Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2013, Article ID 917507, 5 pages
http://dx.doi.org/10.1155/2013/917507

Research Article

Another Class of Perfect Nonlinear Polynomial Functions

Menglong Su,[1,2] Zhengbang Zha,[1,3] and Zhonghai Xu[4]

[1] *College of Mathematics, Luoyang Normal University, Luoyang 471022, China*
[2] *Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education, Jilin University, Changchun 130012, China*
[3] *Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[4] *National Key Laboratory of Science and Technology on Advanced Composites in Special Environments, Harbin Institute of Technology, Harbin 150080, China*

Correspondence should be addressed to Menglong Su; sumenglongjlu@163.com

Received 2 June 2013; Revised 10 November 2013; Accepted 24 November 2013

Academic Editor: Gradimir Milovanović

Perfect nonlinear (PN) functions have been an interesting subject of study for a long time and have applications in coding theory, cryptography, combinatorial designs, and so on. In this paper, the planarity of the trinomials $x^{p^k+1} + ux^2 + vx^{2p^k}$ over $\mathrm{GF}(p^{2k})$ are presented. This class of PN functions are all EA-equivalent to x^2.

1. Introduction

Let p be a prime and $\mathrm{GF}(p^n)$ a finite field with p^n elements. Let f be a mapping from $\mathrm{GF}(p^n)$ to itself. Let $N(a,b)$ denote the number of solutions $x \in \mathrm{GF}(p^n)$ of $f(x+a) - f(x) = b$, where $a, b \in \mathrm{GF}(p^n)$, and let $\Delta_f = \max\{N(a,b) \mid a,b \in \mathrm{GF}(p^n), a \neq 0\}$. Nyberg [1] defined a mapping f to be differentially k-uniform if $\Delta_f = k$. For applications in cryptography, one would like to employ functions for which Δ_f is as small as possible. The differentially 2-uniform function is called APN function. And we know that APN functions are optimal over $\mathrm{GF}(2^n)$. This concept is of interest in cryptography since differential and linear cryptanalysis exploit the uniform property of the functions which are used in many block ciphers, such as DES. The differentially 1-uniform function is called PN function. It is interesting to observe that PN functions have also been studied under the name of planar functions which are functions such that $f(x+a) - f(x)$ is a permutation polynomial for all $a \in \mathrm{GF}(p^n)^* = \mathrm{GF}(p^n) \setminus \{0\}$. Planar functions were introduced in [2] to describe projective planes with certain properties. In recent papers [3, 4], PN functions were used to describe new finite commutative semifields of odd order. In [5, 6], it was shown that a PN function yields either a skew Hadamard difference set or a Paley type partial difference set depending on $p^n \pmod 4$. PN function is one of the most important cryptographic functions [7, 8] and has extensive applications in cryptography and communication. For example, PN and APN functions were used to construct optimal constant-composition codes and signal sets [9, 10].

Since PN functions have many applications in coding theory, cryptography, combinatorial designs, and so on, it is interesting to find new PN functions. We call a function "new" only if it is CCZ-inequivalent to the old ones. As we know, there are only three classes of PN monomials. Whether there exists another class of PN monomials is an open problem. In [11], Coulter and Matthews introduced the first family of PN polynomials. Ding and Yuan [5] generalized their results and presented a new skew Hadamard difference set. Helleseth et al. [12] showed a family of PN binomials $ux^{p^k+1} + x^2$ over $\mathrm{GF}(p^{2k})$ which is equivalent to the monomial x^2. After that, some new methods were used to construct new PN functions (please see [13–17] and references therein), but it is still difficult to find more new PN functions. Many constructions of PN functions are used of the link between quadratic PN functions and commutative semifields. Bierbrauer [18] introduced a general projection method to construct commutative semifields and generalized the known PN functions. Pott and Zhou presented a switching construction of PN functions in [19] and introduced a character

theoretic approach to prove the planarity of a function in [20]. Recently, they presented new commutative semifields with two parameters and then get new PN functions [21]. In their paper [22], Kyureghyan and Özbudak constructed some new PN functions by the products of two linearized polynomials.

