

Several classes of PcN power functions over finite fields

Xiaoqiang Wang, Dabin Zheng*

Abstract

Recently, a new concept called multiplicative differential cryptanalysis and the corresponding c -differential uniformity were introduced by Ellingsen et al. [11], and then some low differential uniformity functions were constructed. In this paper, we further study the constructions of perfect c -nonlinear (PcN) power functions. First, we give a necessary and sufficient condition for the Gold function to be PcN and a conjecture on all power functions to be PcN over $\text{GF}(2^m)$. Second, several classes of PcN power functions are obtained over finite fields of odd characteristic for $c = -1$ and our theorems generalize some results in [2], [16], [23]. Finally, the c -differential spectrum of a class of almost perfect c -nonlinear (APcN) power functions is determined.

Keywords: C-differential uniformity, perfect c -nonlinear function, almost perfect c -nonlinear function, differential spectrum

2010 Mathematics Subject Classification: 94A60, 11T71.

I. INTRODUCTION

Differential cryptanalysis proposed by Biham and Shamir in literature [5] is a powerful analysis method to attack block cipher, which has attracted extensive attention of researchers. The basic idea of differential cryptanalysis is to recover the key values with the greatest possibility by analyzing the influence of a specific plaintext difference on the ciphertext difference. The security

*Corresponding author. This work was partially supported by the National Natural Science Foundation of China under Grant Numbers 12001175 and 11971156.

Xiaoqiang Wang and Dabin Zheng are with the Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China (E-mail: waxiqq@163.com, dzheng@hubu.edu.cn)

of cryptographic functions against differential attacks has been extensively studied in the past 30 years. In order to measure the ability of a given function to resist differential attack, Nyberg introduced the concept of differential uniformity in [14] : Let $\text{GF}(p^m)$ denote the finite field with q elements. A function f from $\text{GF}(p^m)$ to itself is called differentially Δ_f -uniform, where

$$\Delta_f = \max_{0 \neq a \in \text{GF}(p^m)} \max_{b \in \text{GF}(p^m)} |\{x \in \text{GF}(p^m) \mid f(x+a) - f(x) = b\}|.$$

The lower the quantity of Δ_f , the stronger the ability of the function $f(x)$ to resist differential attack. If $\Delta_f = 1$ and $\Delta_f = 2$, then f is called a perfect nonlinear (PN) function and an almost perfect nonlinear (APN) function, respectively. In the past many years, a lot of progress on the constructions of PN and APN functions have been made. The reader is referred to [6], [7], [8], [9], [10], [21], [22] and the references therein for information.

Recently, a new type of differential was proposed in [5]. The authors extended the type of differential cryptanalysis by using modular multiplication as a primitive operation. For a vectorial Boolean function f , they argued that one should look at new type of differential $(f(cx), f(x))$ and not only $(f(x+a), f(x))$. Based on this work, Ellingsen et al. in [11] defined a new concept called *multiplicative differential*, and proposed the corresponding concept of c -differential uniformity as follows.

Definition 1. Let $\text{GF}(p^m)$ denote the finite field with p^m elements and $a, c \in \text{GF}(p^m)$. For a function $F(x)$ from $\text{GF}(p^m)$ to itself, the (multiplicative) c -derivative of $F(x)$ with respect to a is defined as

$${}_cD_a F(x) = F(x+a) - cF(x), \text{ for all } x.$$

For $a, b \in \text{GF}(p^m)$, let ${}_c\Delta_F(a, b) = \#\{x \in \text{GF}(p^m) : F(x+a) - cF(x) = b\}$. We call ${}_c\Delta_F = \max\{{}_c\Delta_F(a, b) : a, b \in \text{GF}(p^m), \text{ and } a \neq 0 \text{ if } c = 1\}$ the c -differential uniformity of $F(x)$.

If ${}_c\Delta_F = \delta$, then we say that F is differentially (c, δ) -uniform. If $\delta = 1$ and $\delta = 2$, then F is called a perfect c -nonlinear (PcN) function and an almost perfect c -nonlinear (APcN) function, respectively. If $c = 1$, then the c -differential uniformity becomes the usual differential uniformity, and PcN and APcN functions become PN and APN functions, respectively. It is known that APN functions over finite fields of even characteristic have the lowest differential uniformity. However, for the c -differential uniformity, there exist PcN functions.

Since the power functions with low differential uniformity are an ideal choice for S-box design, these functions have attracted a lot of attention, especially the PcN and APcN power

functions. The reader is referred to [2], [5], [13], [16], [18], [19], [23] and the references therein for information. For convenience, we list the known PcN and APcN power functions in Table 1. Among other results, the references [1], [20] also studied PcN and APcN multinomials. Table 1 shows that there are very few results on PcN power functions. For the case over finite fields with even characteristic, except for some very special cases, the Gold function is the only known PcN power function. For the case over finite fields with odd characteristic, most known PcN monomials x^d are either over finite fields $\text{GF}(3^m), \text{GF}(5^m)$ for any positive integer m , or over small extensions of any odd prime field $\text{GF}(p)$. These exponents d can be seen as special solutions of $d(p^k + 1) \equiv 2 \pmod{p^m - 1}$.

In this paper, our main objective is to construct some infinite classes of PcN power functions. First, we give a necessary and sufficient condition for the Gold function to be PcN and a conjecture of necessity and sufficiency conditions for all power functions to be PcN over finite fields with even characteristic. Second, several classes of PcN power functions x^d over $\text{GF}(p^m)$ with $c = -1$ are proposed, where p is an odd prime and d satisfies $d(p^k + 1) \equiv 2 \pmod{p^m - 1}$. Some known PcN power functions in [2], [16], [23] are some special cases of our results. Finally, the c -differential spectrum of a class of APcN power functions is given.

The rest of this paper is organized as follows. Section II documents some preliminaries. Section III gives the necessity and sufficiency for the Gold function being PcN and a conjecture for all power functions being PcN over finite fields with even characteristic. Section IV obtains some PcN power functions over finite fields with odd characteristic. Moreover, the c -differential spectrum of a class of APcN power functions is given. Section V concludes this paper.

II. NOTATION AND PRELIMINARIES

Throughout this paper, we always let m, k, d be positive integers. Let $v_2(\cdot)$ be the 2-adic order function and $v_2(0) = \infty$. Let $\text{GF}(p^m)$ denote the finite field with p^m elements, and $\text{GF}(p^m)^*$ the set of non-zero elements in $\text{GF}(p^m)$. Let η be the quadratic character of $\text{GF}(p^m)^*$, i.e., $\eta(x) = x^{\frac{p^m-1}{2}}$ for $x \in \text{GF}(p^m)^*$. Then $\eta(x) = 1$ if x is a square element in $\text{GF}(p^m)^*$ and $\eta(x) = -1$ if x is a non-square element in $\text{GF}(p^m)^*$.

Let $F(x)$ be a power function over $\text{GF}(p^m)$. It is easy to check that ${}_c\Delta_F(a, b) = {}_c\Delta_F(1, b)$ for $a \in \text{GF}(p^m)^*$ and ${}_c\Delta_F(a, b) = \gcd(d, p^m - 1)$ for $a = 0$ and $c \neq 1$. Hence, the following result on the c -differential uniformity of power functions is easily obtained, which was first given in [19].

TABLE I
PcN and APcN Power functions $F(x) = x^d$ over $\text{GF}(p^m)$ with $c \neq 1$

p	d	condition	$c\Delta_F$	Refs.
any	2	$c \neq 1$	2	[11]
any	$p^m - 2$	$c = 0$	1	[11]
2	$2^m - 2$	$c \neq 0, \text{Tr}_1^m(c) = \text{Tr}_1^m(c^{-1}) = 1$	2	[11]
odd	$p^m - 2$	$c = 4, 4^{-1}$ or $\chi(c^2 - 4c) = \chi(1 - 4c) = -1$	2	[11]
3	$\frac{3^k+1}{2}$	$c = -1, \frac{n}{\gcd(k,m)} = 1$	1	[11]
odd	$\frac{p^2+1}{2}$	$c = -1, m$ odd	1	[2]
odd	$p^2 - p + 1$	$c = -1, m = 3$	1	[2]
odd	$p^4 + (p-2)p^2$ $+(p-1)p + 1$	$c = -1, m = 5$	1	[16]
odd	$(p^5 + 1)/(p + 1)$	$c = -1, m = 5$	1	[16]
odd	$(p-1)p^6 + p^5 + (p-2)p^3$ $+(p-1)p^2 + p$	$c = -1, m = 7$	1	[16]
odd	$(p-2)p^6 + (p-2)p^5 +$ $+(p-1)p^4 + p^3 + p^2 + p$	$c = -1, m = 7$	1	[16]
odd	$(p^7 + 1)/(p + 1)$	$c = -1, m = 7$	1	[16]
3	$\frac{3^n+3}{2}$	$c = -1, m$ even	2	[13]
3	$3^n - 3$	$c = 0$	2	[13]
odd	$\frac{p^k+1}{2}$	$v_2(m) \leq v_2(k) + 1, c = -1$	1	[13]
odd	$p^k + 1$	$v_2(m) \leq v_2(k), 1 \neq c \in \mathbb{F}_{p^{\gcd(m,k)}}$	2	[13]
2	$2^k + 1$	$v_2(m) \leq v_2(k), k \geq 2, 1 \neq c \in \mathbb{F}_{2^{\gcd(m,k)}}$	1	[13]
3	$\frac{3^k+1}{2}$	k odd, $\gcd(k, m) = 1, c = -1$	2	[19]
3	$\frac{3^k+1}{2}d \equiv \frac{3^m+1}{2} \pmod{3^m - 1}$ d odd	k and m are odd such that $\gcd(m, k) = 1$	1	[23]
5	$\frac{5^k+1}{2}d \equiv \frac{5^m+1}{2} \pmod{5^m - 1}$ d odd	k and m are positive integer such that $\gcd(2m, k) = 1$	1	[23]

