A New Family of Perfect Nonlinear Binomials

Zhengbang Zha[1], Gohar M. Kyureghyan[2], and Xueli Wang[3]

[1]College of Mathematics and Econometrics, Hunan University
Changsha 410082, China
[2]Department of Mathematics, Otto-von-Guericke University of Magdeburg,
Universitätplatz 2, 39106 Magdeburg, Germany
[3]School of Mathematical Sciences, South China Normal University,
Guangzhou 510631, China
E-mail: zzb322@yahoo.com.cn; gohar.kyureghyan@ovgu.de; wangxuyuyan@yahoo.com.cn

Abstract

We prove that the binomials $x^{p^s+1} - \alpha x^{p^k+p^{2k+s}}$ define perfect nonlinear mappings in $GF(p^{3k})$ for appropriate choices of the integer s and $\alpha \in GF(p^{3k})$. We show that these binomials are inequivalent to known perfect nonlinear monomials. As a consequence we obtain new commutative semifields for $p \geq 5$ and odd k.

Keywords: Perfect nonlinear; Planar functions; Almost perfect nonlinear; Commutative semifields

1 Introduction

Let p be a prime and $f : GF(p^n) \to GF(p^n)$. Denote by $N(a,b)$ the number of solutions $x \in GF(p^n)$ of $f(x+a) - f(x) = b$ where $a, b \in GF(p^n)$, and let $\Delta_f = \max\{N(a,b) | a, b \in GF(p^n), a \neq 0\}$. In [17] a mapping f is called differentially k-uniform if $\Delta_f = k$. To resist the differential cryptanalysis the mapping f used in the S-box of a DES-like cryptosystem must have a small differential uniformity. A differentially 2-uniform function is called almost perfect nonlinear (APN). Since $f(x+a) + f(x) = f((x+a)+a) + f(x+a)$ for any $f : GF(2^n) \to GF(2^n)$ and $a \in GF(2^n)$, the APN mappings provide the minimal uniformity over $GF(2^n)$.

The differentially 1-uniform functions are called perfect nonlinear (PN). They exist for any odd prime p. In geometry PN mappings are known as planar mappings. Planar mappings were introduced in [10] to describe projective planes with certain properties. In recent papers [7, 8] planar mappings are used to describe new finite commutative semifields of odd order. In [13, 18] it is shown that a planar mapping yields either a skew Hadamard difference set or a Paley type partial difference set depending on $p^n \pmod 4$. In [12, 11] planar and APN mappings are used to construct optimal constant-composition codes and signal sets.

Until recently all known examples of APN mappings in fields of even order were derived from an APN power mapping $x \mapsto x^d$ for some integer d. In [14] it is shown that the APN mappings $x^3 + ux^{36}$ in $GF(2^{10})$ and $x^3 + ux^{528}$ in $GF(2^{12})$, where u is a suitable field element, cannot be obtained from a power one with presently known equivalence transformations. These were the first such examples. The example of $GF(2^{12})$ is shown to be a member of an infinite family [1, 4].

In this paper we show that the binomials introduced in [4] define PN mappings over fields of an odd order. In Section 4 we show that these PN binomials are almost always inequivalent to the known PN monomials. The concept of equivalence of two polynomials is introduced in Section 2. In Section 5 we briefly survey the connection between PN mappings and finite commutative presemifields and conclude that the founded PN binomials yield new commutative presemifields of order p^{3k} for $p \geq 5$ and odd k.

2 Preliminaries

Let p be a prime. The p-weight of a nonnegative integer m is the sum of the digits in its p-adic representation, i.e. if $m = \sum_i b_i p^i$ then the p-ary weight of m is $\sum_i b_i \in \mathbb{Z}$. Recall, that any mapping of $GF(p^n)$ can be represented by a polynomial over $GF(p^n)$ of degree less than p^n. Moreover, different such polynomials define different mappings. This allows us to identify the set of mappings of $GF(p^n)$ with the set of polynomials over $GF(p^n)$ with degree less than p^n. The algebraic degree of a polynomial over $GF(p^n)$ is the maximal p-weight of the exponents in its nonzero terms.

The $GF(p)$-linear mappings $L : GF(p^n) \to GF(p^n)$ are represented by the polynomials of the algebraic degree 1 and with zero constant term, that is $L(x) = \sum_{i=0}^{n-1} c_i x^{p^i}$, $c_i \in GF(p^n)$. Such polynomials are called linearized or p-polynomials. The sum of a linear mapping and a constant from $GF(p^n)$ is called an affine mapping.

Two mappings $F, G : GF(p^n) \to GF(p^n)$ are called extended affine equivalent (EA-equivalent), if $G = A_1 \circ F \circ A_2 + A$ for some affine permutations A_1, A_2 and affine mapping A. EA-equivalent nonconstant mappings have the same algebraic degree.

