Finite Fields and Their Applications 21 (2013) 11–29

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Differential spectrum of some power functions in odd prime characteristic

Sung-Tai Choi [a,*], Seokbeom Hong [a], Jong-Seon No [a], Habong Chung [b]

[a] Department of Electrical Engineering and Computer Science, INMC, Seoul National University, Seoul 151-744, Republic of Korea
[b] School of Electronics and Electrical Engineering, Hongik University, Seoul 121-791, Republic of Korea

ARTICLE INFO

Article history:
Received 28 June 2012
Revised 2 December 2012
Accepted 10 January 2013
Available online 31 January 2013
Communicated by Gary McGuire

MSC:
11T71
94A60

Keywords:
Almost perfect nonlinear
Cyclotomic class
Differential spectrum
Odd prime characteristic
Perfect nonlinear
Power function

ABSTRACT

Upper bound on Δ_f of the power function $x^{\frac{p^k+1}{2}}$ in $\mathbb{F}_{p^n}$ (Helleseth et al. (1999) [7]) is not tight, for example $p=5$, $n=3$, and $k=2$, which is the motivation of this work. In this paper, for an odd prime p, the differential spectrum of the power function $x^{\frac{p^k+1}{2}}$ in $\mathbb{F}_{p^n}$ is calculated. For an odd prime p such that $p \equiv 3 \bmod 4$ and odd n with $m|n$, the differential spectrum of the power function $x^{\frac{p^n+1}{p^m+1}+\frac{p^n-1}{2}}$ in $\mathbb{F}_{p^n}$ is also derived. We also find some new power functions which are differentially 4 and 6-uniform.

1. Introduction

Let p be a prime number and $\mathbb{F}_{p^n}$ the finite field with p^n elements. Let $f(x)$ be a mapping from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$. Let $N_f(a,b)$ denote the number of solutions $x \in \mathbb{F}_{p^n}$ of

$$f(x+a) - f(x) = b, \tag{1}$$

* Corresponding author.
E-mail address: stchoi@ccl.snu.ac.kr (S.-T. Choi).

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.01.002

where $a \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_{p^n}$. Let

$$\Delta_f = \max_{a \in \mathbb{F}_{p^n}^*, b \in \mathbb{F}_{p^n}} N_f(a,b).$$

The mapping f with $\Delta_f = k$ is said to be differentially k-uniform [2]. Mainly for the cryptographical purpose, the functions with low Δ_f have been searched extensively for many years [7–15]. Especially for an odd prime characteristic, there exist functions with $\Delta_f = 1$, which are said to be perfect nonlinear (PN). The functions with $\Delta_f = 2$, called almost perfect nonlinear (APN) are also studied extensively. Functions with Δ_f larger than two are studied in [9] and [16].

Let $f(x)$ be a power function in $\mathbb{F}_{p^n}$ given as $f(x) = x^d$. For any $a \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_{p^n}$, (1) can be rewritten as

$$f(x+a) - f(x) = a^d \left(\left(\frac{x}{a} + 1 \right)^d - \left(\frac{x}{a} \right)^d \right) = b,$$

which means that

$$N_f(a,b) = N_f\left(1, \frac{b}{a^d}\right).$$

Hence, in dealing with power functions, we will only consider $N_f(1,b)$ instead of $N_f(a,b)$.

The differential spectrum of the function $f(x)$ with $\Delta_f = k$ is defined as $(\omega_0, \omega_1, \ldots, \omega_k)$, where ω_i is given as

$$\omega_i = \left| \left\{ b \in \mathbb{F}_{p^n} \mid N_f(1,b) = i \right\} \right|.$$

Recently, the differential spectrum of some power functions have been studied [3–5]. In [5], the relationship between the differential spectrum of x^{2^t-1} and $x^{2^{n-t+1}-1}$ in $\mathbb{F}_{2^n}$ is studied and the differential spectrum of x^{2^t-1} for $t \in \{3, \lfloor n/2 \rfloor, \lceil n/2 \rceil + 1, n-2\}$ is also calculated.

For an odd prime characteristic p, Δ_f of the power function $x^{\frac{p^k+1}{2}}$ in $\mathbb{F}_{p^n}$ was first studied in [7] and it was shown that Δ_f is upper bounded as $\Delta_f \leqslant \gcd((p^k-1)/2, p^{2n}-1)$. Nevertheless, the upper bound is not tight in some cases of p, n, and k, which motivates us to derive the exact value of Δ_f for $x^{(p^k+1)/2}$.

In this paper, the differential spectrum of $x^{\frac{p^k+1}{2}}$ is first derived. Consequently the explicit Δ_f of the function is also determined. We also compute the differential spectrum of $x^{\frac{p^n+1}{p^m+1}+\frac{p^n-1}{2}}$ in $\mathbb{F}_{p^n}$ for an odd prime p such that $p \equiv 3 \bmod 4$, odd n, and $m|n$. We believe that our paper is the first to calculate the differential spectrum of power functions with an odd prime characteristic.

This paper is organized as follows. In Section 2, some preliminaries and notations are stated. In Section 3, the differential spectrum of $x^{\frac{p^k+1}{2}}$ in $\mathbb{F}_{p^n}$ is computed. In Section 4, the differential spectrum of $x^{\frac{p^n+1}{p^m+1}+\frac{p^n-1}{2}}$ in $\mathbb{F}_{p^n}$ is calculated. The conclusion is given in Section 5.

2. Preliminaries and notations

Let p be an odd prime, α be a primitive element of the finite field $\mathbb{F}_{p^n}$. Let C_0 and C_1 denote the set of squares and nonsquares in $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$, respectively. Then the cyclotomic number (i,j) is defined as the number of solutions $(x_i, x_j) \in C_i \times C_j$ such that $x_i + 1 = x_j$ for $0 \leqslant i, j \leqslant 1$.

Lemma 1. *(See [17, Lemma 6].) The cyclotomic numbers (i, j) are given as*:

1) $p^n \equiv 1 \bmod 4$:

$$(0,0) = \frac{p^n - 5}{4}; \qquad (0,1) = (1,0) = (1,1) = \frac{p^n - 1}{4}.$$

2) $p^n \equiv 3 \bmod 4$:

$$(0,0) = (1,0) = (1,1) = \frac{p^n - 3}{4}; \qquad (0,1) = \frac{p^n + 1}{4}.$$

Let E_{ij}, $0 \leqslant i, j \leqslant 1$, be the set defined as

$$E_{ij} = \left\{ x \in \mathbb{F}_{p^n}^* \;\middle|\; x \in C_i \text{ and } x + 1 \in C_j \right\}. \tag{2}$$

Then $(i, j) = |E_{ij}|$.

In the following lemma, we are going to express each $x \in E_{ij}$ in terms of the primitive element of $\mathbb{F}_{p^n}$ or $\mathbb{F}_{p^{2n}}$. The lemma will play an important role in the rest of the paper. Let $[a, b]$ denote the set of consecutive integers between a and b including a and b, that is, $[a, b] = \{a, a + 1, \ldots, b\}$.

Lemma 2. *Any element x in E_{00} can be represented as*

$$x = \left(\frac{\alpha^t - \alpha^{-t}}{2} \right)^2 \tag{3}$$

where t varies over $\mathcal{T}_1 = [1, (p^n - 3)/4]$ for $p^n \equiv 3 \bmod 4$ and over $\mathcal{T}_2 = [1, (p^n - 5)/4]$ for $p^n \equiv 1 \bmod 4$.

Any element x in E_{11} can be represented as

$$x = \gamma \left(\frac{\alpha^t - \gamma^{-1}\alpha^{-t}}{2} \right)^2 \tag{4}$$

where $\gamma = -1$ and t varies over $\mathcal{T}_1$ for $p^n \equiv 3 \bmod 4$ and $\gamma = -\alpha$ and t varies over $\mathcal{T}_2 \cup \{0\}$ for $p^n \equiv 1 \bmod 4$.