In [12], the binomial composed with inequivalent monomials x^2 and x^{q+1} was shown to be equivalent to the monomial x^2 over GF(q^2). What about the planarity of trinomial composed with monomials x^2, x^{2q} and x^{q+1}? In this paper, we will answer this question. In Section 2, we recall some definitions and tools used later in the paper. In Section 3, we characterize the planarity of the trinomials $x^{p^k+1} + ux^2 + vx^{2p^k}$ over GF(p^{2k}). These PN trinomials are shown to be equivalent to monomial x^2 in Section 4. We then conclude this paper in Section 5 with some future work.

2. Preliminaries

Let p be an odd prime, and let n be a positive integer. Let $\chi(x)$ be a function on GF(p^n) defined by $\chi(x) = x^{(p^n-1)/2}$. Then, we get that $\chi(x) = 0$ when $x = 0$, $\chi(x) = 1$ when x is a square in GF(p^n)$\setminus\{0\}$, and $\chi(x) = -1$ when x is a nonsquare in GF(p^n) $\setminus$ $\{0\}$.

The p-weight of a nonnegative integer m is the sum of the digits in its p-adic representation; that is, if $m = \sum_i b_i p^i$ with $0 \le b_i < p$, 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 of its nonzero terms. A polynomial is called quadratic if it has algebraic degree 2. The following polynomials of algebraic degree 2

$$\sum_{i,j=0}^{n-1} a_{i,j} x^{p^i+p^j}, \quad a_{i,j} \in \mathrm{GF}\left(p^n\right) \tag{1}$$

are called Dembowski-Ostrom (DO) polynomials in [2].

Let $c_i \in$ GF(p^n). A polynomial of the form $L(x) = \sum_{i=0}^{n-1} c_i x^{p^i}$ is called linearized or p-polynomial over GF(p^n). The sum of a linear mapping and a constant in GF(p^n) is called an affine mapping.

Two functions f, g : GF(p^n) $\to$ GF(p^n) are called extended affine (EA) equivalent, if $g = L_1 \circ f \circ L_2 + L_3$ for some affine permutations L_1, L_2 and affine function L_3. The functions f and g are called Carlet-Charpin-Zinoviev (CCZ) equivalent if the graphs of f and g are affine equivalent [23]. CCZ-equivalent functions have the same differential uniformity and the same extended Walsh spectrum. It is showed in [24] that the CCZ-equivalence coincides with the EA-equivalence for PN functions. For planar DO polynomials, CCZ-equivalence coincides with linear equivalence [14].

In [3], Coulter and Henderson proved that planar DO polynomials are equivalent to commutative semifields with odd characteristic. Many new PN functions are defined by corresponding commutative semifields with no explicit function expressions, such as Dickson semifields and Cohen-Ganley semifileds [4, 25, 26]. In the following, we just list the known EA-inequivalent PN functions which have explicit function expressions:

(a) x^2 over GF(p^n) (folklore);

(b) x^{p^k+1} over GF(p^n), where $k \le n/2$ and $n/(k,n)$ is odd ([2, 11]);

(c) $x^{10} \pm x^6 - x^2$ over GF(3^n), where $n \ge 5$ is odd ([5, 11]);

(d) $x^{p^s+1} - vx^{p^{2k}+p^{k+s}}$ over GF(p^{3k}), where $k_1 = k/\gcd(k,s)$, $s_1 = s/\gcd(k,s)$, k_1 is odd, $\mathrm{ord}(v) = q^2+q+1$, and at least one of the following conditions hold: $k_1 + s_1 \equiv 0 \bmod 3$, $p^k \equiv p^s \equiv 1 \bmod 3$ ([13, 17]);

(e) $x^{p^s+1} - vx^{p^{3k}+p^{k+s}}$ over GF(p^{4k}), where $2k/\gcd(2k,s)$ is odd, $\mathrm{ord}(v) = q^3+q^2+q+1$, and $p^k \equiv p^s \equiv 1 \bmod 4$ ([13]);