Lemma 2. [19, Lemma 1] Let $F(x) = x^d$ be a power function over $\text{GF}(p^m)$. Then

$$c\Delta_F = \max \{ \{c\Delta_F(1, b) : b \in \text{GF}(p^m)\} \cup \{\gcd(d, p^m - 1)\} \}.$$

PcN functions have the lowest c -differential uniformity and have been widely studied. The following result on PcN power functions is well-known and has been analyzed in [13], [15], [16], [19].

Lemma 3. [13, Theorem 6] Let p be an odd prime and m, k be integers with $1 \leq k < m$ and

$m \geq 3$. Let $F(x) = x^{\frac{p^k+1}{2}} \in \text{GF}(p^m)[x]$. If $c = -1$, then F is PcN if and only if $v_2(m) \leq v_2(k) + 1$. Otherwise, ${}_{-1}\Delta_F = \frac{p^{\gcd(k,m)+1}}{2}$.

Following the definition in [3], the c -differential spectrum of a function is given as follows.

Definition 4. Let $F(x) = x^d$ be a function over $\text{GF}(p^m)$. Denote by ω_i the number of output differences b that occur i times, that is, $\omega_i = \#\{b \in \text{GF}(p^m) \mid {}_c\Delta_F(a, b) = i\}$ for each $0 \leq i \leq {}_c\Delta_F$. The differential spectrum of F is defined to be the set

$$\mathbb{S} = \{\omega_i \mid 0 \leq i \leq {}_c\Delta_F(a, b) \text{ and } \omega_i > 0\}.$$

The following lemma will be used to compute the c -differential spectrum of some APcN functions.

Lemma 5. [4, Theorem 5.6] Let $g(x) = x^{p^k+1} - bx + b$ with $b \in \text{GF}(p^m)^*$. Then the number of the solutions to $g(x) = 0$ in $\text{GF}(p^m)$ is 0, 1, 2 or $p^{\gcd(m,k)} + 1$. Let N_i denote the number of $b \in \text{GF}(p^m)^*$ such that $g(x) = 0$ has exactly i roots in $\text{GF}(p^m)$. Let $Q = p^{\gcd(m,k)}$ and $h = [\text{GF}(p^m) : \text{GF}(p^{\gcd(m,k)})]$, then the following statements hold.

(1) If h is even, then

$$N_0 = \frac{Q^{h+1} - Q}{2(Q+1)}, N_1 = Q^{h-1}, N_2 = \frac{(Q-2)(Q^h - 1)}{2(Q-1)}, N_{Q+1} = \frac{Q^{h-1} - Q}{Q^2 - 1}.$$

(2) If p and h are odd, then

$$N_0 = \frac{Q^{h+1} - 1}{2(Q+1)}, N_1 = Q^{h-1}, N_2 = \frac{Q^{h+1} - 2Q^h - 2Q + 3}{2(Q-1)}, N_{Q+1} = \frac{Q^{h-1} - Q}{Q^2 - 1}.$$

(3) If p is even and h is odd, then

$$N_0 = \frac{Q^{h+1} + Q}{2(Q+1)}, N_1 = Q^{h-1} - 1, N_2 = \frac{(Q-2)(Q^h - 1)}{2(Q-1)}, N_{Q+1} = \frac{Q^{h-1} - 1}{Q^2 - 1}.$$

The following is a known result, which will be used throughout this paper.

Lemma 6. Let p be a prime and m, k be positive integers, then

$$\gcd(p^k + 1, p^m - 1) = \begin{cases} \frac{2^{\gcd(2k,m)} - 1}{2^{\gcd(k,m)} - 1}, & \text{if } p = 2, \\ 2, & \text{if } v_2(m) \leq v_2(k), \\ p^{\gcd(k,m)} + 1, & \text{if } v_2(m) > v_2(k). \end{cases}$$

In order to discuss the existence of the solutions of a congruence equation, we need the following known fact.

Lemma 7. *Let ϕ, φ, μ be three non-zero elements in $\text{GF}(p^m)$. Then the congruence equation $\phi x \equiv \varphi \pmod{\mu}$ has solutions if and only if $\text{gcd}(\phi, \mu) \mid \varphi$.*

III. PCN POWER FUNCTIONS OVER $\text{GF}(2^m)$

In this section, we present a necessary and sufficient condition for the Gold function to be PcN and give a conjecture of necessity and sufficiency conditions for all power functions to be PcN. To this end, we first give a general result on PcN monomials over $\text{GF}(p^m)$, where p is a prime.

Lemma 8. *Let $F(x) = x^d$ be a PcN function over $\text{GF}(p^m)$, then $F'(x) = x^{d^{-1}}$ is also a Pc'N function, where $c' = c^d$ and d^{-1} is the inverse of d modulo $p^m - 1$. Moreover, $c = c'$ if $c = \pm 1$ or 0.*

Proof. If $c = 0$, it is easy to see that the result holds. In the following, we always assume that $c \neq 0$. By the definition of PcN functions, for any $a, b \in \text{GF}(p^m)$,

$$(x+a)^d - cx^d = b$$

has only one solution in $\text{GF}(p^m)$. If $b = 0$, then the above equation becomes $(x+a)^d = cx^d$, which implies $(1+a/x)^d = c$ has only one solution for any $a \in \text{GF}(p^m)$. Hence, $(1+a/x)^d$ is a permutation polynomial over $\text{GF}(p^m)$. This means that $\text{gcd}(p^m - 1, d) = 1$. Then d has the inverse modulo $p^m - 1$ and $c = c^d$ if $c = \pm 1$. Hence,

$$(x+a)^d - cx^d = b \iff (x+a)^d = cx^d + b \iff (x+a) = (cx^d + b)^{d^{-1}}. \quad (1)$$

Let $cx^d = y$, then x can be expressed as $x = (yc^{-1})^{d^{-1}}$ and the equation in (1) becomes $(y+b)^{d^{-1}} - c^d y^{d^{-1}} = a$. Hence, $x^{d^{-1}}$ is a Pc'N function if x^d is a PcN function over $\text{GF}(p^m)$, where $c' = c^d$. This completes the proof. \square

It is known that there is no PN functions, but exist PcN functions over finite fields of even characteristic. In [13], [15], [17], [19], the authors considered the c -differential uniformity of the Gold function $F(x) = x^{2^k+1}$ over $\text{GF}(2^m)$ and showed that the Gold function has low c -differential uniformity if c, k and m satisfy some conditions. In the following theorem, we continue to analysis the Gold function $F(x) = x^{2^k+1}$ and give a necessary and sufficient condition for the Gold function to be PcN.

Theorem 9. Let $F(x) = x^{2^k+1}$ over $\text{GF}(2^m)$. Then $F(x)$ is PcN if and only if $v_2(m) \leq v_2(k)$ and $c \in \text{GF}(2^{\text{gcd}(k,m)}) \setminus \{1\}$.

Proof. It is known there does not exist PcN functions over \mathbb{F}_{2^m} if $c = 1$. From Lemma 6, $F(x)$ is PcN if and only if $v_2(m) \leq v_2(k)$ if $c = 0$. In the following, we always assume that $c \neq 0$ and $c \neq 1$.