Any element x in E_{10} can be represented as

$$x = \left(\frac{\delta^{2t} - \delta^{-2t}}{2} \right)^2 \tag{5}$$

where $\delta = \beta^{(p^n-1)/2}$ and β is a primitive element in $\mathbb{F}_{p^{2n}}$ and t varies over $\mathcal{T}_1$ for $p^n \equiv 3 \bmod 4$ and over $\mathcal{T}_2 \cup \{(p^n - 1)/4\} = [1, (p^n - 1)/4]$ for $p^n \equiv 1 \bmod 4$.

Finally, any element x in E_{01} can be represented as

$$x = \left(\frac{\delta^{2t+1} - \delta^{-(2t+1)}}{2} \right)^2 \tag{6}$$

where t varies over $\mathcal{T}_1 \cup \{0\} = [0, (p^n - 3)/4]$ for $p^n \equiv 3 \bmod 4$ and over $\mathcal{T}_2 \cup \{0\} = [0, (p^n - 5)/4]$ for $p^n \equiv 1 \bmod 4$.

Proof. For $x \in E_{00}$, we can set $x+1=u^2$ and $x=v^2$ for some $u, v \in \mathbb{F}_{p^n}^*$. Then we have $u^2-v^2=(u+v)(u-v)=1$. Let $u+v=\alpha^t$. Then we have $u=(\alpha^t+\alpha^{-t})/2$ and $v=(\alpha^t-\alpha^{-t})/2$. Hence x in E_{00} is represented as $x=(\alpha^t-\alpha^{-t})^2/4$. Then we have to determine the range over which t varies. From Lemma 1, we know that $|E_{00}|=(p^n-3)/4$ for $p^n \equiv 3 \bmod 4$ and $(p^n-5)/4$ for $p^n \equiv 1 \bmod 4$. It is easy to check that $\{\alpha^t, \alpha^{-t}, -\alpha^t, -\alpha^{-t}\}$ induce the same x in (3). Note that $t=0$ makes $x=0$ and $t=(p^n-1)/4$ makes $x=0$ when $p^n \equiv 1 \bmod 4$. Hence t varies over $1 \leqslant t \leqslant (p^n-3)/4$ for $p^n \equiv 3 \bmod 4$ and $1 \leqslant t \leqslant (p^n-5)/4$ for $p^n \equiv 1 \bmod 4$.

For $x \in E_{11}$, we can set $x+1=\gamma u^2$ and $x=\gamma v^2$ for some $u, v \in \mathbb{F}_{p^n}^*$, where γ is a nonsquare in $\mathbb{F}_{p^n}^*$. Then we have $u^2-v^2=(u+v)(u-v)=\gamma^{-1}$. Let $u+v=\alpha^t$. Then we have $u-v=\gamma^{-1}\alpha^{-t}$ and thus $u=(\alpha^t+\gamma^{-1}\alpha^{-t})/2$ and $v=(\alpha^t-\gamma^{-1}\alpha^{-t})/2$. Hence $x \in E_{11}$ is represented as $x=\gamma(\alpha^t-\gamma^{-1}\alpha^{-t})^2/4$. Now, we have to determine the range over which t varies. From Lemma 1, we know that $|E_{11}|=(p^n-3)/4$ for $p^n \equiv 3 \bmod 4$ and $(p^n-1)/4$ for $p^n \equiv 1 \bmod 4$. It is easy to check that $\{\alpha^t, -\alpha^t, \gamma^{-1}\alpha^{-t}, -\gamma^{-1}\alpha^{-t}\}$ induce the same x in (4). Clearly, for the case of $p^n \equiv 3 \bmod 4$, if we set $\gamma=-1$, then each t in $\mathcal{T}_1$ makes distinct x in E_{11}. For the case of $p^n \equiv 1 \bmod 4$, each t in $\mathcal{T}_2$ makes distinct x in E_{11} for $\gamma=-\alpha$ similarly.

For $x \in E_{10}$ or E_{01}, the proof becomes a little more tricky. For $x \in E_{10}$, we can set $x+1=u^2$ and $x=\gamma v^2$ for some $u, v \in \mathbb{F}_{p^n}$, where γ is a nonsquare in $\mathbb{F}_{p^n}^*$. Then we have $u^2-\gamma v^2=1$, which can be factorized in $\mathbb{F}_{p^{2n}}$ as $u^2-\gamma v^2=(u+\lambda v)(u-\lambda v)=(u+\lambda v)(u+\lambda^{p^n} v)=(u+\lambda v)^{p^n+1}=1$, where λ and $-\lambda=\lambda^{p^n}$ are the two solutions in $\mathbb{F}_{p^{2n}}$ of $X^2=\gamma$ [1]. Since $u+\lambda v$ is the (p^n+1)-st root of unity in $\mathbb{F}_{p^{2n}}$, we can set $u+\lambda v=\beta^{(p^n-1)t}=\delta^{2t}$, where $\delta=\beta^{(p^n-1)/2}$ and β is a primitive element of $\mathbb{F}_{p^{2n}}$. Since $u+\lambda v=\delta^{2t}$ and $u-\lambda v=\delta^{-2t}$, we have $x=(\delta^{2t}-\delta^{-2t})^2/4$. Then we have to determine the range over which t varies. From Lemma 1, we know that $|E_{10}|=(p^n-3)/4$ for $p^n \equiv 3 \bmod 4$ and $(p^n-1)/4$ for $p^n \equiv 1 \bmod 4$. Note that $\{\delta^{2t}, \delta^{-2t}, -\delta^{2t}, -\delta^{-2t}\}$ induce the same x in (5). The values $t=0$, $t=(p^n+1)/2$ which make $x=0$ and $t=(p^n+1)/4$ which makes $x=-1$ should be excluded. Then each $t \in \mathcal{T}_1$ gives distinct x for $p^n \equiv 3 \bmod 4$ and so does $t \in \mathcal{T}_2 \cup \{(p^n-1)/4\}$ for $p^n \equiv 1 \bmod 4$. We can prove the case for $x \in E_{01}$ similarly. □

3. Differential spectrum of $x^{\frac{p^k+1}{2}}$ in $\mathbb{F}_{p^n}$

In [7], for an odd prime p, the upper bound on Δ_f of the power function $f(x)=x^{\frac{p^k+1}{2}}$ in $\mathbb{F}_{p^n}$ is derived. The result is stated in the following theorem.

Theorem 1. *(See [7, Theorem 11].) Let $f(x)=x^d$ be the function defined on $\mathbb{F}_{p^n}$, where p is an odd prime and $d=(p^k+1)/2$. Then we have*

$$\Delta_f \leqslant \gcd\left(\frac{p^k-1}{2}, p^{2n}-1\right).$$

However, in some cases of p, n, and k, the upper bound is not tight, which motivates us to compute the differential spectrum and Δ_f. Lemmas 3 and 4 are needed to prove the following lemmas and theorem.

Lemma 3. *Define the set $\mathcal{A}=[1, N]$ for a positive integer N. Let $N=qv+r$, where v is a positive integer divisor, q is a quotient, and r is a remainder. For an integer μ with $0 \leqslant \mu \leqslant v/2$, n_μ denote the number of $a \in \mathcal{A}$ such that $a \bmod v$ is equal to either $+\mu$ or $-\mu$. Then n_μ is determined as*:

1) *When $\mu=0$ or $v/2$ for even v*:

$$n_\mu = \begin{cases} q+1, & \text{for } \mu=\frac{v}{2} \leqslant r \text{ with even } v \\ q, & \text{for } \mu=0 \text{ or } \mu=\frac{v}{2} > r \text{ with even } v. \end{cases}$$

Table 1
Relationships among parameters.

p^n	n/e	k/e	g and e	p^k	p^e
3 mod 4	odd	odd	$g=e$	3 mod 4	3 mod 4
		even	$g=2e$	1 mod 4	
1 mod 4	even	odd	$g=e$	1 mod 4	1 mod 4
				3 mod 4	3 mod 4
	odd	odd	$g=e$	1 mod 4	1 mod 4
		even	$g=2e$		

2) *When* $0<\mu<v/2$:

$$n_\mu=\begin{cases}2(q+1), & \text{for } v-r\leqslant\mu\leqslant r\\ 2q+1, & \text{for } \mu\geqslant\max(v-r,r+1) \text{ or } \mu\leqslant\min(r,v-r-1)\\ 2q, & \text{for } r<\mu<v-r.\end{cases}$$

We will omit the proof because it is nothing more than a simple counting.