(f) $x^{(3^k+1)/2}$ over GF(3^n), where $k \ge 3$ is odd and $(k,n) = 1$ ([11]);

(g) $x^{q+1} + \omega\beta x^{p^s+1} + \omega\beta^q x^{q(p^s+1)}$ over GF(q^2), where $q = p^m$, $\omega, \beta \in$ GF(q^2), $\omega + \omega^q = 0$, s is a positive integer, β is not a $\gcd(q+1, p^s+1)$th power, and there is no $0 \ne a \in$ GF(q^2) such that $a^q + a = 0$ and $a^{p^s} = -a$ ([14, 18]);

(h) $x^2 + x^{2q^m} + G(x^{q^2+1})$ over GF(q^{2m}), where q is a power of an odd prime p, $m = 2k+1$, and $G(x) = h(x - x^{q^m})$ with $h(x) = \sum_{i=0}^{k}(-1)^i x^{q^{2i}} + \sum_{j=0}^{k-1}(-1)^{k+j} x^{q^{2j+1}}$ ([18, 27]);

(i) $x^2 + x^{90}$ over GF(3^5) ([28]).

Below, we always let p be an odd prime and q, n, k positive integers with $n = 2k$ and $q = p^k$.

3. A New Family of PN Trinomials over GF(p^{2k})

In this section, we propose a new family of PN trinomials over GF(p^{2k}) which are composed of inequivalent monomials x^2 and x^{p^k+1}.

Theorem 1. *Let $u, v, \theta \in GF(q^2)$ with $\theta = (v^{q+1} - u^{q+1})^2 - (u - v^q)^{q+1}$, and let $f : GF(q^2) \to GF(q^2)$ be given by $f(x) = x^{q+1} + ux^2 + vx^{2q}$. Then, $f(x)$ is PN if and only if $\theta^{(q-1)/2} = 1$.*

Proof. We need to count the number of solutions of $f(x+a) - f(x) = b$ under the conditions defined above for any $a \ne 0, b$ in GF(q^2). The equation $f(x+a) - f(x) = b$ can be written as

$$\begin{aligned}&(x+a)^{q+1} + u(x+a)^2 + v(x+a)^{2q}\\ &\quad - x^{q+1} - ux^2 - vx^{2q} = b.\end{aligned} \tag{2}$$

Let $\Delta = b - f(a)$. Then, (2) turns to

$$ax^q + a^q x + 2uax + 2va^q x^q = \Delta. \quad (3)$$

As (3) is affine, we just need to consider the case $\Delta = 0$. When $\Delta = 0$, for the function $f(x)$ to be PN, it is necessary and sufficient that $ax^q + a^q x + 2uax + 2va^q x^q = 0$ has $x = 0$ as its only solution for any nonzero $a \in \mathrm{GF}(q^2)$. That is, say $x^{q-1} = -(a^q + 2ua)/(a + 2va^q) \neq 0$ has no solution over $\mathrm{GF}(q^2)$. Therefore, $f(x)$ is PN if and only if the equation $(a^q + 2ua)^{q+1} = (a + 2va^q)^{q+1}$ is not true. It can be written as

$$\left(u - v^q\right) a^2 + 2\left(u^{q+1} - v^{q+1}\right) a^{q+1} + \left(u^q - v\right) a^{2q} = 0. \quad (4)$$

If $u - v^q = 0$, (4) is always true. We assume that $u - v^q \neq 0$. Let $t = a^{q-1}$. Since $a \neq 0$, we can get

$$\left(u^q - v\right) t^2 + 2\left(u^{q+1} - v^{q+1}\right) t + u - v^q = 0 \quad (5)$$

from (4). Then, we get $t(v^{q+1} - u^{q+1} \pm \theta^{1/2})/(u^q - v)$ with $\theta = (v^{q+1} - u^{q+1})^2 - (u - v^q)^{q+1}$. As we know $t^{q+1} = 1$, then we have

$$\frac{\left(v^{q+1} - u^{q+1}\right)^2 \pm \left(\theta^{1/2} + \theta^{q/2}\right)\left(v^{q+1} - u^{q+1}\right) + \theta^{(q+1)/2}}{(u - v^q)^{q+1}} = 1. \quad (6)$$