Assume that $F(x)$ is PcN, then $\Delta(x) = b$ has only one solution for $b \in \text{GF}(2^m)$, where

$$\Delta(x) = (x+1)^{2^k+1} + cx^{2^k+1} = (c+1)x^{2^k+1} + x^{2^k} + x + 1.$$

Since $\text{gcd}(2^k, 2^m - 1) = 1$, there exists an element $\beta \in \text{GF}(2^m)^*$ such that $\beta^{2^k} = \frac{1}{c+1}$. Let $y = x + \beta$, then $\Delta(x) = b$ can be rewritten as

$$\begin{aligned} b &= (c+1)(y+\beta)^{2^k+1} + (y+\beta)^{2^k} + y + \beta + 1 \\ &= (c+1)y^{2^k+1} + (\beta^{2^k}(c+1)+1)y + (\beta(c+1)+1)y^{2^k} + \beta^{2^k+1} + \beta^{2^k} + \beta + 1 \\ &= (c+1)y^{2^k+1} + (\beta^{1-2^k}+1)y^{2^k} + \beta^{2^k+1} + \beta^{2^k} + \beta + 1 \\ &= ((c+1)y + \beta^{1-2^k} + 1)y^{2^k} + \beta^{2^k+1} + \beta^{2^k} + \beta + 1. \end{aligned} \tag{2}$$

Let $b = \beta^{2^k+1} + \beta^{2^k} + \beta + 1$, then Eq. (2) becomes

$$((c+1)y + \beta^{1-2^k} + 1)y^{2^k} = 0$$

and this equation has only one solution $y = 0$ since $\Delta(x) = b$ has only one solution for $b \in \text{GF}(2^m)$. This means that $(c+1)y + \beta^{1-2^k} + 1 = 0$ has not solutions except for $y = 0$. Since $(c+1)y$ is a permutation polynomial over $\text{GF}(2^m)$, then $\beta^{1-2^k} + 1 = 0$. Hence, Eq. (2) can be rewritten as

$$(c+1)y^{2^k+1} + \beta^{2^k+1} + \beta^{2^k} + \beta + 1 = b. \tag{3}$$

By the definition of PcN, we can deduce $\text{gcd}(2^m - 1, 2^k + 1) = 1$. From Lemma 6, we have $v_2(m) \leq v_2(k)$. From $\beta^{2^k} = \frac{1}{c+1}$, we have $\beta = \frac{1}{c^{2^m-k} + 1}$. Then $\beta^{1-2^k} + 1 = 0$ if and only if

$$\frac{\beta}{\beta^{2^k}} = \frac{1}{c^{2^m-k} + 1} / \frac{1}{c+1} = 1, \text{ i.e., } c^{2^m-k-1} = 1.$$

Since $\text{gcd}(2^{m-k} - 1, 2^m - 1) = \text{gcd}(2^k - 1, 2^m - 1)$, we have $c \in \text{GF}(2^{\text{gcd}(m,k)})$. Hence, we deduce that $v_2(m) \leq v_2(k)$ and $c \in \text{GF}(2^{\text{gcd}(m,k)}) \setminus \{1\}$ if $F(x)$ is PcN.

Now, we assume that $v_2(m) \leq v_2(k)$ and $c \in \text{GF}(2^{\text{gcd}(m,k)}) \setminus \{1\}$. From Lemma 6,

$$(c+1)y^{2^k+1} + \beta^{2^k+1} + \beta^{2^k} + \beta + 1 \tag{4}$$

is a permutation polynomial over $\text{GF}(2^m)$, where $\beta = \frac{1}{c^{2^m-k}+1}$. Let $y = x + \beta$. From Eq.(2) we know that the polynomial in (4) can be rewritten as $(c+1)x^{2^k+1} + x^{2^k} + x + 1$, which is also a permutation polynomial. This means that $F(x)$ is PcN. \square

Remark 10. In [13, Theorem 4], the authors proposed the following result: Let $2 \leq k < m$, $m \geq 3$ and $F(x) = x^{2^k+1}$ be the Gold function over $\text{GF}(2^m)$. Assume that $m = ld$, where $d = \text{gcd}(m, k)$ and $l \geq 3$. If $1 \neq c \in \text{GF}(2^d)$, the c -differential uniformity of F is ${}_c\Delta_F = \frac{2^{\text{gcd}(2k, m)} - 1}{2^{\text{gcd}(k, m)} - 1}$. If $c \in \text{GF}(2^m) \setminus \text{GF}(2^d)$, the c -differential uniformity of F is ${}_c\Delta_F = 2^d + 1$. From this result, it is easy to get that when $1 \neq c \in \text{GF}(2^d)$, $F(x) = x^{2^k+1}$ is PcN if $2 \leq k < m$ and $v_2(m) \leq v_2(k)$, where $m = ld$, $d = \text{gcd}(m, k)$ and $l \geq 3$. However, it cannot get the the necessity and sufficiency for the Gold function $F(x) = x^{2^k+1}$ to be PcN for any k .

Let $d = 2^j$ for $0 \leq j \leq m-1$ and $c \in \text{GF}(2^m) \setminus \{1\}$, one can easily deduce that the equation

$$(x+a)^d + cx^d = b$$

has only one solution in $\text{GF}(2^m)$ for any $a, b \in \text{GF}(2^m)$. Moreover, let $c \in \text{GF}(2^m)$, the c -differential uniformity of the power functions x^d and x^{dp^h} is the same for any non-negative integer h . Then combining Lemmas 8 and 9, we have the following result.

Corollary 11. Let $F(x) = x^d$ be a monomial over $\text{GF}(2^m)$. Then $F(x)$ is a PcN function if one of the following conditions hold:

- (1) $d = 2^j$ for $0 \leq j \leq m-1$ and $c \in \text{GF}(2^m) \setminus \{1\}$.
- (2) d belongs to $\{2^j(2^k+1), j=0, 1, \dots, m-1\}$ or the set of their multiplicative inverses modulo (2^m-1) for some positive integer k with $v_2(m) \leq v_2(k)$ and $c \in \text{GF}(2^{\text{gcd}(k, m)}) \setminus \{1\}$.

Example 12. Let $m = 6$ and $d \in U$, where

$$U = \{1, 2, 4, 8, 10, 13, 16, 17, 19, 20, 26, 32, 34, 38, 40, 41, 52\}.$$

Then $F(x) = x^d$ is PcN when c satisfies the corresponding condition in Corollary 11. These results have been verified by Magma programs.

We checked that the necessity of Corollary 11 by numerical experiment and found that the necessity of Corollary 11 is also right for $2 \leq m \leq 10$. However, it is not clear that whether the necessity of Corollary 11 holds for any m . So, we give the following conjecture.

Conjecture 13. Let $F(x) = x^d$ be a power function over $\text{GF}(2^m)$, then $F(x) = x^d$ is a PcN function if and only if one of the following conditions holds:

- (1) $d = 2^j$ for $0 \leq j \leq m-1$ and $c \in \text{GF}(2^m) \setminus \{1\}$.
- (2) d belongs to $\{2^j(2^k+1), j=0,1,\dots,m-1\}$ or the set of their multiplicative inverses modulo (2^m-1) for some positive integer k with $v_2(m) \leq v_2(k)$ and $c \in \text{GF}(2^{\text{gcd}(k,m)}) \setminus \{1\}$.

IV. PCN AND APCN POWER FUNCTIONS OVER $\text{GF}(p^m)$

In this section, let p be an odd prime. We will study the c -differential uniformity of some monomials and obtain some PcN power functions over $\text{GF}(p^m)$ for $c = -1$, and generalize some results in [2], [16], [23]. To this end, we need to investigate the solutions of the following equations.

$$\text{(I)} \begin{cases} x_1^2 + y_1^2 = 1, \\ x_1^{p^k+1} - y_1^{p^k+1} = -b^{\frac{p^k+1}{2}}, \end{cases} \quad \text{(II)} \begin{cases} x_2^2 - y_2^2 = 1, \\ x_2^{p^k+1} + y_2^{p^k+1} = -b^{\frac{p^k+1}{2}}, \end{cases} \quad (5)$$

$$\text{(III)} \begin{cases} x_3^2 - y_3^2 = -1, \\ x_3^{p^k+1} + y_3^{p^k+1} = b^{\frac{p^k+1}{2}}, \end{cases} \quad \text{(IV)} \begin{cases} x_4^2 + y_4^2 = -1, \\ x_4^{p^k+1} - y_4^{p^k+1} = b^{\frac{p^k+1}{2}}. \end{cases}$$

Lemma 14. Let $p^k \equiv 3 \pmod{4}$ and $p^m \equiv 3 \pmod{4}$. Let $i = 1, 2, 3, 4$ and N_i denote the tuples $(x_i, y_i) \in (\text{GF}(p^m)^*)^2$ satisfying the i -th system of equations in (5), respectively. Then $N_i = 4$ or 0 for any $b \in \text{GF}(p^m)$. Moreover, $N_i = 0$ if $b = \pm 1$.