Lemma 4. *(See [18, Theorem 2.4].) Let p be an odd prime and $l=\gcd(a,b)$. Let $a'=a/l$ and $b'=b/l$. Then*

$$\gcd\left(p^a+1,p^b-1\right)=\begin{cases}p^l+1, & \text{for odd } a' \text{ and even } b'\\ 2, & \text{otherwise}.\end{cases}$$

Let $D_f(x)=f(x+1)-f(x)$ and $\mathcal{I}_{ij}$ be the image of E_{ij} under D_f, that is,

$$\mathcal{I}_{ij}=\left\{D_f(x)\;\middle|\;x\in E_{ij}\right\}$$

where $i,j\in\{0,1\}$. Also, define the set $\mathcal{U}_{ij}(b)$, $b\in\mathcal{I}_{ij}$, as the set of elements $x\in E_{ij}$ such that $D_f(x)=b$. In the following Lemmas 5–7, the cardinalities of each $\mathcal{I}_{ij}$ and $\mathcal{U}_{ij}(b)$'s, $b\in\mathcal{I}_{ij}$, will be determined. Let $e=\gcd(n,k)$ and $g=\gcd(2n,k)$ in the remainder of this section. In each proof of Lemmas 5–7, $\theta:t\mapsto x$ denotes the four bijective mappings from t to x defined in Lemma 2 shown as in (3)–(6), without distinguishing them from each other. In Table 1, the relationships among parameters p, n, k, e, and g are summarized, which is useful for separating cases in each of the lemmas and theorems in this section.

Lemma 5. *For $\mathcal{I}_{00}$ and $D_f|_{E_{00}}$, we have*:

1) *For an odd n/e (n is even or odd)*:

$$|\mathcal{I}_{00}|=\left(p^n+p^e-2\right)/\left(2\left(p^e-1\right)\right)$$

$$\left|\mathcal{U}_{00}(b)\right|=\begin{cases}\frac{p^e-3}{4}, & \text{for } b=1 \text{ and } p^n\equiv 3 \bmod 4\\ \frac{p^e-5}{4}, & \text{for } b=1 \text{ and } p^n\equiv 1 \bmod 4\\ \frac{p^e-1}{2}, & \text{for } b(\neq 1)\in\mathcal{I}_{00}.\end{cases}$$

2) *For an even n/e (n is even)*:

$$|\mathcal{I}_{00}|=\left(p^n+2p^e-3\right)/\left(2\left(p^e-1\right)\right)$$

$$\left|\mathcal{U}_{00}(b)\right| = \begin{cases} \frac{p^e-3}{4}, & \text{for } b = \pm 1 \text{ and } p^e \equiv 3 \bmod 4 \\ \frac{p^e-5}{4}, & \text{for } b = 1 \text{ and } p^e \equiv 1 \bmod 4 \\ \frac{p^e-1}{4}, & \text{for } b = -1 \text{ and } p^e \equiv 1 \bmod 4 \\ \frac{p^e-1}{2}, & \text{for } b(\neq \pm 1) \in \mathcal{I}_{00}. \end{cases}$$

Proof. From Lemma 2, $D_f(x)|_{E_{00}}$ is represented in terms of t as

$$D_f(x)|_{E_{00}} = \frac{\alpha^{(p^k-1)t} + \alpha^{-(p^k-1)t}}{2} \triangleq M\left(\alpha^{(p^k-1)t}\right) \tag{7}$$

where $x = (\alpha^t - \alpha^{-t})^2/4$ and t varies over $\mathcal{T}_1$ for $p^n \equiv 3 \bmod 4$ and $\mathcal{T}_2$ for $p^n \equiv 1 \bmod 4$.

Assume that there exist x_1 and $x_2(\neq x_1)$ in E_{00} such that $D_f(x_1) = D_f(x_2)$. Let $t_1 = \theta^{-1}(x_1)$ and $t_2 = \theta^{-1}(x_2)$. From (7), it is straightforward that t_1 and t_2 satisfy either

$$t_1 + t_2 \equiv 0 \bmod v \tag{8}$$

or

$$t_1 \equiv t_2 \bmod v \tag{9}$$

where $v = (p^n - 1)/(p^e - 1)$.

Define the set

$$S_\mu = \begin{cases} \{t \equiv \pm\mu \bmod v \mid t \in \mathcal{T}_1\}, & \text{for } p^n \equiv 3 \bmod 4 \\ \{t \equiv \pm\mu \bmod v \mid t \in \mathcal{T}_2\}, & \text{for } p^n \equiv 1 \bmod 4 \end{cases} \tag{10}$$

where $0 \leqslant \mu \leqslant \lfloor v/2 \rfloor$. Then, from (8) and (9), all the elements in S_μ give a single value $M(\alpha^{(p^k-1)t})$ in $\mathcal{I}_{00}$ and the elements in each S_μ give distinct values in $\mathcal{I}_{00}$.

Therefore, $|\mathcal{I}_{00}|$ is equal to the number of distinct sets S_μ's. Since $0 \leqslant \mu \leqslant \lfloor v/2 \rfloor$, $|\mathcal{I}_{00}|$ is equal to $(v+1)/2$ for odd v and $v/2+1$ for even v. Note that v is even when n/e is even and odd when n/e is odd.

Clearly, S_μ corresponds to $\mathcal{U}_{00}(M(\alpha^{(p^k-1)t}))$. Thus, obtaining $|\mathcal{U}_{00}(b)|$ for $b \in \mathcal{I}_{00}$ is finding the cardinality of corresponding S_μ, which can be done easily by applying Lemma 3.

Case 1). For $p^n \equiv 3 \bmod 4$.

In this case, we have

$$S_\mu = \{t \equiv \pm\mu \bmod v \mid t \in \mathcal{T}_1\}.$$

Since $\frac{p^n-3}{4} = \frac{p^e-3}{4}v + \frac{v-1}{2}$, from Lemma 3, we have

$$|S_\mu| = \left|\mathcal{U}_{00}(b)\right| = \begin{cases} \frac{p^e-1}{2}, & \text{for } 0 < \mu < \frac{v}{2} \\ \frac{p^e-3}{4}, & \text{for } \mu = 0 \end{cases}$$

where $b = D_f(x)$ for $\theta^{-1}(x) \equiv \pm\mu \bmod v$.

Since n/e is odd, i.e., v is odd, in this case, we don't need to consider $S_{v/2}$. Note that S_0 corresponds to $\mathcal{U}_{00}(1)$.

Case 2). For $p^n \equiv 1 \bmod 4$.
In this case, we have

$$S_\mu = \{t \equiv \pm\mu \bmod v \mid t \in \mathcal{T}_2\}.$$

Clearly, p^e can be congruent to 3 or 1 modulo 4 in this case.

Since $\frac{p^n-5}{4} = \frac{p^e-3}{4}v + (\frac{v}{2} - 1)$ for $p^e \equiv 3 \bmod 4$, from Lemma 3, we have

$$|S_\mu| = \left|\mathcal{U}_{00}(b)\right| = \begin{cases} \frac{p^e-1}{2}, & \text{for } 0 < \mu < \frac{v}{2} \\ \frac{p^e-3}{4}, & \text{for } \mu = 0 \text{ or } \frac{v}{2} \end{cases}$$

where $b = D_f(x)$ for $\theta^{-1}(x) \equiv \pm\mu \bmod v$. Note that n/e is even, i.e., v is even, in this case, $S_{v/2}$ should be considered. Note that S_0 corresponds to $\mathcal{U}_{00}(1)$ and $S_{v/2}$ corresponds to $\mathcal{U}_{00}(-1)$.

