ on the right is a multiple of P^3-1. It follows that the right side is in $Z = (F^*)^{(q-1)(P^2+P+1)}$. Recall $u = va^m$ and $a^m \in Z$. It follows $v^{q+q'} \in Z$. As v generates $(F^*)^{q-1}$ it must be that $q+q' = P^{s'}+P^{t'}$ is a multiple of P^2+P+1. This is not the case.

In the second case of Theorem 4 we have $d' = 3$ (see Lemma 5). The right side of the equation in Lemma 3 is in $(F^*)^m$. The exponent on the left side is $q+q' \equiv 2(\bmod 3)$, contradiction.

It follows that we can assume $0 \neq x \in K$. By Lemma 1 equation $\Delta_a(ax) = 0$ simplifies to $(1-u)(x+x^{q'}) = 0$. As s' is odd, $x+x^{q'} \neq 0$. As $d' > 1$ we have $v \notin (F^*)^m$ and $u = va^m \neq 1$, contradiction. □

Our new family of planar functions arises in case $k = 4$.

Theorem 5. *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.

Proof. The assumptions of Definition 6 are satisfied.

Lemma 6. *We have $d' = 4$. If Z is the subgroup of order $q+1$, then $|(F^*)^{q-1}/(Z(F^*)^m)| = 2$. In particular $u \notin Z$ and $u \notin (F^*)^m$.*

Proof. We have $d' = \gcd((q+1)(q^2+1), q^3/q' - 1)$ and

$$\gcd(q^3/q' - 1, q - 1) = p^{\gcd(t,s)} - 1, \gcd(q^3/q' - 1, q^4 - 1) = p^{\gcd(3s-t,4s)} - 1,$$

$$\gcd(q - 1, q^3 + q^2 + q + 1) = \gcd(q - 1, 4) = 4.$$

Let $s = 2^i s_0$ for odd s_0. Then $t = 2^{i+1}t_0$. Let $\gcd(3s-t, 4s) = c\gcd(t,s)$. Then c is odd as a common divisor $2\gcd(t,s)$ would divide t and therefore also $3s$, contradiction. As c is odd we have that $c\gcd(t,s)$ divides s and t. It follows $\gcd(3s-t, 4s) = \gcd(t,s)$. This shows that the common divisor of $q^3/q' - 1$ and $q^4 - 1$ divides $q - 1$. It follows $d' = \gcd(q^3/q' - 1, 4) = \gcd(q - 1, 4) = 4$. The remaining claims follow. □

Consider the equation of Lemma 1. Only two of the proof steps described in Section 2 remain to be taken. Assume the two K-linear equations of Lemma 2 are dependent. The right side of the equation in Lemma 3 is in $(F^*)^m$, the left side is not.

It has been proved that $x \in L = \mathbb{F}_{q^2}$. The original equation becomes $x + x^{q'} = u(x^q + x^{q'q})$. As $2s/gcd(t, 2s)$ is odd we have $x + x^{q'} \neq 0$. It follows that u is a $(q-1)$-st power of an element in L. This is not true as $u \notin Z$. □

5 Towards the nuclei

Theorem 6. *The semifields isotopic to the presemifields determined by the planar functions of Theorem 5 have left nucleus of dimension a multiple of $\gcd(s,t)$ and middle nucleus of dimension a multiple of $\gcd(2s,t)$.*

Proof. Let $J = GF(p^{\gcd(4s,t)})$. Then $L = \mathbb{F}_{q^2}$ is of odd degree over $J \cap L$, and $J \cap L$ has degree 2 over $J \cap K$.

Define a presemifield product corresponding to the planar function $f(x)$ as

$$x * y = \frac{f(x+y) - f(x) - f(y)}{4 - 4v} = \frac{1}{2 - 2v}(xy^{q'} + x^{q'}y - vx^{q^3}y^{q'q} - vx^{q'q}y^{q^3}).$$

In particular $1 * 1 = 1$. The semifield product $\circ$ is defined by $(x * 1) \circ (y * 1) = x * y$.