Proof. We only show the possible values of N_1 and N_2 . The possible values of N_3 and N_4 can be computed similarly.

Firstly, we consider the system (I) and calculate the possible values of N_1 . There exists an element $t \in \text{GF}(p^{2m}) \setminus \text{GF}(p^m)$ such that $t^2 = -1$. The equation $x_1^2 + y_1^2 = 1$ can be rewritten as

$$x_1^2 - t^2 y_1^2 = (x_1 - t y_1)(x_1 + t y_1) = 1. \quad (6)$$

Denote $\theta = x_1 - t y_1$ and $\theta^{-1} = x_1 + t y_1$ in Eq. (6). So, all solutions of Eq. (6) can be expressed as

$$x_1 = \frac{\theta + \theta^{-1}}{2} \text{ and } y_1 = \frac{t(\theta - \theta^{-1})}{2}. \quad (7)$$

Since $x_1^{p^m} = x_1$, $y_1^{p^m} = y_1$ and $t^{p^m} = -t$, we have

$$(\theta + \theta^{-1})^{p^m} = \theta + \theta^{-1} \text{ and } (\theta - \theta^{-1})^{p^m} = -(\theta - \theta^{-1}).$$

These are equivalent to

$$(\theta^{p^{m+1}} - 1)(\theta^{p^m - 1} - 1) = 0 \text{ and } (\theta^{p^{m+1}} - 1)(\theta^{p^m - 1} + 1) = 0.$$

Hence,

$$\theta^{p^{m+1}} = 1. \quad (8)$$

From Eq.(7) we obtain

$$x_1^{p^k+1} - y_1^{p^k+1} = \frac{1}{4}((\theta + \theta^{-1})^{p^k+1} - (\theta - \theta^{-1})^{p^k+1}) = \frac{1}{2}(\theta^{p^k-1} + \theta^{1-p^k}) = -b \frac{p^k+1}{2}.$$

Let $\gamma = \theta^{p^k-1}$. This equation is rewritten as

$$\gamma^2 + 2b \frac{p^k+1}{2} \gamma + 1 = 0. \quad (9)$$

Assume that $b = \pm 1$. Then $b \frac{p^k+1}{2} = 1$ and Eq.(9) has only one solution $\gamma = -1$. So, $\theta^{2(p^k-1)} = 1$. Since $p^m \equiv 3 \pmod{4}$ and $p^k \equiv 3 \pmod{4}$, we know that m and k are odd. By Lemma 6, $\gcd(2(p^k - 1), p^m + 1) = 2 \gcd(p^k - 1, p^m + 1) = 4$. From Eq.(8) we have $\theta^4 = 1$. This means that $\theta^2 = \pm 1$. However, $\theta^2 = 1$ is contradictory to that $\theta^{p^k-1} = -1$. Hence, $\theta^2 = -1$, i.e., $\theta = -\theta^{-1}$. This is impossible since $x_1 \neq 0$. Therefore, $N_1 = 0$ if $b = \pm 1$.

Assume that $b \neq \pm 1$. From Lemma 6, it is easy to check that $\gcd(p^m - 1, \frac{p^k+1}{2}) = 1$ since $p^m \equiv 3 \pmod{4}$ and $p^k \equiv 3 \pmod{4}$. Then one can deduce that $b \frac{p^k+1}{2} \neq \pm 1$. So, Eq.(9) has no or two solutions in $\text{GF}(p^{2m})$. If Eq.(9) has two solutions γ_1 and γ_2 . From Eq.(8) we have

$$\gamma_1 = \theta^{p^k-1}, \theta^{p^{m+1}} = 1, \quad (10)$$

and

$$\gamma_2 = \theta^{p^k-1}, \theta^{p^{m+1}} = 1. \quad (11)$$

Since $\gamma_1 \gamma_2 = 1$, $\theta \in \text{GF}(p^{2m})$ satisfies Eq.(10) if and only if θ^{-1} satisfies Eq.(11). If $\theta_1, \theta_2 \in \text{GF}(p^{2m})$ satisfy Eq.(10), then $(\frac{\theta_1}{\theta_2})^{p^m+1} = (\frac{\theta_1}{\theta_2})^{p^k-1} = 1$. So, $(\frac{\theta_1}{\theta_2})^2 = 1$ since $\gcd(p^k - 1, p^m + 1) = 2$. As a result, if there is a θ satisfying Eq.(10), then all solutions of Eq.(10) can be represented as $\pm\theta$, and all solutions of Eq.(11) can be represented as $\pm\theta^{-1}$. Therefore, $N_1 = 4$ or 0 for any $b \in \text{GF}(p^m) \setminus \{\pm 1\}$.

Secondly, we study the system **(II)** and calculate the possible values of N_2 . From the first equation of the system **(II)**, we know

$$x_2^2 - y_2^2 = (x_2 - y_2)(x_2 + y_2) = 1.$$

Let $\delta = x_2 - y_2$ and $\delta^{-1} = x_2 + y_2$. Then,

$$x_2 = \frac{\delta + \delta^{-1}}{2} \text{ and } y_2 = \frac{\delta - \delta^{-1}}{2}.$$

Substituting x_2 and y_2 into the second equation of the system (II), we have

$$x_2^{p^k+1} + y_2^{p^k+1} = \frac{1}{4}((\delta + \delta^{-1})^{p^k+1} + (\delta - \delta^{-1})^{p^k+1}) = \frac{1}{2}(\delta^{p^k+1} + \delta^{-(p^k+1)}) = -b \frac{p^k+1}{2}. \quad (12)$$

Let $v = \delta^{p^k+1}$. Eq.(12) can be rewritten as

$$v^2 + 2b \frac{p^k+1}{2} v + 1 = 0. \quad (13)$$

Assume that $b = \pm 1$. Analysis similar to that in above cases above implies that $N_2 = 0$. Assume that $b \neq \pm 1$. We know that $b \frac{p^k+1}{2} \neq \pm 1$ since $\gcd(p^m - 1, \frac{p^k+1}{2}) = 1$. So, Eq.(13) has no or two solutions in $\text{GF}(p^{2m})$. If Eq.(13) has two solutions v_1 and v_2 . Then, we have

$$\delta^{p^m-1} = 1, v_1 = \delta^{p^k+1},$$

and

$$\delta^{p^m-1} = 1, v_2 = \delta^{p^k+1}.$$

By a similar analysis above, we know that $N_2 = 4$ or 0 for any $b \in \text{GF}(p^m) \setminus \{\pm 1\}$. \square

Lemma 15. *Let $p^k \equiv 3 \pmod{4}$ and $p^m \equiv 3 \pmod{4}$. For $b \in \text{GF}(p^m)$, any two systems in (5) cannot have solutions in $(\text{GF}(p^m)^*)^2$ simultaneously.*

Proof. We only prove that the systems (I) and (II), the systems (II) and (III) cannot have solutions simultaneously. The other cases can be similarly proved.

From Lemma 14 we know that x_1 and y_1 in (I) can be represented as $x_1 = \frac{\theta + \theta^{-1}}{2}$ and $y_1 = \frac{\theta(\theta - \theta^{-1})}{2}$, respectively, where $\theta \in \text{GF}(p^{2m})$ and $\theta^{p^m+1} = 1$. From the second equation of (I) we have

$$\frac{1}{2}(\theta^{p^k-1} + \theta^{1-p^k}) = -b \frac{p^k+1}{2}. \quad (14)$$

Similarly, x_2 and y_2 in (II) can be expressed as $x_2 = \frac{\delta + \delta^{-1}}{2}$ and $y_2 = \frac{\delta - \delta^{-1}}{2}$, respectively, where $\delta \in \text{GF}(p^m)$. From the second equation of (II) we have

$$\frac{1}{2}(\delta^{p^k+1} + \delta^{-(p^k+1)}) = -b \frac{p^k+1}{2}. \quad (15)$$

From Eqs.(14) and (15), we obtain

$$\theta^{p^k-1} + \theta^{1-p^k} - \delta^{p^k+1} - \delta^{-(p^k+1)} = 0. \quad (16)$$

Multiplying the both sides of Eq.(16) by $\theta^{p^k-1}\delta^{p^k+1}$, we have

$$\theta^{2(p^k-1)}\delta^{p^k+1} + \delta^{p^k+1} - \theta^{p^k-1}\delta^{2(p^k+1)} - \theta^{p^k-1} = (\delta^{p^k+1} - \theta^{p^k-1})(1 - \theta^{p^k-1}\delta^{p^k+1}) = 0.$$

So, $\delta^{p^k+1} = \theta^{p^k-1}$ or $\delta^{p^k+1} = \theta^{-(p^k-1)}$. Hence,

$$\delta^{(p^k+1)(p^m-1)} = \theta^{-(p^k-1)(p^m-1)} = 1.$$

Since $p^k \equiv 3 \pmod{4}$ and $p^m \equiv 3 \pmod{4}$, one can verify that $\gcd((p^k-1)(p^m-1), p^m+1) = 4$ by Lemma 6. So, $\theta^4 = 1$, i.e., $\theta^2 = 1$ or $\theta^2 = -1$. If $\theta^2 = 1$ then $y_1 = \frac{t(\theta-\theta^{-1})}{2} = 0$ and if $\theta^2 = -1$ then $x_1 = \frac{\theta+\theta^{-1}}{2} = 0$. This is contradictory to that $x_1, y_1 \in \text{GF}(p^m)^*$. Hence, (I) and (II) cannot have solutions $(x, y) \in (\text{GF}(p^m)^*)^2$ simultaneously.