Since $\frac{p^n-5}{4} = \frac{p^e-5}{4}v + (v - 1)$ for $p^e \equiv 1 \bmod 4$, from Lemma 3, we have

$$|S_\mu| = \left|\mathcal{U}_{00}(b)\right| = \begin{cases} \frac{p^e-1}{2}, & \text{for } 0 < \mu < \frac{v}{2} \\ \frac{p^e-5}{4}, & \text{for } \mu = 0 \\ \frac{p^e-1}{4}, & \text{for } \mu = \frac{v}{2} \text{ and even } \frac{n}{e} \end{cases}$$

where $b = D_f(x)$ for $\theta^{-1}(x) \equiv \pm\mu \bmod v$. Here, $S_{v/2}$ should be considered only when n/e is even. Note that S_0 corresponds to $\mathcal{U}_{00}(1)$ and $S_{v/2}$ corresponds to $\mathcal{U}_{00}(-1)$. □

Lemma 6. *For $\mathcal{I}_{11}$ and $D_f|_{E_{11}}$, we have*:

1) *For an odd n/e (n is even or odd)*:

$$|\mathcal{I}_{11}| = \left(p^n + p^e - 2\right)/\left(2\left(p^e - 1\right)\right)$$

$$\left|\mathcal{U}_{11}(b)\right| = \begin{cases} \frac{p^e-3}{4}, & \textit{for } b = 1,\ p^n \equiv 3 \bmod 4,\ \textit{even } k/e \\ & \quad \textit{or } b = -1,\ p^n \equiv 3 \bmod 4,\ \textit{odd } k/e \\ \frac{p^e-1}{4}, & \textit{for } b = 1,\ p^n \equiv 1 \bmod 4,\ \textit{even } k/e \\ & \quad \textit{or } b = -1,\ p^n \equiv 1 \bmod 4,\ \textit{odd } k/e \\ \frac{p^e-1}{2}, & \textit{for remaining } b \in \mathcal{I}_{11}. \end{cases}$$

2) *For an even n/e (n is even)*:

$$|\mathcal{I}_{11}| = \left(p^n - 1\right)/\left(2\left(p^e - 1\right)\right)$$
$$\left|\mathcal{U}_{11}(b)\right| = \left(p^e - 1\right)/2, \quad \textit{for any } b \in \mathcal{I}_{11}.$$

Proof. *Case* 1). For $p^n \equiv 3 \bmod 4$.

By Lemma 2, we know that in this case $\gamma = -1$ and $D_f(x)|_{E_{11}}$ is represented as

$$D_f(x)|_{E_{11}} = M\left((-1)^{\frac{p^k-1}{2}}\alpha^{(p^k-1)t}\right) = (-1)^{\frac{p^k-1}{2}}M\left(\alpha^{(p^k-1)t}\right) \tag{11}$$

where $t \in \mathcal{T}_1$ and $x = -(\alpha^t + \alpha^{-t})^2/4$.

Since

$$(-1)^{\frac{p^k-1}{2}} = \begin{cases} 1, & \text{if } p^k \equiv 1 \bmod 4 \\ -1, & \text{if } p^k \equiv 3 \bmod 4 \end{cases}$$

and t varies over $\mathcal{T}_1$, we have $\mathcal{I}_{00} = \mathcal{I}_{11}$ for $p^k \equiv 1 \bmod 4$ and $\mathcal{I}_{00} = -\mathcal{I}_{11}$ for $p^k \equiv 3 \bmod 4$. Therefore, $|\mathcal{I}_{11}|$ and $|\mathcal{U}_{11}(b)|$ are equal to $|\mathcal{I}_{00}|$ and $|\mathcal{U}_{00}(b)|$ in Lemma 5, respectively. Note that n/e is odd in this case.

Case 2). For $p^n \equiv 1 \bmod 4$.

By Lemma 2, we know that in this case $\gamma = -\alpha$ and $D_f(x)|_{E_{11}}$ is represented as

$$D_f(x)|_{E_{11}} = M\big((-\alpha)^{\frac{p^k-1}{2}} \alpha^{(p^k-1)t}\big) \tag{12}$$

where $t \in \mathcal{T}_2 \cup \{0\}$ and $x = -\alpha(\alpha^t + \alpha^{-(t+1)})^2/4$.

Assume that $D_f(x_1) = D_f(x_2)$ for two distinct elements x_1 and x_2 in E_{11}. Let $t_1 = \theta^{-1}(x_1)$ and $t_2 = \theta^{-1}(x_2)$. Then, from (12), t_1 and t_2 should satisfy

$$t_1 + t_2 + 1 \equiv 0 \bmod v \tag{13}$$

or

$$t_1 \equiv t_2 \bmod v \tag{14}$$

where $v = (p^n - 1)/(p^e - 1)$.

Note that $\mathcal{T}_2 \cup \{0\} \cong \mathbb{Z}_{\frac{p^n-1}{4}}$. Let R_i, $0 \leqslant i \leqslant v-1$, be the equivalent class congruent to i modulo v in $\mathbb{Z}_{\frac{p^n-1}{4}}$.

From (13) and (14), we know that all the elements t in $R_i \cup R_{v-i-1}$ map to a single value in $\mathcal{I}_{11}$. Thus, obtaining $|\mathcal{U}_{11}(b)|$ is just finding out the corresponding $|R_i \cup R_{v-i-1}|$. When v is odd, i.e., n/e is odd, and $i = (v-1)/2$, R_i coincides with R_{v-i-1}. In this case, we can easily check that any t in $R_{(v-1)/2}$ maps to 1 for even k/e and -1 for odd k/e. Otherwise, $|\mathcal{U}_{11}(b)| = (p^e - 1)/2$ because $|R_i| = (p^e - 1)/4$. □

Lemma 7. *For $\mathcal{I}_{10}$, $\mathcal{I}_{01}$, $D_f|_{E_{10}}$, and $D_f|_{E_{01}}$, we have*:

1) *For an odd k/e*:
   D_f is bijective on both E_{10} and E_{01} so that $|\mathcal{I}_{10}| = |E_{10}| = (1,0)$ and $|\mathcal{I}_{01}| = |E_{01}| = (0,1)$;
   $1 \notin \mathcal{I}_{10}$ and $1 \notin \mathcal{I}_{01}$.
2) *For an even k/e*:

$$|\mathcal{I}_{10}| = |\mathcal{I}_{01}| = \big(p^n + p^e + 2\big)/\big(2\big(p^e + 1\big)\big)$$

$$\big|\mathcal{U}_{10}(b)\big| = \begin{cases} \frac{p^e-1}{4}, & \text{for } b = 1,\ p^n \equiv 1 \bmod 4 \\ \frac{p^e-3}{4}, & \text{for } b = 1,\ p^n \equiv 3 \bmod 4 \\ \frac{p^e+1}{2}, & \text{for } b(\neq 1) \in \mathcal{I}_{10} \end{cases}$$

$$\big|\mathcal{U}_{01}(b)\big| = \begin{cases} \frac{p^e-1}{4}, & \text{for } b = 1,\ p^n \equiv 1 \bmod 4 \\ \frac{p^e+1}{4}, & \text{for } b = 1,\ p^n \equiv 3 \bmod 4 \\ \frac{p^e+1}{2}, & \text{for } b(\neq 1) \in \mathcal{I}_{01}. \end{cases}$$

Proof. *Case* 1). For I_{10} and $D_f|_{E_{10}}$.

From Lemma 2, $D_f(x)|_{E_{10}}$ can be written as

$$D_f(x)|_{E_{10}} = M\big(\beta^{(p^k-1)(p^n-1)t}\big) = M\big(\delta^{2(p^k-1)t}\big) \tag{15}$$

where $x = (\delta^{2t} - \delta^{-2t})^2/4$ and t varies over $[1, (p^n-3)/4]$ for $p^n \equiv 3 \bmod 4$ and over $[1, (p^n-1)/4]$ for $p^n \equiv 1 \bmod 4$.