Let $(1, \xi)$ be a basis of $GF(p^{2n})$ over $GF(p^n)$. An affine mapping $\mathcal{A} : GF(p^{2n}) \to GF(p^{2n})$ is uniquely described by the linear mappings $L_1, L_2 : GF(p^{2n}) \to GF(p^n)$ and $c \in GF(p^{2n})$ satisfying

$$\mathcal{A}(z) = L_1(z) + L_2(z)\xi + c \quad \text{for any} \quad z \in GF(p^{2n}).$$

A linear mapping $L : GF(p^{2n}) \to GF(p^n)$ is given by a linearized polynomial $\sum_{i=0}^{n-1} a_i z^{p^i} + \big(\sum_{i=0}^{n-1} a_i z^{p^i}\big)^{p^n}$ with $a_i \in GF(p^{2n})$. Further note that if $f : GF(p^n) \to GF(p^n)$ and $x \in GF(p^n)$, then

$$\begin{aligned} L(x + f(x)\xi) &= \sum_{i=0}^{n-1} a_i \big(x + f(x)\xi\big)^{p^i} + \Big(\sum_{i=0}^{n-1} a_i \big(x + f(x)\xi\big)^{p^i}\Big)^{p^n} \\ &= \sum_{i=0}^{n-1} (a_i + a_i^{p^n}) x^{p^i} + \sum_{i=0}^{n-1} \big(a_i \xi^{p^i} + (a_i \xi^{p^i})^{p^n}\big) f(x)^{p^i} \qquad (1) \\ &= \sum_{i=0}^{n-1} b_i x^{p^i} + \sum_{i=0}^{n-1} d_i f(x)^{p^i}, \end{aligned}$$

where $b_i, d_i \in GF(p^n)$.

Two mappings F, $G : GF(p^n) \to GF(p^n)$ are called Carlet-Charpin-Zinoviev equivalent (CCZ-equivalent) if the set $\{x + G(x)\xi \mid x \in GF(p^n)\} \subset GF(p^{2n})$ is the image of the set $\{x + F(x)\xi \mid x \in GF(p^n)\} \subset GF(p^{2n})$ under an affine permutation of $GF(p^{2n})$. In other words, two mapping of $GF(p^n)$ are CCZ-equivalent if their graphs in $GF(p^{2n})$ are affine equivalent. Thus F and G are CCZ-equivalent if and only if there exits an affine permutation $\mathcal{A}(z) = L_1(z) + L_2(z)\xi + c_1 + c_2\xi$ such that

$$y = F(x) \iff L_2(x + y\xi) + c_2 = G(L_1(x + y\xi) + c_1).$$

Then $L_1(x+F(x)\xi)$ is a permutation of $GF(p^n)$ and using (1) it must hold

$$\sum_{i=0}^{n-1} b_i x^{p^i} + \sum_{i=0}^{n-1} d_i F(x)^{p^i} + c_2 = G\big(\sum_{i=0}^{n-1} e_i x^{p^i} + \sum_{i=0}^{n-1} h_i F(x)^{p^i} + c_1\big),$$

where all coefficients b_i, c_i, d_i, e_i, h_i are from $GF(p^n)$.

In [6], it is shown that CCZ-equivalent mappings have equal differential uniformity and that the EA-equivalence is a particular case of the CCZ-equivalence. Over fields of even order there are CCZ-equivalent APN mappings which are not EA-equivalent [5]. To our knowledge, there are not such examples known for PN mappings. So it is not clear whether the CCZ-equivalence does not coincide with the EA-equivalence for PN mappings.

Let p be odd. Currently known EA-inequivalent PN mappings are

(a) x^2 in $GF(p^n)$ (folklore)

(b) x^{p^k+1} in $GF(p^n)$, $k \le n/2$ and $n/(k,n)$ is odd ([10, 9])

(c) $x^{10}+x^6-x^2$ in $GF(3^n)$, $n \ge 5$ is odd ([9])

(d) $x^{10}+x^6+x^2$ in $GF(3^n)$, $n \ge 5$ is odd ([13])

(e) $x^{(3^k+1)/2}$ in $GF(3^n)$, $k \ge 3$ is odd and $(k,n)=1$ ([9, 15]).

Note that the mappings in (a)-(d) are of shape

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

The polynomials of this type are called Dembowski-Ostrom polynomials.

3 A Family of PN binomials in $GF(p^{3k})$

In this section we generalize the results from [1, 4] to the fields of odd order and obtain a new family of PN binomials over $GF(p^{3k})$. Our proof is inspired by the technique from [2, 3] and yields a new simple proof for the APN binomials in the fields of even order.

In the following claim we collect some well known facts that are used in the proofs.