Since $\theta^q = \theta$, then we get $\theta^{q/2} = \pm\theta^{1/2}$. If $\theta^{(q-1)/2} = 0$ or -1, we can obviously find that (6) is true. If $\theta^{(q-1)/2} = 1$, then we get

$$\left(v^{q+1} - u^{q+1}\right)^2 \pm 2\theta^{1/2}\left(v^{q+1} - u^{q+1}\right) + \theta = \left(u - v^q\right)^{q+1} \quad (7)$$

from (6). It leads to $\theta^{1/2} = \pm(v^{q+1} - u^{q+1})$ and $u - v^q = 0$, which contradicts the first assumption $u - v^q \neq 0$. Therefore, $f(x)$ is PN if and only if $\theta^{(q-1)/2} = 1$. □

We can get the following corollary from Theorem 1.

Corollary 2. *Let $f : GF(q^2) \to GF(q^2)$ be given by $f(x) = x^{q+1} + ux^2 + vx^{2q}$, where $u^{1+q} = v^{1+q}$. Then, $f(x)$ is PN if and only if $q \equiv 1$ (mod 4), $\chi(u^q - v) = 1$ or $q \equiv 3$ (mod 4), $\chi(u^q - v) = -1$.*

Proof. From Theorem 1, we get that $f(x)$ is PN if and only if $((v^{q+1} - u^{q+1})^2 - (u - v^q)^{q+1})^{(q-1)/2} = 1$. Since $u^{1+q} = v^{1+q}$, we just need $(-(u - v^q)^{q+1})^{(q-1)/2} = 1$; that is, $0 \neq -(u - v^q)^{q+1}$ is a $2(q+1)$th power. When $\chi(u^q - v) = 1$, $-(u - v^q)^{q+1}$ is a $2(q+1)$th power if and only if -1 is a $2(q+1)$th power, which is equivalent to $q \equiv 1$ (mod 4). When $\chi(u^q - v) = -1$, we get that $(u - v^q)^{q+1}$ is a $(q+1)$th power and not $2(q+1)$th power. In this case, $-(u - v^q)^{q+1}$ is a $2(q+1)$th power if and only if $q \equiv 3$ (mod 4). □

Remark 3. If $f(x)$ is PN in Corollary 2, we have $u^{(1+q)/2} = -v^{(1+q)/2}$ for accuracy. Since $((u - v^q)/(u^q - v)) \cdot (v/u) = (uv - v^{q+1})/(u^{q+1} - uv) = -1$, then we get $(u^q - v)^{q-1}(v/u) = -1$. Whether $q \equiv 1$ (mod 4), $\chi(u^q - v) = 1$ or $q \equiv 3$ (mod 4), $\chi(u^q - v) = -1$, we get that v/u is a $(q-1)$th power and not a $2(q-1)$th power, which implies $u^{(1+q)/2} = -v^{(1+q)/2}$.

The PN functions defined in Corollary 2 exist. For example, the function $x^{3^k+1} - x^2 + x^{2\cdot 3^k}$ is PN over $\mathrm{GF}(3^{2k})$, where k is even.

4. The Linear Equivalence of the New PN Trinomials

In this section, we will discuss the linear equivalence between our new PN functions and the known PN monomial x^2. First, we give a simple proof to show that the PN functions defined in Corollary 2 are equivalent to x^2.

Theorem 4. *The PN function $f(x)$ defined in Corollary 2 is linear equivalent to x^2.*

Proof. Since $u^{(1+q)/2} = -v^{(1+q)/2}$, we obtain $(v/u)^{1+q} = 1$ and v/u is a $(q-1)$th power. Let $\theta^2 = v/u$, and let $L_1(x) = ((1 - 2\theta v^q)/(u - v^q))x + ((2\theta u - 1)/(u - v^q))x^q$, $L_2(x) = x + \theta x^q$ be linear polynomials on $\mathrm{GF}(q^2)$. We can get $L_1(f(x)) = L_2(x)^2$.