Let $t = \theta^{-1}(x)$. Then from (15), $\theta(t_1)$ and $\theta(t_2)$ give the same value of $D_f(x)$ if and only if

$$t_1 \pm t_2 \equiv 0 \bmod L \tag{16}$$

where $L = (p^n+1)/\gcd(p^k-1, p^n+1)$. From Lemma 4, $L = (p^n+1)/2$ for odd k/e and $L = (p^n+1)/(p^e+1)$ for even k/e.

Now, consider the case when $p^n \equiv 3 \bmod 4$ and odd k/e. Since $\mathcal{T}_1 = [1, (p^n-3)/4]$, no t_1 and t_2 in $\mathcal{T}_1$ satisfy (16) so that D_f is bijective on E_{10}. Note that there exists no $t \in \mathcal{T}_1$ such that $t \bmod L \equiv 0$, that is, $D_f(x) \neq 1$. Hence we can conclude that $|\mathcal{I}_{10}| = |E_{10}| = (p^n-3)/4$ and $1 \notin \mathcal{I}_{10}$.

For the case when $p^n \equiv 3 \bmod 4$ and even k/e, we can use Lemma 3 by setting $v = L = (p^n+1)/(p^e+1)$. In this case, q and r become $q = (p^e-3)/4$ and $r = v-1$. Note that v is odd in this case. From Lemma 3, it is derived that $|\mathcal{U}_{10}(b)| = (p^e+1)/2$ for $b(\neq 1) \in \mathcal{I}_{10}$ and $|\mathcal{U}_{10}(1)| = (p^e-3)/4$. For the case when $p^n \equiv 1 \bmod 4$, the proof can be done similarly.

Case 2). For I_{01} and $D_f|_{E_{01}}$.

In this case, $D_f(x)|_{E_{01}}$ can be written as

$$D_f(x)|_{E_{01}} = M\big(\delta^{(2t+1)(p^k-1)}\big)$$

where $x = (\delta^{2t+1} - \delta^{-(2t+1)})^2/4$ and t varies over $[0, (p^n-3)/4]$ for $p^n \equiv 3 \bmod 4$ and over $[0, (p^n-5)/4]$ for $p^n \equiv 1 \bmod 4$.

Using the similar argument to the previous case, $\theta(t_1)$ and $\theta(t_2)$ give the same value of $D_f(x)$ if and only if

$$(2t_1+1)\big(p^k-1\big) \pm (2t_2+1)\big(p^k-1\big) \equiv 0 \bmod 2\big(p^n+1\big). \tag{17}$$

Then (17) can be rewritten as either

$$t_1 - t_2 \equiv 0 \bmod L \tag{18}$$

or

$$t_1 + t_2 + 1 \equiv 0 \bmod L. \tag{19}$$

For the case when $p^n \equiv 3 \bmod 4$ and odd k/e, again D_f is bijective on E_{01} and there exists no x such that $D_f(x) = 1$. Thus, $|\mathcal{I}_{01}| = |E_{01}| = (p^n+1)/4$ and $1 \notin \mathcal{I}_{01}$.

For the case when $p^n \equiv 3 \bmod 4$ and even k/e, applying Lemma 3 to (18) and (19) yields that $|\mathcal{U}_{01}(b)| = (p^e+1)/2$ for $b(\neq 1) \in \mathcal{I}_{01}$ and $|\mathcal{U}_{01}(1)| = (p^e+1)/4$. For the case when $p^n \equiv 1 \bmod 4$, the proof can be done similarly. □

So far, we have investigated the cardinality of the images, $|\mathcal{I}_{ij}|$, and the inverse images, $|\mathcal{U}_{ij}(b)|$, of $D_f|_{E_{ij}}$, $i, j \in \{0, 1\}$. In order to unify Lemmas 5–7 and to see the overall mapping property of D_f, we have to look into the relationship between $\mathcal{I}_{00}$, $\mathcal{I}_{11}$, $\mathcal{I}_{10}$, and $\mathcal{I}_{01}$ in the following three lemmas.

Lemma 8. *For $\mathcal{I}_{00}$ and $\mathcal{I}_{11}$, we have*

$$\begin{cases} \mathcal{I}_{00} = \mathcal{I}_{11}, & \text{for even } \frac{k}{e} \\ \mathcal{I}_{00} \cap \mathcal{I}_{11} = \emptyset, & \text{for odd } \frac{k}{e}. \end{cases}$$

Proof. *Case* 1). For $p^n \equiv 3 \bmod 4$.

From Lemma 6, if $p^k \equiv 1 \bmod 4$, we have $\mathcal{I}_{00} = \mathcal{I}_{11}$, k/e is even, and the first equation of the lemma is proved. From the same lemma, if $p^k \equiv 3 \bmod 4$, we have $\mathcal{I}_{00} = -\mathcal{I}_{11}$ and k/e is odd. To prove the second equation, we want to show that any two elements a and $-a$ cannot belong to $\mathcal{I}_{00}$. Assume that there are two distinct elements x_1 and x_2 in E_{00} such that $D_f(x_1) = -D_f(x_2)$. Let $t_1 = \theta^{-1}(x_1)$ and $t_2 = \theta^{-1}(x_2)$. Then from (7), it is easy to see that either $\alpha^{(p^k-1)t_1} = -\alpha^{(p^k-1)t_2}$ or $\alpha^{(p^k-1)t_1} = -\alpha^{-(p^k-1)t_2}$ must hold. But this is a contradiction because $-\alpha^{\pm(p^k-1)t_2}$ is a nonsquare in $\mathbb{F}_{p^n}$, whereas $\alpha^{(p^k-1)t_1}$ is a square in $\mathbb{F}_{p^n}$. Therefore, $\mathcal{I}_{00} \cap \mathcal{I}_{11} = \mathcal{I}_{00} \cap (-\mathcal{I}_{00}) = \emptyset$ for odd k/e.

Case 2). For $p^n \equiv 1 \bmod 4$.

Again, assume that there exist $x_1 \in E_{00}$ and $x_2 \in E_{11}$ such that $D_f(x_1) = D_f(x_2)$. Let $t_1 = \theta^{-1}(x_1) \in \mathcal{T}_2$ and $t_2 = \theta^{-1}(x_2) \in \mathcal{T}_2 \cup \{0\}$. Then, from (7) and (12), we have

$$(-\alpha)^{\frac{p^k-1}{2}} \alpha^{(p^k-1)t_2} = \alpha^{(p^k-1)t_1} \text{ or } \alpha^{-(p^k-1)t_1}. \tag{20}$$

For $p^k \equiv 3 \bmod 4$, (20) cannot be satisfied because the left-hand side of (20) is a nonsquare in $\mathbb{F}_{p^n}$, while the right-hand side of (20) is a square in $\mathbb{F}_{p^n}$.

For $p^k \equiv 1 \bmod 4$, (20) implies that either $\alpha^{\frac{p^k-1}{2}(2t_1+2t_2+1)} = 1$ or $\alpha^{\frac{p^k-1}{2}(2t_2-2t_1+1)} = 1$, which further implies that either $2(t_1+t_2)+1$ or $2(t_2-t_1)+1$ must be divisible by $2(p^n-1)/(p^e-1)$ for odd k/e and $(p^n-1)/(p^e-1)$ for even k/e.