Let $c \in J \cap K = GF(p^{\gcd(s,t)})$. Then

$$c * 1 = c, \ c * y = c(1 * y) = (cy) * 1 \text{ for all } y.$$

As

$$(c * 1) \circ ((x * 1) \circ (y * 1)) = (c * 1) \circ (x * y)$$

and

$$((c * 1) \circ (x * 1)) \circ (y * 1) = (cx * 1) \circ (y * 1) = (cx) * y = (c * 1) \circ (x * y)$$

it follows that $J \cap K$ is in the left nucleus of the semifield $(F, \circ)$.

Let $c \in J \cap L$. We show that $c * 1$ is in the middle nucleus of $(F, \circ)$. Here $c * 1 = \frac{1}{1-v}\{c - vc^q\}$ and $x * c = (cx) * 1$ for all x. It follows

$$((x * 1) \circ (c * 1)) \circ (y * 1) = (cx * 1) \circ (y * 1) = (cx) * y$$

$$(x * 1) \circ ((c * 1) \circ (y * 1)) = x * (cy).$$

As $x * (cy) = (cx) * y$ for all x, y the proof is complete. □

6 Semifields of order p^{4s} for odd $s > 1$.

Consider the subfamily of Theorem 5 corresponding to $p \equiv 1 \pmod 4, t = 2$ and odd $s > 1$. We have the PN function $x^{1+p^2} - vx^{q^3+p^2q}$. The corresponding presemifield product is

$$x * y = \frac{1}{2}(xy^{p^2} + x^{p^2}y - vx^{p^2q}y^{q^3} - vx^{q^3}y^{p^2q}).$$

Let $M = \mathbb{F}_{p^2}$. Observe that

$$(cx) * y = x * (cy) \text{ for all } x, y \in F \text{ and } c \in M. \tag{1}$$

Theorem 7. *A commutative semifield of order p^{4s} isotopic to the special case $t = 2, s > 1$ odd of Theorem 5 is neither quadratic over its middle nucleus nor a commutative Albert semifield.*

The remainder of this section is dedicated to the proof of Theorem 7. Let $*$ be our presemifield product introduced above and assume it is isotopic to a commutative semifield $\circ$ which is either quadratic over its middle nucleus (the **Cohen-Ganley case**) or to a commutative Albert semifield (the **Albert case**). Denote by N_m, N_l the middle and left nucleus of $(F, \circ)$, respectively. In the Cohen-Ganley case $N_m = L$, in the Albert case $s = s_1 s_2$ for $s_1 > 1$ and $N_m = N_l = \mathbb{F}_{p^{4s_2}}$. It can be assumed that $c \circ x = cx$ and $(cx) \circ y = x \circ (cy)$ for all $c \in N_m$. Assume there is an isotopy:

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

It has been proved (Theorem 2.6 of [10]) that we can choose $\alpha_2 = m\alpha_1$ where $m \in N_m$ and either $m = 1$ (strong isotopy) or $m \notin N_l$. It follows that in the Albert case we can choose $m = 1$. Write the isotopy relation as

$$\beta(x \circ y) = \alpha(x) * (m\alpha(y))$$

where either $m = 1$ or $m \in N_m \setminus N_l$. Substituting $x = 1$ or $y = 1$ shows

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

In particular β is uniquely determined by α, m and the isotopy takes on the form

$$\alpha(1) * (m\alpha(x \circ y)) = \alpha(x) * (m\alpha(y)). \tag{2}$$

The fact that $\circ$ is in standard form ($(cx) \circ y = x \circ (cy)$ for all x, y and $c \in N_m$) implies

$$\alpha(x) * (m\alpha(cy)) = \alpha(cx) * (m\alpha(y)) \text{ for all } c \in N_m. \tag{3}$$