Claim 1. *Let p be a prime.*
(a) *Let $1 \le l \le p^n - 1$ and a be nonzero element from $GF(p^n)$. Then $x^l = a$ has a solution in $GF(p^n)$ if and only if a is a l-th power in $GF(p^n)$.*
(b) *Let u be a primitive element of $GF(p^n)$ and $1 \le l \le p^n - 1$ be a divisor of $p^n - 1$. Then a nonzero element a of $GF(p^n)$ is a l-th power in $GF(p^n)$ if and only if $a = u^r$ with r divisible by l.*
(c) *Let p be odd and $1 \le s \le n-1$. Then the equation $x^{p^s-1} = -1$ has a solution in $GF(p^n)$ if and only if $n/(n,s)$ is even.*

Proof. Statements (a) and (b) are clearly true. To prove (c) recall that $(p^s - 1, p^n - 1) = p^t - 1$ where $t = (s, n)$. Since $-1 = u^{(p^n-1)/2}$, then by (a)-(b) the equation $x^{p^s-1} = -1$ has a solution if and only if $p^t - 1$ is a divisor of $(p^n - 1)/2$. Let $n = t \cdot v$. Then $p^n - 1 = (p^t - 1)(p^{t(v-1)} + \ldots + p^t + 1)$. Thus $p^t - 1$ divides $(p^n - 1)/2$ if and only if $p^{t(v-1)} + \ldots + p^t + 1$ is even or equivalently it has even number of summands.

□

Theorem 1. *Let p be a prime, $n = 3k$ with $(3, k) = 1$ and u be a primitive element of $GF(p^n)$. Choose a positive integer s such that $k - s \equiv 0 \pmod 3$ and set $(s, n) = t$. Then the mapping*

$$F(x) = x^{p^s+1} - u^{p^k-1} x^{p^k + p^{2k+s}}$$

is

- *PN if p and n/t are odd,*
- *APN if $p = 2$ and $t = 1$.*

Proof. Given a nonzero $a \in GF(p^n)$, set $D_a(x) = F(x + a) - F(x) - F(a)$. Then it holds

$$D_a(x) = a x^{p^s} + a^{p^s} x - u^{p^k-1}(a^{p^k} x^{p^{-k+s}} + a^{p^{-k+s}} x^{p^k}). \tag{2}$$

Observe that $D_a(x)$ is linear, and thus the uniformity of $F(x)$ is determined by the maximal dimension of the kernel of $D_a(x)$, $a \in GF(p^n)^*$. So let us consider the equation

$$a x^{p^s} + a^{p^s} x - u^{p^k-1}(a^{p^k} x^{p^{-k+s}} + a^{p^{-k+s}} x^{p^k}) = 0.$$

Substituting ax for x in the above equation we get

$$x + x^{p^s} - \beta(x^{p^{-k+s}} + x^{p^k}) = 0 \tag{3}$$

where

$$\beta = u^{p^k-1}a^{p^{-k+s}+p^k-p^s-1} = u^{p^k-1}a^{(1-p^k)(p^{s-k}-1)}.$$

Observe that β is a (p^k-1)-th power and thus $\beta^{1+p^k+p^{2k}} = 1$.

Given a nonzero $\theta \in GF(p^{3k})$, consider the linearized polynomial

$$L_\theta(X) = X + \theta X^{p^k} + \theta^{p^k+1}X^{p^{2k}}.$$

Suppose that θ is a (p^k-1)-th power, then $L_\theta(y - \theta y^{p^k}) = 0$ for any $y \in GF(p^{3k})$. In particular, $L_\beta(-y + \beta y^{p^k}) = 0$. Thus for any solution x of (3) we get

$$L_\beta(x^{p^s} - \beta x^{p^{-k+s}}) = L_\beta(-x + \beta x^{p^k}) = 0,$$

which implies

$$(1 - \beta^{p^k+1})x^{p^s} + (\beta - 1)x^{p^{k+s}} + (\beta^{p^k+1} - \beta)x^{p^{-k+s}} = 0. \tag{4}$$

Taking equation (4) to the p^{-s}-th power we obtain

$$(1 - \beta^{p^{k-s}+p^{-s}})x + (\beta^{p^{-s}} - 1)x^{p^k} + (\beta^{p^{k-s}+p^{-s}} - \beta^{p^{-s}})x^{p^{-k}} = 0. \tag{5}$$

Clearly β^{-p^k} is a (p^k-1)-th power as well. Direct calculations show that any $y \in GF(p^{3k})$ satisfies

$$L_{\beta^{-p^k}}(-\beta y^{p^{-k+s}} + y^{p^s}) = 0.$$

Thus if x is a solution of (3) we get $L_{\beta^{-p^k}}(x - \beta x^{p^k}) = 0$. Consequently,

$$(1 - \beta^{-p^k})x + (\beta^{-p^k} - \beta)x^{p^k} + (\beta - 1)x^{p^{-k}} = 0. \tag{6}$$

Note that $1 - \beta \neq 0$. Indeed, otherwise $u^{p^k-1} = a^{(p^k-1)(p^{s-k}-1)}$. Thus a primitive element u is a $(p^{s-k}-1)$-th power, a contradiction to the choice of s assuring $(p^{s-k}-1, p^n-1) \neq 1$. Further, $\beta^{p^{k-s}+p^{-s}} - \beta^{p^{-s}} = \beta^{p^{-s}}(\beta - 1)^{p^{k-s}}$ shows that $\beta^{p^{k-s}+p^{-s}} - \beta^{p^{-s}} \neq 0$. Combining equations (5) and (6) we get

$$\begin{aligned} &((1-\beta)(1-\beta^{p^{k-s}+p^{-s}}) + (1-\beta^{-p^k})(\beta^{p^{k-s}+p^{-s}} - \beta^{p^{-s}}))x \\ &- ((1-\beta)(1-\beta^{p^{-s}}) + (\beta - \beta^{-p^k})(\beta^{p^{k-s}+p^{-s}} - \beta^{p^{-s}}))x^{p^k} \;=\; 0. \end{aligned} \tag{7}$$