Assume that $L_2(x + a) = L_2(x)$, we obtain $a + \theta a^q = 0$, which implies that $a = 0$ or $a^{q-1} = -\theta$. If $a^{q-1} = -\theta$, we get $a^{2(q-1)} = v/u$. Since v/u is not a $2(q-1)$th power in Corollary 2 then we have $a^{q-1} \neq -\theta$ and $a = 0$. Thus, $L_2(x) = x + \theta x^q$ is a linear permutation.

If one of $1 - 2\theta v^q$ and $2\theta u - 1$ equals to 0, we can get that $L_1(x)$ is a linear permutation. If both of $1 - 2\theta v^q$ and $2\theta u - 1$ equal 0, we can get $u^q = v$. This is not true for $\chi(u^q - v) \neq 0$. Otherwise, we assume $L_1(x + a) = L_1(x)$. Then, we get $a = 0$ or $a^{q-1} = (2\theta v^q - 1)/(2\theta u - 1)$. If $a \neq 0$, we get $(2\theta v^q - 1)^{1+q} = (2\theta u - 1)^{1+q}$. We can deduce that $\theta^q(u^q - v) = -\theta(u - v^q)$. It leads to

$$\left(\frac{v}{u}\right)^{(q+1)/2} = \theta^{q+1} = -\frac{u - v^q}{u^q - v} \cdot \frac{v}{u} = \frac{v^{q+1} - uv}{u^{q+1} - uv} = 1. \quad (8)$$

Then, we get that v/u is a $2(q-1)$th power which contradicts the known result $u^{(1+q)/2} = -v^{(1+q)/2}$. Therefore, $L_1(x) = ((1 - 2\theta v^q)/(u - v^q))x + ((2\theta u - 1)/(u - v^q))x^q$ is also a linear permutation. This completes the proof. □

Inspired by the proof of Theorem 4, we get a generalized result in the following theorem.

Theorem 5. *The PN function $f(x)$ defined in Theorem 1 is linear equivalent to x^2.*

Proof. If the PN function $f(x) = x^{q+1} + ux^2 + vx^{2q}$ is linear equivalent to x^2 over $\mathrm{GF}(q^2)$, there must exist linear

permutations $L_1(x) = \sum_{j=0}^{n-1} b_j x^{p^j}$ and $L_2(x) = \sum_{j=0}^{n-1} c_j x^{p^j}$ such that

$$\sum_{j=0}^{n-1} b_j \left(x^{1+q} + ux^2 + vx^{2q}\right)^{p^j} = \sum_{i,j=0}^{n-1} c_i c_j x^{p^i+p^j}. \tag{9}$$

When $i-j \neq 0$, $k \in \mathbb{Z}_{2k}$, there is no item of the type $x^{p^i+p^j}$ on the left side of (9). Then, we can get that the coefficient of $x^{p^i+p^j}$ equals to 0. It shows that $2c_ic_j = 0$. Assume that $c_l \neq 0$ for some l, we obtain that $c_j = 0$ when $j \neq l$, $l+k \in \mathbb{Z}_{2k}$. Then, (9) can be written as

$$\begin{aligned} &\sum_{j=0}^{n-1} b_j \left(x^{1+p^k} + ux^2 + vx^{2p^k}\right)^{p^j} \\ &\quad = c_l^2 x^{2p^l} + c_{l+k}^2 x^{2p^{l+k}} + 2c_l c_{l+k} x^{p^l+p^{l+k}}. \end{aligned} \tag{10}$$