Since $2(t_2 \pm t_1)+1$ is odd, we can easily see that the above is possible only when k/e is even and n/e is odd and that such t_1 and t_2 can be always found in $\mathcal{T}_2$ and $\mathcal{T}_2 \cup \{0\}$, respectively. Note that n/e is always odd when k/e is even. Hence we conclude that $\mathcal{I}_{00} = \mathcal{I}_{11}$ for even k/e and $\mathcal{I}_{00} \cap \mathcal{I}_{11} = \emptyset$, otherwise. □

Lemma 9. *For $\mathcal{I}_{10}$ and $\mathcal{I}_{01}$, we have*

$$\begin{cases} \mathcal{I}_{10} \cap \mathcal{I}_{01} = \emptyset, & \text{for odd } \frac{k}{e} \text{ and } p^e \equiv 3 \bmod 4 \\ \mathcal{I}_{10} = \mathcal{I}_{01}, & \text{otherwise}. \end{cases}$$

Proof. Assume that there exist $x_1 \in E_{10}$ and $x_2 \in E_{01}$ such that $D_f(x_1) = D_f(x_2)$. Let $t_1 = \theta^{-1}(x_1)$ and $t_2 = \theta^{-1}(x_2)$. Then, from Lemma 2, we have

$$\delta^{2t_1(p^k-1)} + \delta^{-2t_1(p^k-1)} = \delta^{(2t_2+1)(p^k-1)} + \delta^{-(2t_2+1)(p^k-1)}. \tag{21}$$

Since $\delta^{2(p^n+1)} = 1$, the necessary and sufficient conditions for (21) to hold is

$$2(t_2 \pm t_1) + 1 \equiv 0 \bmod L \tag{22}$$

where $L = 2(p^n+1)/\gcd(2(p^n+1), p^k-1)$.

Note that t_1 lies in $[1, (p^n-3)/4]$ for $p^n \equiv 3 \bmod 4$ and in $[1, (p^n-1)/4]$ for $p^n \equiv 1 \bmod 4$ and t_2 lies in $[0, (p^n-3)/4]$ for $p^n \equiv 3 \bmod 4$ and in $[0, (p^n-5)/4]$ for $p^n \equiv 1 \bmod 4$.

When L becomes even, which occurs only if k/e is odd and $p^e \equiv 3 \bmod 4$, (22) cannot be satisfied because the left-hand side of (22) is odd. Hence we conclude that $\mathcal{I}_{01} \cap \mathcal{I}_{10} = \emptyset$ in this case.

Otherwise, it is not difficult to find t_2 satisfying (22) for each t_1 because L is either $(p^n+1)/2$ or $(p^n+1)/(p^e+1)$ which is odd. Since $|\mathcal{I}_{10}| = |\mathcal{I}_{01}|$ in Lemma 7, the proof is done. □

Lemma 10. *Let $\mathcal{S}_1 = \mathcal{I}_{00} \cup \mathcal{I}_{11}$ and $\mathcal{S}_2 = \mathcal{I}_{01} \cup \mathcal{I}_{10}$. Then we have*

$$\mathcal{S}_1 \cap \mathcal{S}_2 = \begin{cases} \emptyset, & \text{for odd } \frac{k}{e} \\ \{1\}, & \text{for even } \frac{k}{e}. \end{cases}$$

Proof. The proof is in Appendix A. □

Using the previous lemmas, the main theorem can be stated as follows. Note that the differential spectrum of $f(x)$ with $\Delta_f = k$ is defined as $(\omega_0, \omega_1, \ldots, \omega_k)$, where ω_i denotes the number of $b \in \mathbb{F}_{p^n}$ such that $N_f(1, b) = i$.

Theorem 2. *For an odd prime p, $d = (p^k + 1)/2$, and $e = \gcd(n, k)$, the differential spectrum of the function $f(x) = x^d$ in $\mathbb{F}_{p^n}$ is given as*:

1) *For an odd k/e*:
   1-i) *For $p^e \equiv 3 \bmod 4$*:

$$\omega_i = \begin{cases} 2, & \text{if } i = \frac{p^e+1}{4} \text{ (the corresponding two } b\text{'s are } \pm 1) \\ \frac{p^n-p^e}{p^e-1}, & \text{if } i = \frac{p^e-1}{2} \\ \frac{p^n-1}{2}, & \text{if } i = 1 \\ \frac{p^n-3}{2} - \frac{p^n-p^e}{p^e-1}, & \text{if } i = 0 \\ 0, & \text{otherwise}. \end{cases}$$

   1-ii) *For $p^e \equiv 1 \bmod 4$*:

$$\omega_i = \begin{cases} 1, & \text{if } i = \frac{p^e+3}{4} \text{ (the corresponding } b \text{ is } 1) \\ 1, & \text{if } i = \frac{p^e-1}{4} \text{ (the corresponding } b \text{ is } -1) \\ \frac{p^n-p^e}{p^e-1}, & \text{if } i = \frac{p^e-1}{2} \\ \frac{p^n-1}{4}, & \text{if } i = 2 \\ \frac{(p^n-1)(3p^e-7)}{4(p^e-1)}, & \text{if } i = 0 \\ 0, & \text{otherwise}. \end{cases}$$

2) *For an even k/e*:

$$\omega_i = \begin{cases} 1, & \text{if } i = p^e \text{ (the corresponding } b \text{ is } 1) \\ \frac{p^n-p^e}{2(p^e-1)}, & \text{if } i = p^e - 1 \\ \frac{p^n-p^e}{2(p^e+1)}, & \text{if } i = p^e + 1 \\ p^n - \frac{p^{n+e}-1}{p^{2e}-1}, & \text{if } i = 0 \\ 0, & \text{otherwise}. \end{cases}$$

Proof. So far, we have derived $|\mathcal{I}_{ij}|$'s and $|\mathcal{U}_{ij}(b)|$'s in Lemmas 5–7. From Lemmas 8 and 9, we have seen that $\mathcal{I}_{00}$ and $\mathcal{I}_{11}$ are either disjoint or identical and so be $\mathcal{I}_{01}$ and $\mathcal{I}_{10}$. Finally, from Lemma 10, we have seen that $\mathcal{I}_{00} \cup \mathcal{I}_{11}$ and $\mathcal{I}_{01} \cup \mathcal{I}_{10}$ are either disjoint or almost disjoint. For the proof of this theorem, we have to combine these results.

Case 1). Combining $D_f|_{E_{00}}$ and $D_f|_{E_{11}}$.

For the case when k/e is odd, we have $|\mathcal{I}_{00} \cup \mathcal{I}_{11}| = (p^n + p^e - 2)/(p^e - 1)$ because $\mathcal{I}_{00}$ and $\mathcal{I}_{11}$ are disjoint. For any $b \in (\mathcal{I}_{00} \cup \mathcal{I}_{11}) \setminus \{1, -1\}$, the cardinality of $\mathcal{U}_0(b)$, the inverse image in $E_{00} \cup E_{11}$ of b, is $(p^e - 1)/2$. For the elements $\pm 1 \in \mathcal{I}_{00} \cup \mathcal{I}_{11}$, we have

$$\big(|\mathcal{U}_0(1)|, |\mathcal{U}_0(-1)|\big) = \begin{cases} (\frac{p^e-5}{4}, \frac{p^e-1}{4}), & \text{for } p^e \equiv 1 \bmod 4 \\ (\frac{p^e-3}{4}, \frac{p^e-3}{4}), & \text{for } p^e \equiv 3 \bmod 4. \end{cases}$$

For the case when k/e is even, we have $|\mathcal{I}_{00} \cup \mathcal{I}_{11}| = (p^n + p^e - 2)/(2(p^e - 1))$ since $\mathcal{I}_{00}$ and $\mathcal{I}_{11}$ coincide. Also, we have

$$|\mathcal{U}_0(b)| = \begin{cases} p^e - 1, & \text{if } b \in (\mathcal{I}_{00} \cup \mathcal{I}_{11}) \setminus \{1\} \\ \frac{p^e-3}{2}, & \text{if } b = 1. \end{cases}$$

Case 2). Combining $D_f|_{E_{10}}$ and $D_f|_{E_{01}}$.