Note that

$$\begin{aligned}
&(1-\beta)(1-\beta^{p^{k-s}+p^{-s}})+(1-\beta^{-p^k})(\beta^{p^{k-s}+p^{-s}}-\beta^{p^{-s}}) \\
&= (1-\beta)(1-\beta^{p^{-s}})+(\beta-\beta^{-p^k})(\beta^{p^{k-s}+p^{-s}}-\beta^{p^{-s}})\,.
\end{aligned}$$

Hence equation (7) can be reduced to

$$((1-\beta)(1-\beta^{p^{k-s}+p^{-s}})+(1-\beta^{-p^k})(\beta^{p^{k-s}+p^{-s}}-\beta^{p^{-s}}))(x-x^{p^k})=0. \tag{8}$$

Observe that

$$((1-\beta)(1-\beta^{p^{k-s}+p^{-s}})+(1-\beta^{-p^k})(\beta^{p^{k-s}+p^{-s}}-\beta^{p^{-s}}))\neq 0\,. \tag{9}$$

Indeed otherwise

$$\beta^{p^{-s}}=(1-\beta^{-1})^{p^k(p^{k-s}-1)}(1-\beta)^{-(p^{k-s}-1)}$$

since $\beta^{p^{k-s}+p^{-s}}=\beta^{-p^{-(k+s)}}$. This implies that β is a $(p^{k-s}-1)$-th power. Since $\beta=u^{p^k-1}a^{(1-p^k)(p^{s-k}-1)}$, then u^{p^k-1} is a $(p^{k-s}-1)$-th power. Now the assumptions $k-s\equiv 0 \pmod 3$ and $(3,k)=1$ yield that u must be a (p^2+p+1)-th power in $GF(p^n)$, a contradiction.

Hence (8) and (9) show that $x=x^{p^k}$. Then equation (3) is reduced to

$$(1-\beta)(x+x^{p^s})=0. \tag{10}$$

Remember that $1-\beta\neq 0$ and therefore $x+x^{p^s}=0$. The nonzero solutions of the last equation satisfy $x^{p^s-1}=-1$. The rest of the proof follows from Claim 1.

□

There is another family of PN binomials over $GF(p^{3k})$ which can be obtained from the binomials described in Theorem 1 via EA-equivalence. Note that this binomials correspond to the ones from [1].

Theorem 2. *Let p be an odd prime, $n=3k$ with $(3,k)=1$ and u be a primitive element of $GF(p^n)$. Choose s to be a positive integer such that $k+s\equiv 0 \pmod 3$ and set $(s,n)=t$. Then the mapping $G(x)=x^{p^s+1}-u^{p^k-1}x^{p^{-k}+p^{k+s}}$ is PN over $GF(p^n)$ if n/t is odd.*

Proof. Firstly note that $k+s\equiv 0 \pmod 3$ if and only if $k-(2k+s)\equiv 0 \pmod 3$ and then $(s,n)=(2k+s,n)$. Thus if n/t is odd then by Theorem 1 the binomial $F(x)=x^{p^{2k+s}+1}-u^{-(p^k-1)}x^{p^k+p^{k+s}}$ is PN. Remark that $G(x)=-u^{p^k-1}F(x^{p^{-k}})$.

□

4 On the equivalence with monomials

In this section we consider the EA- and CCZ-equivalence of PN binomials from Theorem 1 with PN monomials.

Firstly we prove an auxiliary result on the certain multisets in $\mathbb{Z}/3k\mathbb{Z}$.

Claim 2. *Let $s \in \mathbb{Z}/3k\mathbb{Z}$ be such that $s \neq k, 2k$; $2s, 4s \neq 0$; $2s, 3s, 4s \neq k$, then the multiset $\{0,\ s+k,\ j,\ j+s\}$, $j \in \mathbb{Z}/3k\mathbb{Z}$, does not coincide with*

(a) the multiset $\{a,\ a+s,\ b,\ b+s\}$ for any $a, b \in \mathbb{Z}/3k\mathbb{Z}$,

(b) the multiset $\{a,\ a+s+k,\ b,\ b+s\}$ for any $a, b \in \mathbb{Z}/3k\mathbb{Z}$ such that $(a, b) \neq (0, j)$,

(c) the multiset $\{a,\ a+s+k,\ b,\ b+s+k\}$ for any $a, b \in \mathbb{Z}/3k\mathbb{Z}$.

Proof. (a) Let $\{0,\ s+k,\ j,\ j+s\} = \{a,\ a+s,\ b,\ b+s\}$. There are four cases depending on the value of a.