When $j \neq l$, $l+k$, we can see that there is no item of type $x^{p^j(1+p^k)}$ and x^{2p^j} on the right side of (10). Then, we have $b_j + b_{j+k} = 0$ and $b_j u^{p^j} + b_{j+k} v^{p^{j+k}} = 0$. This leads to $b_j = -b_{j+k}$ and $b_j(u^{p^j} - v^{p^{j+k}}) = 0$. Since $u - v^{p^k} \neq 0$, then we obtain that $b_j = 0$ when $j \neq l$, $l+k$. Therefore, (10) can be written as

$$\begin{aligned} &b_l \left(x^{1+p^k} + ux^2 + vx^{2p^k}\right)^{p^l} + b_{l+k} \left(x^{1+p^k} + ux^2 + vx^{2p^k}\right)^{p^{l+k}} \\ &\quad = c_l^2 x^{2p^l} + c_{l+k}^2 x^{2p^{l+k}} + 2c_l c_{l+k} x^{p^l+p^{l+k}}. \end{aligned} \tag{11}$$

Comparing the coefficients of x^{2p^l}, $x^{2p^{l+k}}$, and $x^{p^l(1+p^k)}$ of (11), we can get the following equations:

$$b_l + b_{l+k} = 2c_l c_{l+k}, \tag{12}$$

$$b_l u^{p^l} + b_{l+k} v^{p^{l+k}} = c_l^2, \tag{13}$$

$$b_l v^{p^l} + b_{l+k} u^{p^{l+k}} = c_{l+k}^2. \tag{14}$$

From (12) and (13), we obtain $b_{l+k} = (c_l^2 - 2c_l c_{l+k} u^{p^l})/(v^{p^{l+k}} - u^{p^l})$. We can also obtain $b_{l+k} = (c_{l+k}^2 - 2c_l c_{l+k} v^{p^l})/(u^{p^{l+k}} - v^{p^l})$ from (13) and (14). Then, we have

$$\begin{aligned} &\left(u^{p^{l+k}} - v^{p^l}\right)\left(\frac{c_l}{c_{l+k}}\right)^2 + 2\left(v^{p^l(1+p^k)} - u^{p^l(1+p^k)}\right)\left(\frac{c_l}{c_{l+k}}\right) \\ &\quad + u^{p^l} - v^{p^{l+k}} = 0. \end{aligned} \tag{15}$$

We note that $L_2(x) = c_l x^{p^l} + c_{l+k} x^{p^{l+k}}$ is a permutation if and only if c_l/c_{l+k} is not a (p^k-1)th power. Comparing (5) and (15), we have $c_l/c_{l+k} = -t^{p^l}$. Under the conditions of Theorem 1, $t^{q+1} = 1$ is not true. Then, we get that c_l/c_{l+k} is not a (p^k-1)th power and $L_2(x)$ is a permutation.

From (12)–(14), we get $b_{l+k} = (c_l^2 - 2c_l c_{l+k} u^{p^l})/(v^{p^{l+k}} - u^{p^l})$ and $b_l = (2c_l c_{l+k} v^{p^{l+k}} - c_l^2)/(v^{p^{l+k}} - u^{p^l})$. If one of b_l and b_{l+k} equals to 0, then $L_1(x) = b_l x^{p^l} + b_{l+k} x^{p^{l+k}}$ is a monomial permutation. If both of b_l and b_{l+k} equal to 0, we get $u = v^{p^k}$, which leads to a contradiction. Now, we consider the case that both b_l and b_{l+k} are not equal to 0. In this case, $L_1(x) = b_l x^{p^l} + b_{l+k} x^{p^{l+k}}$ is a permutation if and only if b_l/b_{l+k} is not a (p^k-1)th power. We assume that $b_l/b_{l+k} = (2c_{l+k} v^{p^{l+k}} - c_l)/(c_l - 2c_{l+k} u^{p^l})$ is a (p^k-1)th power. Then, we have $(2c_{l+k} v^{p^{l+k}} - c_l)^{p^k+1} = (c_l - 2c_{l+k} u^{p^l})^{p^k+1}$, which implies

$$\begin{aligned} &\left(u^{p^l} - v^{p^{l+k}}\right)\left(\frac{c_l}{c_{l+k}}\right)^{p^k} + \left(u^{p^{k+l}} - v^{p^l}\right)\frac{c_l}{c_{l+k}} \\ &\quad + 2\left(v^{p^l(1+p^k)} - u^{p^l(1+p^k)}\right) = 0. \end{aligned} \tag{16}$$