Next, we show that (II) and (III) cannot have solutions $(x, y) \in (\text{GF}(p^m)^*)^2$ simultaneously. From the first equation of the system (III), let $\gamma = x_3 - y_3$ and $-\gamma^{-1} = x_3 + y_3$, where $\gamma \in \text{GF}(p^m)$. Then,

$$x_3 = \frac{\gamma - \gamma^{-1}}{2} \text{ and } y_3 = -\frac{\gamma^{-1} + \gamma}{2}.$$

The second equation of the system (III) can be rewritten as

$$\frac{1}{4}((\gamma - \gamma^{-1})^{p^k+1} + (\gamma^{-1} + \gamma)^{p^k+1}) = \frac{1}{2}(\gamma^{p^k+1} + \gamma^{-(p^k+1)}) = b^{\frac{p^k+1}{2}}. \quad (17)$$

From Eqs. (15) and (17), we have

$$\delta^{p^k+1} + \delta^{-(p^k+1)} + \gamma^{p^k+1} + \gamma^{-(p^k+1)} = 0. \quad (18)$$

Multiplying the both sides of Eq.(18) by $(\delta\gamma)^{p^k+1}$, we have

$$(\delta^2\gamma)^{p^k+1} + \delta^{p^k+1} + \delta^{p^k+1}\gamma^{2(p^k+1)} + \gamma^{p^k+1} = (\delta^{p^k+1} + \gamma^{p^k+1})((\delta\gamma)^{p^k+1} + 1) = 0.$$

So, $\delta^{p^k+1} = -\gamma^{p^k+1}$ or $\delta^{p^k+1} = -\gamma^{-(p^k+1)}$. This is a contradiction since $\delta, \gamma \in \text{GF}(p^m)$ and -1 is a non-square element in $\text{GF}(p^m)$. Hence, the systems (II) and (III) cannot have solutions simultaneously. \square

With the above preparations, we now prove the following main result.

Theorem 16. *Let $p^m \equiv 3 \pmod{4}$. Let k and d be positive integers such that $d(p^k+1) \equiv 2 \pmod{p^m-1}$. If $c = -1$, then $F(x) = x^d$ is PcN over $\text{GF}(p^m)$ if and only if d is odd.*

Proof. In order to prove this theorem, we need to show the equation

$$x^d + (x+1)^d = b \quad (19)$$

has at most one solution in $\text{GF}(p^m)$ for any $b \in \text{GF}(p^m)$. If d is even, then $x = 0$ and $x = -1$ are solutions of Eq.(19) for $b = 1$. So, d is odd if $F(x) = x^d$ is a PcN function.

In the following we will prove the sufficiency. Since $d(p^k + 1) \equiv 2 \pmod{p^m - 1}$, there exists an integer ℓ such that

$$d(p^k + 1) = 2 + \ell(p^m - 1). \quad (20)$$

If $p^k \equiv 1 \pmod{4}$, then one can deduce that ℓ is even from Eq.(20). So,

$$d\left(\frac{p^k + 1}{2}\right) \equiv 1 \pmod{p^m - 1}. \quad (21)$$

If there exists an element $d \in \text{GF}(p^m)$ such that (21) holds, from Lemma 7 we know that $\gcd(\frac{p^k + 1}{2}, p^m - 1) = 1$, i.e., $\gcd(p^k + 1, p^m - 1) = 2$. This implies that $v_2(m) \leq v_2(k)$ by Lemma 6. From Lemmas 3 and 8, we know that $F(x) = x^d$ is PcN.

Now, we show the result for the case $p^k \equiv 3 \pmod{4}$. It is clear that $x = 0$ and $x = -1$ are solutions of Eq.(19) for $b = 1$ and $b = -1$, respectively, since d is odd. Next, we always assume that x and $x + 1$ are non-zero. Let SQ and NSQ be the sets of the square and non-square elements in $\text{GF}(p^m)$, respectively. From Lemma 7, it is clear that $\gcd(p^k + 1, p^m - 1) = 2$ and $\gcd(d, p^m - 1) = 1$ since $d(p^k + 1) \equiv 2 \pmod{p^m - 1}$ and d is odd. The proof can be done in the following four cases.

Case 1: $x, x + 1 \in \text{SQ}$. We use $\alpha_0^{p^k + 1}$ and $\beta_0^{p^k + 1}$ to represent x and $x + 1$, respectively, where $\alpha_0, \beta_0 \in \text{GF}(p^m)^*$. So, $x^d = (\alpha_0^{p^k + 1})^d = \alpha_0^2$ and $(x + 1)^d = (\beta_0^{p^k + 1})^d = \beta_0^2$. From Eq.(19) we have the following system of equations,

$$\begin{cases} \alpha_0^2 + \beta_0^2 = b, \\ \alpha_0^{p^k + 1} - \beta_0^{p^k + 1} = -1. \end{cases}$$

Set $\alpha_0 = b^{\frac{1}{2}}\alpha_1$ and $\beta_0 = b^{\frac{1}{2}}\beta_1$, then

$$\begin{cases} \alpha_1^2 + \beta_1^2 = 1, \\ \alpha_1^{p^k + 1} - \beta_1^{p^k + 1} = -b^{\frac{p^k + 1}{2}}. \end{cases} \quad (22)$$

It is clear that all pairs $(\pm\alpha_1, \pm\beta_1)$ satisfying Eq. (22) give the same pair $(x, x + 1)$, i.e., the number of pairs (α_1, β_1) satisfying Eq.(22) is four times of the number of $x \in \text{GF}(p^m)^*$ satisfying Eq.(19).

Case 2: $x \in \text{SQ}$ and $x + 1 \in \text{NSQ}$. Since $p^m \equiv 3 \pmod{4}$, -1 is a non-square element in $\text{GF}(p^m)$. We use $\alpha_2^{p^k + 1}$ and $-\beta_2^{p^k + 1}$ to represent x and $x + 1$, respectively, where $\alpha_2, \beta_2 \in \text{GF}(p^m)$. So,

$x^d = (\alpha_2^{p^k+1})^d = \alpha_2^2$ and $(x+1)^d = (-\beta_2^{p^k+1})^d = -\beta_2^2$. From Eq. (19) we get the following system of equations,

$$\begin{cases} \alpha_2^2 - \beta_2^2 = b, \\ \alpha_2^{p^k+1} + \beta_2^{p^k+1} = -1. \end{cases}$$

Let $\alpha_2 = b^{\frac{1}{2}}\alpha_3$ and $\beta_2 = b^{\frac{1}{2}}\beta_3$, then

$$\begin{cases} \alpha_3^2 - \beta_3^2 = 1, \\ \alpha_3^{p^k+1} + \beta_3^{p^k+1} = -b^{\frac{p^k+1}{2}}. \end{cases} \quad (23)$$

It is easy to see that all pairs $(\pm\alpha_3, \pm\beta_3)$ satisfying Eq.(23) give the same pair $(x, x+1)$, i.e., the number of pairs (α_3, β_3) satisfying Eq.(23) is four times of the number of $x \in \text{GF}(p^m)^*$ satisfying Eq.(19).

Case 3: $x \in \text{NSQ}$ and $x+1 \in \text{SQ}$. In order to determine the number of the solutions of Eq.(19) for any $b \in \text{GF}(p^m)$, by a similar analysis to those in Case 1 and Case 2, we need to consider the number of the solutions of the following equations,

$$\begin{cases} \alpha_4^2 - \beta_4^2 = -1, \\ \alpha_4^{p^k+1} + \beta_4^{p^k+1} = b^{\frac{p^k+1}{2}}. \end{cases} \quad (24)$$

Moreover, the number of pairs (α_4, β_4) satisfying Eq.(24) is four times of the number of $x \in \text{GF}(p^m)^*$ satisfying Eq.(19).