Case $a = 0$: Note $a+s = s \neq s+k$. Suppose $a+s = s = j$ then $j+s = 2s \in \{b, b+s\}$. If $j+s = 2s = b$, then $b+s = 3s$ must be $s+k$. This is impossible since $k \neq 2s$. Let $j+s = 2s = b+s$, then $b = s$ and $b = s+k$, a contradiction. Hence $a+s$ must be $j+s$, and consequently $a = j = 0$. Then $\{0,\ s+k,\ j,\ j+s\} = \{0^2, s+k, s\}$ and $\{a,\ a+s,\ b,\ b+s\} = \{0,\ s, b,\ b+s\}$. So $\{b,\ b+s\}$ must be equal to $\{0,\ s+k\}$. If $b = 0$, then $b+s = s \neq s+k$. Finally, if $b = s+k$, then $b+s = 2s+k \neq s+k$. Thus $a \neq 0$.

Case $a = s+k$: Note $a+s = 2s+k \neq 0$. Suppose $a+s = 2s+k = j$ then $j+s = 3s+k \in \{b, b+s\}$. If $j+s = 3s+k = b$, then $b+s = 4s+k$ must be 0, this contradicts the assumption on k, s. So let $j+s = 3s+k = b+s$, then $b = 2s+k$, which again cannot be equal to 0. In the case $a+s = 2s+k = j+s$, we have $j = s+k = a$. Then $\{0,\ s+k,\ j,\ j+s\} = \{0, (s+k)^2, 2s+k\}$ and $\{a,\ a+s,\ b,\ b+s\} = \{s+k,\ 2s+k, b,\ b+s\}$. So $\{b,\ b+s\}$ must be equal to $\{0,\ s+k\}$, which is impossible. Hence $a \neq s+k$.

Note that if $a = j$, then b must be in $\{0, s+k\}$. This is impossible by the previous arguments. So let $a = j+s$. But then $b = j$ is also not possible.

The proof of (b) and (c) is analogous. $\square$

Theorem 3. *Let p be an odd prime, $n = 3k$ and $0 \le r < n$. Let s satisfy the condition of Claim 2. Then the mapping $f(x) = x^{p^s+1} - u^{p^k-1}x^{p^k+p^{-k+s}}$ with nonzero $u \in GF(p^n)$ is not CCZ-equivalent to any Dembowski-Ostrom monomial $g(x) = x^{p^r+1}$ over $GF(p^n)$.*

Proof. Suppose the mappings $f(x)$ and $g(x)$ are CCZ-equivalent. Then there are polynomials

$$L_1(x,y) = a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i y^{p^i}$$

and

$$L_2(x,y) = c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i y^{p^i}$$

where $a, c, a_i, b_i, c_i, e_i \in GF(p^n)$, such that $L_2(x, f(x))$ is a permutation and it holds

$$a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i f(x)^{p^i} = \Big(c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i}\Big)^{p^r+1}. \qquad (11)$$

Let $\alpha = u^{p^k-1}$. Then (11) is equivalent to

$$\begin{aligned}
& a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i x^{p^i+p^{s+i}} - \sum_{i=0}^{n-1} b_i \alpha^{p^i} x^{p^{k+i}+p^{-k+s+i}} \\
= \; & c^{1+p^r} + c\sum_{i=0}^{n-1} c_i^{p^r} x^{p^{i+r}} + c^{p^r}\sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} c_i c_j^{p^r} x^{p^i+p^{j+r}} \qquad (12) \\
+ \; & c^{p^r}\sum_{i=0}^{n-1} e_i x^{p^i+p^{s+i}} - c^{p^r}\sum_{i=0}^{n-1} e_i \alpha^{p^i} x^{p^{k+i}+p^{-k+s+i}} + c\sum_{i=0}^{n-1} e_i^{p^r} x^{p^{r+i}+p^{r+s+i}} \\
- \; & c\sum_{i=0}^{n-1} e_i^{p^r}\alpha^{p^{r+i}} x^{p^{k+r+i}+p^{-k+r+s+i}} + \sum_{i,j=0}^{n-1} c_i e_j^{p^r} x^{p^i+p^{r+j}+p^{r+s+j}} + \sum_{i,j=0}^{n-1} e_i c_j^{p^r} x^{p^i+p^{s+i}+p^{r+j}} \\
- \; & \sum_{i,j=0}^{n-1} c_i e_j^{p^r}\alpha^{p^{j+r}} x^{p^i+p^{k+r+j}+p^{-k+r+s+j}} - \sum_{i,j=0}^{n-1} e_i c_j^{p^r}\alpha^{p^i} x^{p^{k+i}+p^{r+j}+p^{i-k+s}} \\
+ \; & \sum_{i,j=0}^{n-1} e_i e_j^{p^r}\big(x^{p^i+p^{s+i}+p^{r+j}+p^{r+s+j}} - \alpha^{p^i} x^{p^{k+i}+p^{s-k+i}+p^{r+j}+p^{r+s+j}} \\
- \; & \alpha^{p^{j+r}} x^{p^i+p^{s+i}+p^{k+r+j}+p^{-k+r+s+j}} + \alpha^{p^i+p^{j+r}} x^{p^{k+i}+p^{s-k+i}+p^{k+r+j}+p^{-k+r+s+j}}\big).
\end{aligned}$$