From (15), we can get $c_l/c_{l+k} = (u^{p^l(1+p^k)} - v^{p^l(1+p^k)} \pm \theta^{p^l/2})/(u^{p^{k+l}} - v^{p^l})$ with θ defined in Theorem 1. Substituting the value of c_l/c_{l+k} into (16), we have

$$\begin{aligned} &u^{p^l(1+p^k)} - v^{p^l(1+p^k)} \pm \theta^{p^{k+l}/2} + u^{p^l(1+p^k)} \\ &\quad - v^{p^l(1+p^k)} \pm \theta^{p^l/2} + 2\left(v^{p^l(1+p^k)} - u^{p^l(1+p^k)}\right) = 0. \end{aligned} \tag{17}$$

Since $\theta^{(p^k-1)/2} = 1$, from (17), we get $\theta^{p^l/2} = 0$, which is a contradiction. Therefore, we get that b_l/b_{l+k} is not a (p^k-1)th power and $L_1(x)$ is a permutation. The proof is completed. □

5. Conclusion

In this paper, we present a family of PN trinomials and determine the necessary and sufficient conditions which assure their planarity. All these PN functions are shown to be equivalent to the known PN function x^2 by using the definition of linear equivalence. Our results give an answer for the question presented in the introduction. It seems hard to determine the planarity of the linear combination of terms $x^{q^i+q^j}$ $(0 \leq i, j < n)$ over GF(q^n), where $n \geq 3$ and q is an odd prime power. However, it may be possible to determine them in some special cases (e.g., see [15]). We will continue this study and try to find more new PN functions in the future work.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

We would like to thank the anonymous reviewers for their invaluable suggestions and helpful comments, which greatly improved the paper. We sincerely thank the Editor for the kind help provided. This project was supported by NSFC-Union Science Foundation of Henan (no. U1304103), National Nature Science Foundation of China (no. 11201214), Natural Science Foundation of Henan Province (no. 122300410261), and Foundation of Laboratory

of Symbolic Computation and Knowledge Engineering of Ministry of Education (no. 93K172012K07).

References

[1] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in Cryptology—EUROCRYPT '93*, vol. 765 of *Lecture Notes in Computer Science*, pp. 55–64, Springer, Berlin, Germany, 1994.

[2] P. Dembowski and T. G. Ostrom, "Planes of order n with collineation groups of order n^2," *Mathematische Zeitschrift*, vol. 103, no. 3, pp. 239–258, 1968.

[3] R. S. Coulter and M. Henderson, "Commutative presemifields and semifields," *Advances in Mathematics*, vol. 217, no. 1, pp. 282–304, 2008.

[4] R. S. Coulter, M. Henderson, and P. Kosick, "Planar polynomials for commutative semifields with specified nuclei," *Designs, Codes and Cryptography*, vol. 44, no. 1–3, pp. 275–286, 2007.

[5] C. Ding and J. Yuan, "A new family of skew Hadamard difference sets," *Journal of Combinatorial Theory A*, vol. 113, no. 7, pp. 1526–1535, 2006.

[6] G. Weng, W. Qiu, Z. Wang, and Q. Xiang, "Pseudo-Paley graphs and skew Hadamard difference sets from presemifields," *Designs, Codes and Cryptography*, vol. 44, no. 1–3, pp. 49–62, 2007.

[7] Z. Tu and Y. Deng, "A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity," *Designs, Codes and Cryptography*, vol. 60, no. 1, pp. 1–14, 2011.

[8] W. Zhang and G. Xiao, "Constructions of almost optimal resilient Boolean functions on large even number of variables," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5822–5831, 2009.