Case 4: $x, x+1 \in \text{NSQ}$. In order to determine the number of the solutions of Eq.(19) for any $b \in \text{GF}(p^m)$, by a similar analysis to those in Case 1 and Case 2, we need to consider the number of the solutions of the following equations,

$$\begin{cases} \alpha_5^2 + \beta_5^2 = -1, \\ \alpha_5^{p^k+1} - \beta_5^{p^k+1} = b^{\frac{p^k+1}{2}} \end{cases} \quad (25)$$

Moreover, the number of pairs (α_5, β_5) satisfying Eq.(25) is four times of the number of $x \in \text{GF}(p^m)^*$ satisfying Eq.(19). Then the desired conclusion then follows from Lemmas 14 and 15. \square

Example 17. Let $c = -1$ and $k = 1$. If $p = 3, m = 5, d = 61$, or $p = 7, m = 3, d = 43$, or $p = 11, m = 3, d = 111$, then $F(x) = x^d$ is PcN. These results have been verified by Magma programs.

In the following, we discuss the (-1) -differential uniformity of the monomial x^d over $\text{GF}(p^m)$ for the case $p^m \equiv 1 \pmod{4}$, where

$$d(p^k + 1) \equiv 2 \pmod{p^m - 1}. \quad (26)$$

From Lemmas 6 and 7, there are some d such (26) holds if and only if $v_2(m) \leq v_2(k)$. Obviously, the congruence (26) is equivalent to $d(p^k + 1) = 2 + \ell(p^m - 1)$ for some integer ℓ . If ℓ is even, then $d \cdot \frac{p^k+1}{2} \equiv 1 \pmod{p^m - 1}$. In this case, by Lemmas 3 and 8 we know that x^d is a PcN function since $v_2(m) \leq v_2(k)$. If ℓ is odd then d satisfies that $d \cdot \frac{p^k+1}{2} \equiv \frac{p^m+1}{2} \pmod{p^m - 1}$. For d in this case, (-1) -differential uniformity of the monomial x^d is given in the following theorem.

Theorem 18. *Let m and k be positive integers with $v_2(k) = v_2(m)$. Let $p^m \equiv 1 \pmod{4}$ and $d \cdot \frac{p^k+1}{2} \equiv \frac{p^m+1}{2} \pmod{p^m - 1}$. Then the monomial $F(x) = x^d$ is PcN over $\text{GF}(p^m)$, where $c = -1$.*

Proof. For any $b \in \text{GF}(p^m)$, we need to show

$$(x+1)^d + x^d = b \quad (27)$$

has at most one solution in $\text{GF}(p^m)$. Since $d \cdot \frac{p^k+1}{2} \equiv \frac{p^m+1}{2} \pmod{p^m - 1}$, we have $\gcd(p^m - 1, d) \mid \frac{p^m+1}{2}$ by Lemma 7. It is clear that $\gcd(p^m - 1, \frac{p^m+1}{2}) = 1$ since $p^m \equiv 1 \pmod{4}$ and $\gcd(p^m - 1, p^m + 1) = 2$. So, $\gcd(p^m - 1, d) = 1$.

We first assume that $x \neq 0$ and $x \neq 1$. If $b = 0$, then Eq.(27) becomes $(1 + 1/x)^d = -1$ and it has a unique solution since $\gcd(p^m - 1, d) = 1$. If $b \neq 0$, then Eq.(27) can be rewritten as

$$\frac{(x+1)^d}{b} + \frac{x^d}{b} = 1. \quad (28)$$

Let $h = (p-1)/4$ if $p \equiv 1 \pmod{4}$ and $h = (3p-1)/4$ if $p \equiv 3 \pmod{4}$. Let $\gamma \in \text{GF}(p^{2m})^*$ be a solution of $x^2 + \mu x + h^2 = 0$, where $\mu \in \text{GF}(p^m)$. It is easy to check that $h^2\gamma^{-1}$ is also a solution of $x^2 + \mu x + h^2 = 0$. Then $\mu = \gamma + h^2\gamma^{-1}$. This means that any element in $\text{GF}(p^m)$ can be expressed by $-(\gamma + h^2\gamma^{-1})$ for some $\gamma \in \text{GF}(p^{2m})$. Let $-x^d/b$ denote by $\gamma + h^2\gamma^{-1} + 2h = (\gamma + h)^2/\gamma$ and $1 - x^d/b$ denote by $\gamma + h^2\gamma^{-1} + 2h + 1 = (\gamma - h)^2/\gamma$, i.e.,

$$x^d = -b \cdot \frac{(\gamma + h)^2}{\gamma} \text{ and } (x+1)^d = b \cdot \frac{(\gamma - h)^2}{\gamma}. \quad (29)$$

Let η denote the quadratic characteristic of $\text{GF}(p^m)^*$. Raising the both sides of Eqs.(29) to $\frac{p^k+1}{2}$ -th power, we have

$$x\eta(x) = x^{\frac{p^m+1}{2}} = x^d \frac{p^k+1}{2} = - \left(\frac{b}{\gamma} \right)^{\frac{p^k+1}{2}} (\gamma + h)^{p^k+1} \quad (30)$$

since $\frac{p^k+1}{2}$ is odd, and

$$(x+1)\eta(x+1) = (x+1)^{\frac{p^m+1}{2}} = (x+1)^d \frac{p^k+1}{2} = \left(\frac{b}{\gamma} \right)^{\frac{p^k+1}{2}} (\gamma - h)^{p^k+1}. \quad (31)$$

Since $d \cdot \frac{p^{k+1}}{2} \equiv \frac{p^{m+1}}{2} \pmod{p^m - 1}$ and $p^m \equiv 1 \pmod{4}$, we know that d is odd. Raising the both sides of Eqs.(30) and (31) to d th power, respectively and combining Eqs.(29), we get

$$\eta(x) = \left(\frac{b}{\gamma}\right)^{\frac{p^m-1}{2}} (\gamma+h)^{p^m-1} \text{ and } \eta(x+1) = \left(\frac{b}{\gamma}\right)^{\frac{p^m-1}{2}} (\gamma-h)^{p^m-1}. \quad (32)$$

Case I: $\eta(x+1) = \eta(x)$. From Eqs.(32) we get

$$1 = \frac{\eta(x+1)}{\eta(x)} = \left(\frac{\gamma-h}{\gamma+h}\right)^{p^m-1}.$$

This implies that $\gamma^{p^m-1} = 1$, i.e., $\gamma \in \text{GF}(p^m)$. Eq.(31) subtracting Eq.(30) implies that

$$\gamma^{p^{k+1}} - \frac{1}{2}b^{-\frac{p^{k+1}}{2}}\eta(x)\gamma^{\frac{p^{k+1}}{2}} + h^2 = 0. \quad (33)$$

Set $\theta = \gamma^{\frac{p^{k+1}}{2}}$. Since $\gamma \in \text{GF}(p^m)^*$ and $\gcd(\frac{p^{k+1}}{2}, p^m - 1) = 1$, we know that γ corresponds θ one by one. Then Eq.(33) can be rewritten as

$$\theta^2 - \frac{1}{2}b^{-\frac{p^{k+1}}{2}}\eta(x)\theta + h^2 = 0. \quad (34)$$

It is known that Eq.(34) has most two solutions θ_1 and θ_2 in $\text{GF}(p^m)$, and they satisfy $\theta_2 = h^2\theta_1^{-1}$. Since γ and θ are one one corresponding, we know that Eq.(33) has at most two solutions γ_1 and γ_2 , and they satisfy $\gamma_2^{\frac{p^{k+1}}{2}} = h^2\gamma_1^{-\frac{p^{k+1}}{2}}$. This implies that $\gamma_2 = h^2\gamma_1^{-1}$ since $\gcd(\frac{p^{k+1}}{2}, p^m - 1) = 1$ and $h \in \mathbb{F}_p$. Then $\gamma_1 + h^2\gamma_1^{-1} + 2h = \gamma_2 + h^2\gamma_2^{-1} + 2h$. This means that γ_1 and γ_2 gives the same value of x since $-x^d/b$ is denoted by $\gamma_i + h^2\gamma_i^{-1} + 2h$ for $i = 1, 2$ and $\gcd(p^m - 1, d) = 1$. Hence, Eq. (27) has at most one solution in this case.