For the case when k/e is odd, we have $|\mathcal{I}_{10} \cup \mathcal{I}_{01}| = |\mathcal{I}_{10}| = |\mathcal{I}_{01}| = (p^n - 1)/4$ for $p^e \equiv 1 \bmod 4$ and $|\mathcal{I}_{10} \cup \mathcal{I}_{01}| = |\mathcal{I}_{10}| + |\mathcal{I}_{01}| = (p^n - 1)/2$ for $p^e \equiv 3 \bmod 4$. The cardinality of $\mathcal{U}_1(b)$, the inverse image in $E_{10} \cup E_{01}$ of $b \in (\mathcal{I}_{10} \cup \mathcal{I}_{01})$, is

$$|\mathcal{U}_1(b)| = \begin{cases} 2, & \text{for } p^e \equiv 1 \bmod 4 \\ 1, & \text{for } p^e \equiv 3 \bmod 4. \end{cases}$$

For the case when k/e is even, we have $|\mathcal{I}_{10} \cup \mathcal{I}_{01}| = |\mathcal{I}_{10}| = |\mathcal{I}_{01}| = (p^n + p^e + 2)/(2(p^e + 1))$. Also, we have

$$|\mathcal{U}_1(b)| = \begin{cases} p^e + 1, & \text{if } b \in (\mathcal{I}_{10} \cup \mathcal{I}_{01}) \setminus \{1\} \\ \frac{p^e-1}{2}, & \text{if } b = 1. \end{cases}$$

The unified mapping property of $D_f|_{E_{10}}$ and $D_f|_{E_{01}}$ is that the cardinality of the inverse image in $E_{10} \cup E_{01}$ of each element in $(\mathcal{I}_{10} \cup \mathcal{I}_{01}) \setminus \{1\}$ is $p^e + 1$ and the cardinality of the inverse image in $E_{10} \cup E_{01}$ of the element $1 \in \mathcal{I}_{10} \cup \mathcal{I}_{01}$ is $(p^e - 1)/2$.

Since $x = 0, -1 \notin (E_{00} \cup E_{11} \cup E_{10} \cup E_{01})$, we have to consider the case when $x = 0$ and $x = -1$. It is easy to derive that $D_f(0) = 1$ and $D_f(-1) = (-1)^{(p^k+3)/2}$. Finally, with Lemma 10, we can combine Case 1) and Case 2). Hence the proof is done. □

Corollary 1. *For an odd prime p and $d = (p^k + 1)/2$, Δ_f of $f(x) = x^d$ in $\mathbb{F}_{p^n}$ is given as*

$$\Delta_f = \begin{cases} \frac{p^e-1}{2}, & \textit{for odd } \frac{k}{e} \\ p^e + 1, & \textit{for even } \frac{k}{e} \end{cases}$$

where $e = \gcd(n, k)$.

Note that the derived differential spectrum in the above theorem is very sparse. The comparison with the existing bound in Theorem 1 and our new result in Corollary 2 is given in Table 2. The bound in Theorem 1 is not tight for some cases of $d = (p^k + 1)/2$, whereas Theorem 2 provides the exact differential spectrum and Δ_f. There have been few works about the differential spectrum. Especially with odd characteristic, we believe that this is the first work to derive the differential spectrum.

Table 2
Comparison between the existing bound in Theorem 1 and new result in Corollary 2.

p	n	k	Upper bound on Δ_f in [7]	Explicit Δ_f (new result)
5	3	2	12	6
5	5	2	12	6
5	5	4	24	6
7	3	2	24	8
7	5	2	24	8
7	5	4	48	8
7	7	2	24	8
7	7	4	48	8
7	7	6	24	8
11	3	2	60	12

4. Differential spectrum of $x^{\frac{p^n+1}{p^m+1}+\frac{p^n-1}{2}}$ in $\mathbb{F}_{p^n}$

Let n be an odd integer, p an odd prime such that $p \equiv 3 \bmod 4$, and m a divisor of n, i.e., $m|n$. Then we consider the power function $f(x) = x^d$ with the power $d = (p^n+1)/(p^m+1) + (p^n-1)/2$. Note that only when $p^m \equiv 3 \bmod 4$, i.e., $p \equiv 3 \bmod 4$, and n is odd, there exists no inverse $d^{-1} = (p^m+1)/2$ which has already been dealt with in the previous section. Therefore we restrict p and n to $p \equiv 3 \bmod 4$ and odd n in computing Δ_f and the differential spectrum of $f(x) = x^d$ in this section.

Define the functions $h_i(x)$ in $\mathbb{F}_{p^n}$, $1 \leqslant i \leqslant 4$, as

$$\begin{aligned}
h_1(x) &= (x+1)^{\frac{p^m+1}{2}} + x^{\frac{p^m+1}{2}} \\
h_2(x) &= (x+1)^{\frac{p^m+1}{2}} - x^{\frac{p^m+1}{2}} \\
h_3(x) &= -(x+1)^{\frac{p^m+1}{2}} + x^{\frac{p^m+1}{2}} \\
h_4(x) &= -(x+1)^{\frac{p^m+1}{2}} - x^{\frac{p^m+1}{2}}.
\end{aligned}$$

Let $\lambda_i(b)$ and $\chi_i(b)$, $1 \leqslant i \leqslant 4$, be the number of solutions of

$$h_i(x) = b^{-\frac{p^m+1}{2}} \tag{23}$$

in E_{00} and E_{11}, respectively.

Lemma 11. *For $f(x) = x^{\frac{p^n+1}{p^m+1}+\frac{p^n-1}{2}}$ and $b \in \mathbb{F}_{p^n}^*$, $N_f(1,b)$ is determined as*:

1) *For $b \neq \pm 1$:*

$$N_f(1,b) = \begin{cases} \lambda_1(b) + \lambda_2(b) + \lambda_3(b) + \lambda_4(b), & \text{for } b \in C_0 \setminus \{1\} \\ \chi_1(b) + \chi_2(b) + \chi_3(b) + \chi_4(b), & \text{for } b \in C_1 \setminus \{-1\}. \end{cases}$$

2) *For $b = \pm 1$:*

$$N_f(1,b) = \begin{cases} \lambda_1(b) + \lambda_2(b) + \lambda_3(b) + \lambda_4(b) + 1, & \text{for } b = 1 \\ \chi_1(b) + \chi_2(b) + \chi_3(b) + \chi_4(b) + 1, & \text{for } b = -1. \end{cases}$$

Proof. Consider the cases when $x \in \mathbb{F}_{p^n}^* \setminus \{-1\}$. Since $\gcd(p^m+1, p^n-1) = 2$, any element $x \in E_{00}$ can be expressed as $x = \nu^{p^m+1}$ and $x+1 = \psi^{p^m+1}$ for some ν and ψ. If this x is a solution to $D_f(x) = b$, then we have

$$(x+1)^{\frac{p^n+1}{p^m+1}+\frac{p^n-1}{2}} - x^{\frac{p^n+1}{p^m+1}+\frac{p^n-1}{2}} = \psi^2 - \nu^2 = b. \tag{24}$$

By setting $y = b^{-1}\nu^2$, we have $y+1 = b^{-1}\psi^2$ and thus y becomes the solution to

$$h_2(y) = (y+1)^{\frac{p^m+1}{2}} - y^{\frac{p^m+1}{2}} = b^{-\frac{p^m+1}{2}}. \tag{25}$$

Since the transformation x to y is one-to-one, each solution $x \in E_{00}$ to $D_f(x) = b$ corresponds to either a solution $y \in E_{00}$ to (25) for $b \in C_0$ or a solution $y \in E_{11}$ to (25) for $b \in C_1$.

Similarly, if $x \in E_{11}$ is a solution to $D_f(x) = b$, then by letting $x+1 = -\psi^{p^m+1}$ and $x = -\nu^{p^m+1}$, we have (24). Again by setting $y = b^{-1}\nu^2$, we have $y+1 = b^{-1}\psi^2$. Thus y is a solution to

$$h_3(y) = -(y+1)^{\frac{p^m+1}{2}} + y^{\frac{p^m+1}{2}} = b^{-\frac{p^m+1}{2}}. \tag{26}$$

Since the transformation x to y is one-to-one, each solution $x \in E_{11}$ to $D_f(x) = b$ corresponds to either a solution $y \in E_{00}$ to (26) for $b \in C_0$, or a solution $y \in E_{11}$ to (26) for $b \in C_1$.