[9] C. Ding and J. Yin, "Signal sets from functions with optimum nonlinearity," *IEEE Transactions on Communications* , vol. 53, no. 5, pp. 936–940, 2007.

[10] C. Ding and J. Yuan, "A family of optimal constant-composition codes," *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3668–3671, 2005.

[11] R. S. Coulter and R. W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," *Designs, Codes and Cryptography*, vol. 10, no. 2, pp. 167–184, 1997.

[12] T. Helleseth, G. Kyureghyan, G. J. Ness, and A. Pott, "On a family of perfect nonlinear binomials," in *Boolean Functions in Cryptology and Information Security*, B. Preenel and O. A. Logachev, Eds., vol. 18, pp. 126–138, IOS, Amsterdam, The Netherlands, 2008.

[13] J. Bierbrauer, "New semifields, PN and APN functions," *Designs, Codes and Cryptography*, vol. 54, no. 3, pp. 189–200, 2010.

[14] L. Budaghyan and T. Helleseth, "New commutative semifields defined by new PN multinomials," *Cryptography and Communications*, vol. 3, no. 1, pp. 1–16, 2011.

[15] G. Kyureghyan and Y. Tan, "On a family of planar mappings," in *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, B. Preenel, S. Dodunekov, V. Rijmen, and S. Nikova, Eds., vol. 23, pp. 175–178, IOS, Amsterdam, The Netherlands, 2009.

[16] Z. Zha, G. M. Kyureghyan, and X. Wang, "Perfect nonlinear binomials and their semifields," *Finite Fields and Their Applications*, vol. 15, no. 2, pp. 125–133, 2009.

[17] Z. Zha and X. Wang, "New families of perfect nonlinear polynomial functions," *Journal of Algebra*, vol. 322, no. 11, pp. 3912–3918, 2009.

[18] J. Bierbrauer, "Commutative semifields from projection mappings," *Designs, Codes and Cryptography*, vol. 61, no. 2, pp. 187–196, 2011.

[19] A. Pott and Y. Zhou, "Switching construction of planar functions on finite fields," in *Proceedings of the Third International Workshop (WAIFI '10)*, vol. 6087 of *Lecture Notes in Computer Science*, pp. 135–150, Springer, 2010.

[20] A. Pott and Y. Zhou, "A character theoretic approach to planar functions," *Cryptography and Communications*, vol. 3, no. 4, pp. 293–300, 2011.

[21] Y. Zhou and A. Pott, "A new family of semifields with 2 parameters," *Advances in Mathematics*, vol. 234, pp. 43–60, 2013.

[22] G. Kyureghyan and F. Özbudak, "Planarity of products of two linearized polynomials," *Finite Fields and Their Applications*, vol. 18, no. 6, pp. 1076–1088, 2012.

[23] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Designs, Codes and Cryptography*, vol. 15, no. 2, pp. 125–156, 1998.

[24] G. Kyureghyan and A. Pott, "Some remarks on planar mappings," in *Proceedings of the 2nd International Workshop (WAIFI '08)*, vol. 5130 of *LNCS*, pp. 117–122, Springer, 2008.

[25] S. D. Cohen and M. J. Ganley, "Commutative semifields, two-dimensional over their middle nuclei," *Journal of Algebra*, vol. 75, no. 2, pp. 373–385, 1982.

[26] L. E. Dickson, "On commutative linear algebras in which division is always uniquely possible," *Transactions of the American Mathematical Society*, vol. 7, no. 4, pp. 514–522, 1906.

[27] G. Lunardon, G. Marino, O. Polverino, and R. Trombetti, "Symplectic spreads and quadric veroneseans," in *Proceedings of the Cryptology, Designs and Finite Groups (CDFG '09)*, Deerfield Beach, Fla, USA, 2009.

[28] N. At and S. D. Cohen, "A new tool for assurance of perfect nonlinearity," in *Sequences and Their Applications—SETA 2008*, vol. 5203, pp. 415–419, Springer, Berlin, Germany, 2008.