Case II: $\eta(x+1) = -\eta(x)$. From (32) we get

$$-1 = \frac{\eta(x+1)}{\eta(x)} = \left(\frac{\gamma-h}{\gamma+h}\right)^{p^m-1}. \quad (35)$$

This equation implies that $(\frac{\gamma}{h})^{p^m+1} = 1$, i.e., $\frac{\gamma}{h}$ is in the subgroup of $(p^m + 1)$ -st roots of unity in $\text{GF}(p^{2m})^*$, denote it by \mathcal{U} . Eq. (31) plus Eq.(30) implies that

$$\gamma^{p^{k-1}} - \frac{1}{2}b^{-\frac{p^{k+1}}{2}}h^{-1}\eta(x)\gamma^{\frac{p^{k-1}}{2}} + 1 = 0. \quad (36)$$

Set $\delta = (\frac{\gamma}{h})^{\frac{p^{k-1}}{2}}$. Since $h \in \mathbb{F}_p^*$, the above equation is equivalent to

$$\delta^2 - \frac{1}{2}b^{-\frac{p^{k+1}}{2}}h^{\frac{p^{k-3}}{2}}\eta(x)\delta + 1 = 0. \quad (37)$$

Eq.(37) has at most two solutions δ_3 and δ_4 in \mathcal{U} . Since $v_2(k) = v_2(m)$, one can verify that $\gcd(\frac{p^{k-1}}{2}, p^m + 1) = 2$. So, for each solution $\delta_i (i = 3, 4)$ of Eq.(37), there are two corresponding

solutions $\pm \frac{\gamma_i}{h}$ of Eq.(36) such that $\delta_i = (\pm \frac{\gamma_i}{h})^{(p^k-1)/2}$, $i = 3, 4$. So, all possible solutions of Eq.(36) in \mathcal{U} are $\pm \frac{\gamma_3}{h}$ and $\pm \frac{\gamma_4}{h}$.

From Eq. (36), we have $\eta(x) = -2(\gamma^{p^k}h + \gamma h)(\frac{b}{\gamma})^{\frac{p^k+1}{2}}$. If $\frac{\gamma_i}{h}$ for $i = 3, 4$, is a solution of Eq.(36), substituting the values of $\eta(x)$ and $\eta(x) = -\eta(x+1)$ into Eqs.(30) and (31), respectively, we get

$$x = -\frac{(\gamma_i/h + h)^{p^k+1}}{2[(\gamma_i/h)^{p^k}h + \gamma_i]} \text{ and } x+1 = -\frac{(\gamma_i/h - h)^{p^k+1}}{2[(\gamma_i/h)^{p^k}h + \gamma_i]}. \quad (38)$$

Moreover, if $-\frac{\gamma_i}{h}$ for $i = 3, 4$, is also a solution of Eq.(36), substituting the values of $\eta(x)$ and $\eta(x) = -\eta(x+1)$ into Eqs.(30) and (31), respectively, we get

$$x = \frac{(\gamma_i/h - h)^{p^k+1}}{2[(\gamma_i/h)^{p^k}h + \gamma_i]} \text{ and } x+1 = \frac{(\gamma_i/h + h)^{p^k+1}}{2[(\gamma_i/h)^{p^k}h + \gamma_i]}. \quad (39)$$

The pairs $(x, x+1)$ in Eqs.(38) and (39) satisfying Eq.(28) simultaneously imply that $b = 0$. This is a contradiction. So, we can assume that all possible solutions of Eq.(36) in \mathcal{U} are $\frac{\gamma_3}{h}$ and $\frac{\gamma_4}{h}$. Moreover, $(\gamma_3\gamma_4/h^2)^{\frac{p^k-1}{2}} = 1$. This implies that $(\gamma_3\gamma_4/h^2)^2 = 1$ since $\gcd(\frac{p^k-1}{2}, p^m-1) = 2$. So, $\gamma_4 = \pm h^2\gamma_3^{-1}$. A similar analysis as above implies that $\gamma_4 = h^2\gamma_3^{-1}$. Then $\gamma_3 + h^2\gamma_3^{-1} + 2h = \gamma_4 + h^2\gamma_4^{-1} + 2h$. This means that γ_3 and γ_4 gives the same value of x since $-x^d/b$ is denoted by $\gamma_i + h^2\gamma_i^{-1} + 2h$ for $i = 3, 4$ and $\gcd(p^m-1, d) = 1$. Hence, Eq. (27) has at most one solution in this case since $\gcd(p^m-1, \frac{p^k+1}{2}) = 1$.

Combining the above two cases, we know that for any $b \in \text{GF}(p^m)$, Eq.(27) has at most one solution in $\text{GF}(p^m)$ if $x \neq 0$ and $x \neq -1$. Obviously, $x = 0$ and $x = -1$ are solutions of Eq.(27) for $b = 1$ and $b = -1$, respectively, since d is odd. In the following, we only show that there is no other solution to Eq.(27) than $x = 0$ for the case $b = 1$. The case of $b = -1$ can be similarly proved and the details are omitted here.

Assume that x_0 is a solution of $(x+1)^d + x^d = 1$, where $x_0 \neq 0$ and $x_0 \neq -1$. If $\eta(x_0) = \eta(x_0+1)$, Eq.(34) becomes

$$\theta^2 - \frac{1}{2}\eta(x_0)\theta + h^2 = 0. \quad (40)$$

It is easy to see that Eq.(40) has only one solution $\theta = h$ or $\theta = -h$. By the definition of θ , we have $\gamma^{\frac{p^k+1}{2}} = h$ or $\gamma^{\frac{p^k+1}{2}} = -h$. Since $h \in \text{GF}(p)$, then $(\gamma^{\frac{p^k+1}{2}})^{p-1} = 1$. Hence, $\gamma \in \text{GF}(p)$ since $\gamma^{p^m-1} = 1$ and $\gcd(p^m-1, \frac{(p^k+1)(p-1)}{2}) = p-1$. This means that $\gamma = h$ or $\gamma = -h$. This is contradictory to the equations in (29) since $x_0 \neq 0$ and $x_0 \neq -1$.

If $\eta(x_0) = -\eta(x_0+1)$, then Eq.(37) becomes

$$\delta^2 - \frac{1}{2}h^{\frac{p^k-3}{2}}\eta(x)\delta + 1 = 0. \quad (41)$$

It is easy to see that $h^{\frac{p^k-3}{2}} = \pm h^{-1}$ since $h \in \text{GF}(p)$. Then we have that Eq.(41) has only one solution $\delta = 1$ or $\delta = -1$. By the definition of δ , we have $(\frac{\gamma}{h})^{p^k-1} = 1$. Since $(\frac{\gamma}{h})^{p^{m+1}} = 1$ and $\gcd(p^m + 1, p^k - 1) = 2$, then $\gamma = h$ or $\gamma = -h$. This is contradictory to the equations in (29) since $x_0 \neq 0$ and $x_0 \neq -1$. The desired conclusion then follows. \square

Example 19. Let $c = -1$ and $k = 1$. If $p = 5, m = 5, d = 3645$, or $p = 13, m = 3, d = 157$, or $p = 17, m = 3, d = 111$, then $F(x) = x^d$ is PcN. These results have been verified by Magma programs.

Remark 20. It is clear that [23, Theorem 2] and [23, Theorem 4] can be seen as two special cases of Theorem 16 and Theorem 18 for $p = 3$ and $p = 5$, respectively.

Remark 21. In references [2], [16], authors have showed that the monomials x^d are PcN for the following exponents: $d = p^2 - p + 1$, $d = p^4 + (p-2)p^2 + (p-1)p + 1$, $d = (p^5 + 1)/(p+1)$, $d = (p-1)p^6 + p^5 + (p-2)p^3 + (p-1)p^2 + p$, $d = (p-2)p^6 + (p-2)p^5 + (p-1)p^4 + p^3 + p^2 + p$ and $d = (p^7 + 1)/(p+1)$. It is easy to show that all d listed above are special solutions of $d(p^k + 1) \equiv 2 \pmod{p^m - 1}$ for some special k and m . Hence, our results generalizes the results about PcN monomials in [2], [16].

At last, we determine the c -differential spectrum of a class of APcN power functions.

Theorem 22. Let $F(x) = x^d$ be a power function over $\text{GF}(p^m)$, where $d = p^k + 1$, k is a positive integer and p is an odd prime. If $c \in \text{GF}(p^{\gcd(m,k)}) \setminus \{1\}$, then $F(x)$ is APcN with c -differential spectrum

$$\mathbb{S} = \left\{ \omega_0 = \frac{p^m - 1}{2}, \omega_1 = 1, \omega_2 = \frac{p^m - 1}{2} \right\} \quad (42)$$

if and only if $v_2(m) \leq v_2(k)$. If $c \notin \text{GF}(p^{\gcd(m,k)})$, then $F(x)$ is APcN with c -differential spectrum

$$\mathbb{S} = \left\{ \omega_0 = \frac{p^m - p^{\frac{m}{2}}}{2}, \omega_1 = p^{\frac{m}{2}}, \omega_2 = \frac{p^m - p^{\frac{m}{2}}}{2} \right\} \quad (43)$$

if and only if m is even and $k = \frac{m}{2}$.