We modify the last part of (12) to

$$\sum_{i,j=0}^{n-1} e_i e_{j-r}^{p^r} x^{p^i+p^{s+i}+p^j+p^{s+j}} - \sum_{i,j=0}^{n-1} e_{i-k} e_{j-r}^{p^r} \alpha^{p^{i-k}} x^{p^i+p^{s+k+i}+p^j+p^{s+j}}$$
$$- \sum_{i,j=0}^{n-1} e_i e_{j-k-r}^{p^r} \alpha^{p^{j-k}} x^{p^i+p^{s+i}+p^j+p^{j+k+s}} + \sum_{i,j=0}^{n-1} e_{i-k} e_{j-k-r}^{p^r} \alpha^{p^{i-k}+p^{j-k}} x^{p^i+p^{s+k+i}+p^j+p^{s+k+j}}.$$

The last sum is equal to

$$\sum_{i,j=0}^{n-1} e_i e_{j+i-r}^{p^r} x^{p^i(1+p^s+p^j+p^{s+j})} + \sum_{i,j=0}^{n-1} e_{i-k} e_{j+i-k-r}^{p^r} \alpha^{p^{i-k}+p^{j+i-k}} x^{p^i(1+p^{s+k}+p^j+p^{j+s+k})}$$
$$- \sum_{i,j=0}^{n-1} (e_{i-k} e_{j+i-r}^{p^r} + e_{j+i} e_{i-k-r}^{p^r}) \alpha^{p^{i-k}} x^{p^i(1+p^{s+k}+p^j+p^{j+s})}.$$

Claim 2 implies that the coefficient of the monomial $x^{p^i(1+p^{s+k}+p^j+p^{j+s})}$ is $(e_{i-k} e_{j+i-r}^{p^r} + e_{j+i} e_{i-k-r}^{p^r}) \alpha^{p^{i-k}}$ for any i, j. Note that the p-weight of $1+p^{s+k}+p^j+p^{j+s}$ is 4 because of the assumptions on s and k. The lefthand side of (12) has no term with such exponents, which forces

$$e_{i-k} e_{j+i-r}^{p^r} + e_{j+i} e_{i-k-r}^{p^r} = 0. \tag{13}$$

Choosing $j = -k$ in (13) we get that $e_{i-k} e_{i-k-r}^{p^r} = 0$ for all i. Suppose $e_{i-k} \neq 0$ for some fixed i, then $e_{i-r} = 0$. Then from (13), we can get $e_{j+i-r} = 0$ for any $0 \leq j \leq n-1$, a contradiction. Thus, $e_i = 0$ for any $0 \leq i \leq n-1$.

Now equation (12) is reduced to

$$\begin{aligned} & a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i x^{p^i+p^{s+i}} - \sum_{i=0}^{n-1} b_i \alpha^{p^i} x^{p^{k+i}+p^{-k+s+i}} \\ = \; & c^{1+p^r} + c \sum_{i=0}^{n-1} c_i^{p^r} x^{p^{i+r}} + c^{p^r} \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} c_i c_j^{p^r} x^{p^i+p^{j+r}}. \end{aligned} \tag{14}$$

Note that the lefthand side of (14) contains only exponents of type $(p^s+1)p^i$ and $(p^{k+s}+1)p^j$ and $(p^s+1)p^i \not\equiv (p^{k+s}+1)p^j \pmod{p^n}$ by choice of s, k.

Suppose that $b_m \neq 0$ for some m, then the coefficients of the terms $x^{p^{m+s}+p^m}$ and $x^{p^{m+k}+p^{m-k+s}}$ are nonzero on the lefthand side of (14). Hence on the righthand side of (14) it must hold

$$c_m c_{m+s-r}^{p^r} \neq -c_{m+s} c_{m-r}^{p^r} \tag{15}$$

and

$$c_{m+k}c_{m-k+s-r}^{p^r} \neq -c_{m-k+s}c_{m+k-r}^{p^r}. \tag{16}$$

Further observe that there are no terms of the type $x^{p^m+p^{m+k}}$ and $x^{p^{m+k}+p^{m+s}}$ on the lefthand side of (14) since $s \neq k, 2k, 3k/2$ and $k \neq 3s$. Then from the righthand side of (14) we get the following conditions

$$c_m c_{m+k-r}^{p^r} = -c_{m+k}c_{m-r}^{p^r} \tag{17}$$

and

$$c_{m+k}c_{m+s-r}^{p^r} = -c_{m+s}c_{m+k-r}^{p^r}. \tag{18}$$

Suppose $c_{m+k-r} = 0$, then (16) implies $c_{m+k} \neq 0$. Then from (17) and (18) it follows $c_{m-r} = 0$ and $c_{m+s-r} = 0$, a contradiction to (15). So let $c_{m+k-r} \neq 0$. Note that lefthand side of (14) has no term of type x^{2p^i}, therefore from the righthand side of (14) we get $c_{m+k}c_{m+k-r} = 0$. Since $c_{m+k-r} \neq 0$ then $c_{m+k} = 0$. Using (17) and (18) we get $c_m = 0$ and $c_{m+s} = 0$, which contradicts to (15).