Let

$$\alpha(x) = \sum_{i=0}^{4s-1} \alpha_i x^{p^i}$$

and $\beta_0 = \alpha_0 + \alpha_2 + \cdots + \alpha_{4s-2}$, $\beta_1 = \alpha_1 + \alpha_3 + \cdots + \alpha_{4s-1}$. For $c \in M = \mathbb{F}_{p^2}$ we have $\alpha(c) = \beta_0 c + \beta_1 c^p$. Restrict the arguments in Equation 3 to M : $\alpha(c) * (m\alpha(d)) = \alpha(1) * (m\alpha(cd))$ for $c, d \in M$. Equivalently

$$(\beta_0 c + \beta_1 c^p) * (m(\beta_0 d + \beta_1 d^p)) = (\beta_0 + \beta_1) * (m(\beta_0 cd + \beta_1 (cd)^p)).$$

After simplification and observing Equation 1 this yields

$$0 = \beta_0 * (m\beta_1(cd^p + c^p d - (cd)^p - cd)) = \beta_0 * (m\beta_1(c - c^p)(d^p - d)).$$

This shows that either $\beta_0 = 0$ or $\beta_1 = 0$. Without restriction assume $\beta_1 = 0$. This implies $\alpha(c) = \beta_0 c$ for $c \in M$. Apply Equation 3 when $y = d \in M$:

$$\alpha(cx) * (m\beta_0 d) = \alpha(x) * (m\beta_0 cd).$$

This implies $\alpha(cx) = c\alpha(x)$ for all $c \in M$. As x is arbitrary a polynomial equality is obtained:

Lemma 7. *Either* $\alpha(x) = \alpha_0 x + \alpha_2 x^{p^2} + \cdots + \alpha_{4s-2} x^{p^{4s-2}}$ *or* $\alpha(x) = \alpha_1 x^p + \alpha_3 x^{p^3} + \cdots + \alpha_{4s-1} x^{p^{4s-1}}$. *Let* $c \in M$. *Then* $\alpha(cx) = c'\alpha(x)$ *where either* $c' = c$ *or* $c' = c^p$.

Definition 7. *For* $i, j = 0, 1, \ldots 4s-1$ *define the modular distance by* $d(p^i + p^j) = |i - j|$ *mod* $4s$.

Consider the isotopy relation Equation 2 in the special case $y = x$:

$$\alpha(1) * (m\alpha(x \circ x)) = \alpha(x) * (m\alpha(x)). \tag{4}$$

In the Cohen-Ganley case all monomials in $x \circ x$ have exponents with modular distances 0 or $2s$. This is still true for the left side of Equation 4. In the Albert case it follows from the normal form of [11] that all modular distances of exponents of monomials on the left are multiples of 4. It will therefore suffice to prove the following:

Lemma 8. *If* $\alpha(x)$ *is as in Lemma 7 and satisfies that* $\alpha(x) * (m\alpha(x))$ *has no monomial terms with exponents of modular distance* 2 *then* α *is the* 0 *polynomial.*

Proof. Clearly it can be assumed $\alpha(x) = \alpha_0 x + \alpha_2 x^{p^2} + \cdots + \alpha_{4s-2} x^{p^{4s-2}}$. We have

$$\alpha(x) * (m\alpha(x)) = \frac{1}{2}(m + m^{p^2})\alpha(x)^{1+p^2} - \frac{v}{2}(m^{p^{s+2}} + m^{p^{3s}})\alpha(x)^{p^{s+2}+p^{3s}}.$$

In the Albert case $m = 1$ and the coefficients are nonzero. Assume $m + m^{p^2} = 0$. Then we are in the Cohen-Ganley case, $m^{p^4} = m$ and $m \in L \cap \mathbb{F}_{p^4} = M$, contradiction. For the same reason $m^{p^{s+2}} + m^{p^{3s}} \neq 0$.