Proof. If $c = 1$, the c -differential uniformity of $F(x) = x^{p^k+1}$ was thoroughly analyzed in [7], [12]. In the following, we always assume that $c \neq 1$, and investigate solutions of $\Delta(x) = b$ for $b \in \text{GF}(p^m)$, where

$$\Delta(x) = (x+1)^{p^k+1} - cx^{p^k+1} = (1-c)x^{p^k+1} + x^{p^k} + x + 1.$$

Let $a = \frac{1}{1-c}$. The equation $\Delta(x) = b$ is equivalent to

$$x^{p^k+1} + ax^{p^k} + ax + a(1-b) = 0. \quad (44)$$

Let $x = y - a$, then Eq.(44) becomes

$$(x-a)^{p^k+1} + a(x-a)^{p^k} + a(x-a) + a(1-b) = x^{p^k+1} + (a-a^{p^k})x - a^2 + a - ab = 0. \quad (45)$$

It is clear that

$$a = a^{p^k} \iff \frac{1}{1-c} = \left(\frac{1}{1-c}\right)^{p^k} \iff c = c^{p^k} \iff c^{p^k-1} = 1 \quad (46)$$

for any $c \neq 1$. Then $a - a^{p^k} = 0$ if and only if $c \in \text{GF}(p^{\text{gcd}(m,k)}) \setminus \{1\}$. The proof can be done in the following two cases.

Case 1: $c \in \text{GF}(p^{\text{gcd}(m,k)}) \setminus \{1\}$. In this case, $a - a^{p^k} = 0$. Since [13, Theorem 3] have proved that $F(x)$ is APcN if $v_2(m) \leq v_2(k)$, we here only prove the c -differential spectrum of $F(x)$.

Since $a - a^{p^k} = 0$, Eq.(45) becomes

$$x^{p^k+1} = a^2 - a + ab. \quad (47)$$

From Lemma 6, we have $\text{gcd}(p^m - 1, p^k + 1) = 2$ since $v_2(m) \leq v_2(k)$. Then Eq.(47) has no solution, or one solution, or two solutions if $a^2 - a + ab$ is a non-square element, or zero, or a square element in $\text{GF}(p^m)$, respectively. Hence, we can obtain the c -differential spectrum of $F(x)$, which is given in (42).

If $F(x)$ is APcN, then Eq. (47) has at most two solutions. From Lemma 6, we have $v_2(m) \leq v_2(k)$. Hence, then $F(x)$ is APcN if and only if $v_2(m) \leq v_2(k)$.

Case 2: $c \notin \text{GF}(p^{\text{gcd}(m,k)})$. In this case, we have $a - a^{p^k} \neq 0$ from (46). If $a^2 - a + ab = 0$, then Eq.(45) can be rewritten as

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

It is clear that $x_1 = 0$ and $x_2 = a - a^{p^k}$ are the solutions of the above equation. If $a^2 - a + ab \neq 0$, by a simple substitution of variable x with $\frac{a^2 + a - ab}{a - a^k}x$ and dividing $(\frac{a^2 - a + ab}{a - a^k})^{p^k+1}$, then Eq. (45) becomes

$$x^{p^k+1} + Bx - B = 0,$$

where $B = \frac{(a - a^{p^k})^{p^k+1}}{(a^2 - a + ab)^{p^k}}$. Obviously, B runs over $\text{GF}(p^m)^*$ if b runs over $\text{GF}(p^m) \setminus (1 - a)$. From Lemma 5, we know that $F(x)$ is APcN if and only if m is even and $k = \frac{m}{2}$. And $F(x)$ has the c -differential spectrum given in (43). The desired conclusion then follows. \square

Remark 23. When $k = 0$, then x^{p^k+1} becomes x^2 . Ellingsen et al. in [11] proved that this function is APcN over $\text{GF}(p^m)$ for any $c \neq 1$. It is very easy to see that the c -differential spectrum of x^2 is the given in (42).

V. CONCLUSIONS

Recently, Ellingsen et al. in [11] proposed a new concept called multiplicative differential, and the corresponding c -differential uniformity. Then some functions with low c -differential uniformity have been constructed. This paper continued the research in [2], [13], [16], [19], [23], and mainly focused on the constructions of PcN power functions. Briefly, a necessary and sufficient condition for the Gold function being PcN was given. According to numerical experiment, we proposed a conjecture about the possible values of d for x^d to be PcN over $\text{GF}(2^m)$, where $c \in \text{GF}(2^m)$. Second, we proved that the monomial x^d over $\text{GF}(p^m)$ was PcN, where $c = -1$ and d satisfies $d(p^k + 1) \equiv 2 \pmod{p^m - 1}$. Our theorems generalized some results on PcN power functions in [2], [16], [23]. At last, the c -differential spectrum of a class of APcN power functions was obtained.

REFERENCES

- [1] D. Bartoli, M. Calderini, On construction and (non)existence of c -(almost) perfect nonlinear functions, *Finite Fields Appl.* 72 (2021) 101835.1-16.
- [2] D. Bartoli, M. Timpanella, On a generalization of planar functions, *J. Algebr. Comb.* 52 (2020) 187-213.
- [3] C. Blondeau, A. Canteaut, P. Charpin, Differential properties of power functions, *Int. J. Inf. Coding Theory*, 1(2) (2010) 149-170.
- [4] A. W. Bluhner, On $x^{q+1} + ax + b$, *Finite Fileds Appl.* 10 (2004) 285-305.
- [5] N. Borisov, M. Chew, R. Johnson, D. Wagner, Multiplicative Differentials, In: Daemen J., Rijmen V. (eds) *Fast Software Encryption. FSE 2002. LNCS 2365*, Springer, Berlin, Heidelberg, (2002) 17-33.
- [6] R. Coulter, R. Matthews, Planar functions and planes of Lenz-Barlotti class II, *Des. Codes Cryptogr.* 10(2) (1997) 167-184.
- [7] P. Dembowski, T. G. Ostrom, Planes of order n with collineation groups of order n^2 , *Math. Z.* 103 (1968) 239-258.
- [8] C. Ding, J. Yuan, A family of skew Hadamard difference sets, *J. Combin. Theory Ser. A* 113 (2006) 1526-1535.
- [9] H. Dobbertin, Almost perfect nonlinear power functions on $\text{GF}(2^n)$: The Welch case, *IEEE Trans. Inf. Theory*, 45(4) (1999) 1271-1275.
- [10] H. Dobbertin, Almost perfect nonlinear power functions on $\text{GF}(2^n)$: The Niho case, *Inform. Comput.* 151(1-2) (1999) 57-72.
- [11] P. Ellingsen, P. Felke, C. Riera, P. Stěnic̃, A. Tkachenko, C -differentials, multiplicative uniformity and (almost) perfect c -nonlinearity, *IEEE Trans. Inf. Theory*, 66(9) (2020) 5781-5789.
- [12] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, *IEEE Trans. Inf. Theory*, 14(1) (1968) 154-156.

- [13] S. Mesnager, C. Riera, P. Stănică, H. Yan, Z. Zhou, Investigations on c -(almost) perfect nonlinear functions, arXiv:2010.10023v2.
- [14] K. Nyberg, Differentially uniform mappings for cryptography, In: T. Helleseth (ed.) EUROCRYPT 1993, LNCS, vol. 765, pp. 55-64. Springer, Heidelberg, 1994.
- [15] C. Riera, P. Stănică, Investigations on c -(almost) perfect nonlinear functions, arXiv:2004.02245v2.
- [16] S. U. Hasan, M. Pal, C. Riera, P. Stănică, On the c -differential uniformity of certain maps over finite fields, Des. Codes Cryptogr. 89 (2021) 221-239.
- [17] P. Stănică, C. Riera, A. Tkachenko, Characters, Weil sums and c -differential uniformity with an application to the perturbed Gold function, arXiv:2009.07779v1.
- [18] H. Yan, On -1 -differential uniformity of ternary APN power functions, arXiv:2101.10543v1.
- [19] H. Yan, S. Mesnager, Z. Zhou, Power functions over finite fields with low c -differential uniformity, arXiv:2003.13019v3.
- [20] Y. Wu, N. Li, X. Zeng, New PcN and APcN functions over finite fields, arXiv:2010.05396v1.
- [21] Z. Zha, X. Wang, New families of perfect nonlinear polynomial functions, J. Algebra 322 (2009) 3912-3918.
- [22] Z. Zha, G. Kyureghyan, X. Wang, Perfect nonlinear binomials and their semifields, Finite Fields Appl. 15 (2009) 125-133.
- [23] Z. Zha, L. Hu, Some classes of power functions with low c -differential uniformity over finite fields, Des. Codes Cryptogr. <https://doi.org/10.1007/s10623-021-00866-8>.