Hence we must have $b_i = 0$ for all i. In that case the lefthand side of (14) has no terms with exponents of p-weight 2. Thus on the righthand side of (14) it must hold

$$c_i c_j^{p^r} = -c_{j+r}c_{i-r}^{p^r}. \tag{19}$$

Taking $i = j + r$, we get $c_{j+r}c_j^{p^r} = 0$ and thus at least one of c_j or c_{j+r} must be 0 for any j. Assume $c_j \neq 0$ for some j, and thus $c_{j+r} = 0$. Then (19) implies $c_i = 0$ for all $0 \leq i \leq n-1$, a contradiction. Hence $c_j = 0$ for every $0 \leq j \leq n-1$, and consequently $L_2(x, f(x)) = c$, a contradiction to the assumption $L_2(x, f(x)) = c$ is a permutation on $GF(p^n)$.

□

Observe if an integer $s \neq k$ in Theorem 1 leads to a PN binomial then s satisfies the assumptions of Theorem 3. In the case $s = k$ the binomial defined in Theorem 1 is of shape $x^{p^k+1} - u^{p^k-1}x^{p^k+1} = (1-u^{p^k-1})x^{p^k+1}$, which is obviously EA-equivalent to x^{p^k+1}. Recall that EA-equivalence is a particular case of CCZ-equivalence, and thus Theorem 3 shows that the mapping $f(x) = x^{p^s+1} - u^{p^k-1}x^{p^{-k}+p^{k+s}}$, $u \in GF(p^n)^*$, is not EA-equivalent to $x^{p^r+1}, 0 \leq r \leq n-1$ over $GF(p^n)$.

Theorem 4. *Let $p \geq 5$ be prime and $s \neq k$. Then the PN binomials described in Theorem 1 are not CCZ-equivalent to the known PN mappings.*

Proof. The only known PN mappings in $GF(p^n)$ with $p \geq 5$ are those obtained from the monomial PN mappings via CCZ-equivalence. Theorem 3 completes the proof.

$\square$

Theorem 5. *Let $p = 3$, k be even and $s \neq k$. Then the PN binomials described in Theorem 1 are not EA-equivalent to the known PN mappings.*

Proof. From Theorem 3 it follows that the PN binomials are not EA-equivalent to both x^{3^r+1} and x^2. There is one more family of PN mappings in $GF(3^n)$, n even, namely $x^{\frac{3^e+1}{2}}$. But since $\frac{3^e+1}{2}$ is not a Dembowski-Ostrom polynomial, it is not EA-equivalent to the binomials considered in Theorem 1.

$\square$

5 Semifields of PN mappings

A finite *presemifield* is a finite set S with two binary operations $+$ and $*$ satisfying the following axioms:

- $(S, +)$ is an Abelian group with identity 0.
- $a * (b + c) = a * b + a * c$ and $(a + b) * c = a * c + b * c$ for all $a, b, c \in S$.
- If $a * b = 0$, then a or b is 0.

If, in addition to this, we also have

- there exists an element $1 \neq 0$ such that $1 * a = a = a * 1$ for all $a \in S$,

then the presemifield is called a *semifield*. Presemifields are commutative if $a * b = b * a$ for all $a, b \in S$.

The additive group of a finite presemifield is elementary Abelian. Consequently, any finite presemifield can be represented by $(GF(p^n), +, *)$, where $+$ is the addition in $GF(p^n)$ and $* : GF(p^n) \times GF(p^n) \to GF(p^n)$. Two finite presemifields $(GF(p^n), +, *)$ and $(GF(p^n), +, \star)$ are called isotopic if there exist linearized permutation polynomials L, M, N over $GF(p^n)$ such that

$$M(x) \star N(y) = L(x * y) \text{ for any } x, y \in GF(p^n).$$

Any presemifield $S = (GF(p^n), +, *)$ is isotopic to a semifield. Indeed, fix any nonzero $a \in GF(p^n)$ and define $\star : GF(p^n) \times GF(p^n) \to GF(p^n)$ as follows

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

Then the element $a * a$ is the identity element of $(GF(p^n), +, \star)$. Note that if $*$ is commutative then so is also $\star$.

The following is the list of known classes of unisotopic finite commutative semifields of odd order:

- finite field of order p^n for any n
- Albert's commutative twisted fields of order p^n for any n
- Dickson semifields of order p^n for even n
- Coulter-Matthews semifields of order 3^n for odd n
- Ding-Yuan semifields of order 3^n for odd n
- Ganley semifields of order 3^{2r} for odd r
- Cohen-Ganley semifields of order 3^{2r}
- Coulter-Henderson-Kosick semifield of order 3^8
- Penttila-Williams semifield of order 3^{10}.