The $2s$ terms with exponents $p^i + p^{i+2}$ for even i appear only in the first summand. The corresponding coefficients have to vanish:

$$\alpha_0^{1+p^2} = -\alpha_2 \alpha_{4s-2}^{p^2},\ \alpha_2^{1+p^2} = -\alpha_4 \alpha_0^{p^2},\ \ldots, \alpha_{4s-2}^{1+p^2} = -\alpha_0 \alpha_{4s-4}^{p^2}.$$

If $\alpha_i = 0$ for one i then all $\alpha_i = 0$. We can assume $\alpha_i \neq 0$ for all $i = 0, 2 \ldots, 4s-2$. Let $\alpha_0 = a,\ \alpha_{4s-2} = ab$. Then $\alpha_0/\alpha_2 = -b^{p^2},\ \alpha_2/\alpha_4 = +b^{p^4}, \ldots$ and in general

$$\alpha_{i-2}/\alpha_i = (-1)^{i/2} b^{p^i} \text{ for even } i. \tag{5}$$

The coefficient of x^{p+p^3} shows $\alpha_{s+1}^{p^{3s}} \alpha_{3s+1}^{p^{s+2}} + \alpha_{s+3}^{p^{3s}} \alpha_{3s-1}^{p^{s+2}} = 0$, equivalently $\alpha_{3s+1} \alpha_{s+1}^{p^{2s-2}} = -\alpha_{3s-1} \alpha_{s+3}^{p^{2s-2}}$ or

$$\alpha_{3s-1}/\alpha_{3s+1} = -(\alpha_{s+1}/\alpha_{s+3})^{p^{2s-2}}.$$

Equation 5 shows

$$(-1)^{(3s+1)/2} b^{p^{3s+1}} = -(-1)^{(s+3)/2} (b^{p^{s+3}})^{p^{2s-2}} = (-1)^{(s+1)/2} b^{p^{3s+1}}.$$

This yields the contradiction $+1 = -1$. □

References

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

[2] S. Ball and M. R. Brown: *The six semifield planes associated with a semifield flock, Advances in Mathematics* **189** (2004), 68-87.

[3] J. Bierbrauer: *A family of crooked functions, Designs, Codes and Cryptography*, to appear.

[4] J. Bierbrauer and G. M. Kyureghyan: *Crooked binomials, Designs, Codes and Cryptography* **46** (2008), 269-301.

[5] C. Bracken, E. Byrne, N. Markin, G. McGuire: New families of quadratic almost perfect nonlinear trinomials and multinomials, manuscript.

[6] L. Budaghyan, C. Carlet, P. Felke, G. Leander: *An infinite class of quadratic APN functions which are not equivalent to power mappings, Proceedings of the IEEE International Symposium on Information Theory 2006, Seattle.*

[7] L. Budaghyan, C. Carlet, G. Leander: *A class of quadratic APN binomials inequivalent to power functions,* submitted.

[8] L. Budaghyan, C. Carlet, G. Leander: *Another class of quadratic APN binomials over* $\mathbb{F}_{2^n}$ *: the case n divisible by* 4, manuscript.

[9] S.D. Cohen and M.J. Ganley: *Commutative semifields, two-dimensional over their middle nuclei, Journal of Algebra* **75** (1982), 373-385.

[10] R.S. Coulter and M. Henderson: *Commutative presemifields and semifields, Advances in Mathematics* **217** (2008), 282-304.

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

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

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

[14] Y. Edel, G. Kyureghyan and A. Pott: *A new APN function which is not equivalent to a power mapping,*
IEEE Transactions on Information Theory **52** (2006), 744-747.

[15] W. M. Kantor: *Commutative semifields and symplectic spreads, Journal of Algebra* **270** (2003), 96-114.

[16] G. Kyureghyan: *Crooked maps in* $\mathbb{F}_{2^n}$, *Finite Fields and Their Applications* **13** (2007), 713-726.

[17] K. Nyberg: *Differentially uniform mappings for cryptography, Advances in Cryptology-EUROCRYPT 93, Lecture Notes in Computer Science* (1994), 55-64.

[18] Z. Zha, G.M. Kyureghyan, X. Wang: *A new family of perfect nonlinear binomials,* manuscript.