If f is a PN Dembowski-Ostrom polynomial over GF(p^n) then $S_f = (GF(p^n), +, *)$ is a commutative presemifield with the multiplication $*$ defined by

$$x * y = \frac{1}{2}(f(x+y) - f(x) - f(y)). \tag{20}$$

Conversely, any commutative presemifield $S = (GF(p^n), +, *)$ yields a PN mapping $f_S : GF(p^n) \to GF(p^n)$ by $f_S : x \mapsto x * x$. Moreover, the mapping f_S has a polynomial representation given by a sum of a PN Dembowski-Ostrom polynomial and an affine polynomial [7]. Hence the classification of finite presemifields of odd order and the one of PN Dembowski-Ostrom polynomials are equivalent. In [7] it is shown that in certain cases the PN Dembowski-Ostrom polynomials define isotopic presemifields if and only if they are EA-equivalent:

Theorem 6 ([7]). *Let $f, g \in GF(p^n)$ be PN Dembowski-Ostrom polynomials and the presemifields S_f and S_g be defined by (20).*

(a) *Let n be odd. Then the presemifields S_f and S_g are isotopic if and only if f and g are EA-equivalent.*

(b) *S_f is isotopic to $GF(p^n)$ if and only if f is EA-equivalent to x^2.*

(c) *S_f is isotopic to a commutative twisted field of Albert if and only if f is EA-equivalent to x^{p^r+1} with $n/(n,r)$ odd.*

The above discussion and Theorems 1,4 imply the following result.

Theorem 7. *Let p be an odd prime, $n = 3k$ with $(3,k) = 1$ and u be a primitive element of $GF(p^n)$. Choose $0 < s < 3k$ such that $k - s \equiv 0 \pmod 3$ and $n/(s,n)$ is odd. If $* : GF(p^n) \times GF(p^n) \to GF(p^n)$ is defined as follows*

$$x * y = x^{p^s} y + x y^{p^s} - u^{p^k - 1}(x^{p^k} y^{p^{2k+s}} + x^{p^{2k+s}} y^{p^k}).$$

Then $S = (GF(p^n), +, *)$ is a commutative presemifield. Moreover this presemifield is not isotopic to any other known one if $p \geq 5$, k is odd and $s \neq k$.

Acknowlegments

Recently it was shown that two PN mappings are CCZ-equivalent exactly when they are EA-equivalent, see [16]. Jürgen Bierbrauer informed us that APN binomials over $GF(2^{4k})$ may be used to obtain PN mappings as well.

References

[1] J. Bierbrauer, *A family of crooked functions*, preprint (2007).

[2] C. Braken, E. Byrne, N. Markin and G. McGuire, *New families of quadratic almost perfect nonlinear trinomials and multinomials*, Preprint.

[3] C. Braken, E. Byrne, N. Markin and G. McGuire, *An infinite family of quadratic quadrinomial APN functions*, arXiv:0707.1223vl.

[4] L. Budaghyan, C. Carlet and G. Leander, *A class of quadratic APN binomials inequivalent to power functions*, submitted; available at http://eprint.iacr.org/2006/445.pdf.

[5] L. Budaghyan, C. Carlet, and A. Pott, *New classes of almost bent and almost perfect nonlinear polynomials*, IEEE Trans. Inform. Theory, 52 (2006), pp. 1141–1152.

[6] C. Carlet, P. Charpin and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr. 15 (1998) pp. 125-156.

[7] R. S. Coulter and M. Henderson, *Commutative presemifields and semifields*, Adv. Math. 217 (2008) pp. 282- 304.

[8] R. S. Coulter, M. Henderson and P. Kosick, *Planar polynomials for commutative semifields with specified nuclei*, Des. Codes Cryptogr. 44 (2007) pp. 275-286.

[9] R. S. Coulter and R. W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr. 10 (1997) pp. 167-184.

[10] P. Dembowski and T. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. 103 (1968) pp. 239-258.

[11] C. Ding and J. Yin, *Signal sets from functions with optimum nonlinearity*, IEEE Trans. Communications, **55** (2007), 936–940.

[12] C. Ding and J. Yuan, *A family of optimal constant-composition codes*,IEEE Trans. Inform. Theory, **51** (2005), 3668–3671.

[13] C. Ding and J. Yuan, *A new family of skew Paley-Hadamard difference sets*, J. Comb. Theory Ser.A 113 (2006) pp. 1526-1535.

[14] Y. Edel, G. Kyureghyan, and A. Pott, *A new APN function which is not equivalent to a power mapping*, IEEE Trans. Inform. Theory, 52 (2006), pp. 744–747.

[15] T. Helleseth and D. Sandberg, *Some power mappings with low differential uniformity*, Applicable Algebra in Engineering, Communications and Computing, 8 (1997), pp. 363–370.

[16] G. Kyureghyan, and A. Pott, *Some theorems on planar mappings*, to appear in Proceedings of WAIFI 2008, LNCS.

[17] K. Nyberg, *Differentially uniform mappings for cryptography*, in Advances in Cryptology-EUROCRYPT 93, Lecture Notes in Computer Science, vol.765. New York: Springer-Verlag, 1994, pp. 134-144.

[18] G. Weng, W. Qiu, Z. Wang and Q. Xiang, *Pseudo-Paley graphs and skew Hadamard sets from presemifields*, Des. Codes Cryptogr. 44 (2007) pp. 49-62.