Similarly, if $x \in E_{10}$ is a solution to $D_f(x) = b$, then by letting $x+1 = \psi^{p^m+1}$ and $x = -\nu^{p^m+1}$, we have (24). Again by setting $y = b^{-1}\nu^2$, we have $y+1 = b^{-1}\psi^2$. Thus y is a solution to

$$h_1(y) = (y+1)^{\frac{p^m+1}{2}} + y^{\frac{p^m+1}{2}} = b^{-\frac{p^m+1}{2}}. \tag{27}$$

Since the transformation x to y is one-to-one, each solution $x \in E_{11}$ to $D_f(x) = b$ corresponds to either a solution $y \in E_{00}$ to (27) for $b \in C_0$ or a solution $y \in E_{11}$ to (27) for $b \in C_1$.

Similarly, if $x \in E_{01}$ is a solution to $D_f(x) = b$, then by letting $x+1 = -\psi^{p^m+1}$ and $x = \nu^{p^m+1}$, we have (24). Again by setting $y = b^{-1}\nu^2$, we have $y+1 = b^{-1}\psi^2$. Thus y is a solution to

$$h_4(y) = -(y+1)^{\frac{p^m+1}{2}} - y^{\frac{p^m+1}{2}} = b^{-\frac{p^m+1}{2}}. \tag{28}$$

Since the transformation x to y is one-to-one, each solution $x \in E_{11}$ to $D_f(x) = b$ corresponds to either a solution $y \in E_{00}$ to (28) for $b \in C_0$ or a solution $y \in E_{11}$ to (28) for $b \in C_1$.

Since $D_f(0) = 1$ and $D_f(-1) = -1$, we have completed the proof. □

Using the above lemma, the differential spectrum of $f(x)$ can be derived as follows.

Theorem 3. *For an odd prime p such that $p \equiv 3 \bmod 4$, odd n with $m|n$, and $d = (p^n+1)/(p^m+1) + (p^n-1)/2$, the differential spectrum of $f(x) = x^d$ in $\mathbb{F}_{p^n}$ is given as*

$$\omega_i = \begin{cases} 2, & \text{if } i = \frac{p^m+1}{4} \text{ (the corresponding two } b\text{'s are } \pm 1) \\ \frac{p^n-p^m}{p^m-1}, & \text{if } i = \frac{p^m+1}{2} \\ \frac{p^n-1}{2} - \frac{p^n-p^m}{p^m-1}, & \text{if } i = 1 \\ \frac{p^n-3}{2}, & \text{if } i = 0 \\ 0, & \text{otherwise.} \end{cases}$$

Proof. From Lemma 11, in order to determine $N_f(1,b)$, we should calculate $\sum_{i=1}^{4}\lambda_i(b)$ and $\sum_{i=1}^{4}\chi_i(b)$ for $b\in C_0$ and $b\in C_1$, respectively. From Lemma 2, $h_1(x)$ and $h_2(x)$ on E_{00} can be represented as

$$h_1(x)|_{E_{00}}=\frac{\alpha^{t(p^m+1)}+\alpha^{-t(p^m+1)}}{2}$$
$$h_2(x)|_{E_{00}}=\frac{\alpha^{t(p^m-1)}+\alpha^{-t(p^m-1)}}{2} \tag{29}$$

where $x=(\alpha^t-\alpha^{-t})^2/4$ and t varies over $\mathcal{T}_1$. Similarly, $h_1(x)$ and $h_2(x)$ on E_{11} can be represented as

$$h_1(x)|_{E_{11}}=\frac{\alpha^{t(p^m+1)}+\alpha^{-t(p^m+1)}}{2}$$
$$h_2(x)|_{E_{11}}=-\frac{\alpha^{t(p^m-1)}+\alpha^{-t(p^m-1)}}{2} \tag{30}$$

where $x=-(\alpha^t+\alpha^{-t})^2/4$ and t varies over $\mathcal{T}_1$. Note that $h_1(x)=-h_4(x)$ and $h_2(x)=-h_3(x)$.

Since $\gcd((p^m+1)/2,p^n-1)=2$, $b^{-\frac{p^m+1}{2}}$ in (23) varies over C_0 twice, while b varies over $\mathbb{F}_{p^n}^*$. Note that $b=\pm\lambda$ give the same $b^{-\frac{p^m+1}{2}}$ and one of $\pm\lambda$ is a square in $\mathbb{F}_{p^n}$ and the other is a nonsquare in $\mathbb{F}_{p^n}$. Hence, in order to determine $N_f(1,b)$ for $b\in\mathbb{F}_{p^n}^*$, we need to derive the mapping property of $h_i(x)=c$, $1\leqslant i\leqslant 4$, where c is a square in $\mathbb{F}_{p^n}$, for $x\in E_{00}$ and $x\in E_{11}$, respectively. Then, using Lemma 11, the differential spectrum of $f(x)$ can be determined.

Define the sets as

$$\mathcal{H}_{ijl}=\left\{h_i(x)\;\middle|\;x\in E_{jl}\right\}.$$

For $b\in C_0$, we should consider the mapping property of $h_i(x)=c$ on E_{00}, where c is a square in $\mathbb{F}_{p^n}$. Assume that there exist $x_1,x_2\in E_{00}$ such that $h_1(x_1)=h_1(x_2)$ for $x_1\neq x_2$. Let $t_1=\theta^{-1}(x_1)$ and $t_2=\theta^{-1}(x_2)$. Then, from (29), it is easy to derive that $(p^m+1)t_1\equiv\pm(p^m+1)t_2 \bmod p^n-1$. Since $(p^m+1,p^n-1)=2$, we have $t_1\pm t_2\equiv 0 \bmod (p^n-1)/2$, which cannot be satisfied because $1\leqslant t_1,t_2\leqslant(p^n-3)/4$. Hence we conclude that $h_1(x)|_{E_{00}}$ is injective on E_{00}, that is, $|\mathcal{H}_{100}|=|E_{00}|=(p^n-3)/4$.

Consider the mapping $h_2(x)|_{E_{00}}$, which has the same form as (7). Therefore we can use the result when $p^n\equiv 3 \bmod 4$ in Lemma 5 and thus we have $|\mathcal{H}_{200}|=(p^n+p^m-2)/(2(p^m-1))$. The cardinality of the inverse image in E_{00} of any element in $\mathcal{H}_{200}\setminus\{1\}$ is $(p^m-1)/2$ and the cardinality of the inverse image in E_{00} of $1\in\mathcal{H}_{200}$ is $(p^m-3)/4$.

Now, consider the relationship of the elements in $\mathcal{H}_{100}$ and $\mathcal{H}_{200}$. Assume that there exist $x_1,x_2\in E_{00}$ such that $h_1(x_1)=h_2(x_2)$. Let $t_1=\theta^{-1}(x_1)$ and $t_2=\theta^{-1}(x_2)$. Then, from (29), we have $(p^m+1)t_1\equiv\pm(p^m-1)t_2 \bmod p^n-1$, which can be rewritten as

$$\frac{p^m+1}{2}t_1\equiv\pm\frac{p^m-1}{2}t_2 \bmod \frac{p^n-1}{2}. \tag{31}$$

Since $\gcd((p^m+1)/2,(p^n-1)/2)=1$, $(p^m+1)/2$ has an inverse modulo $(p^n-1)/2$. Hence for any $t_2\in\mathcal{T}_1$ which is not divisible by $(p^n-1)/(p^m-1)$, there exists $t_1\in\mathcal{T}_1$ satisfying (31). Since t_2 which is divided by $(p^n-1)/(p^m-1)$ gives $h_2(x)=1$, we conclude that $1\in\mathcal{H}_{200}$ and $\mathcal{H}_{100}\supset(\mathcal{H}_{200}\setminus\{1\})$.

Since $h_4(x)=-h_1(x)$ and $h_3(x)=-h_2(x)$, $h_4(x)|_{E_{00}}$ has the same mapping property with $h_1(x)|_{E_{00}}$, and $h_3(x)|_{E_{00}}$ has the same mapping property with $h_2(x)|_{E_{00}}$. Furthermore, it is easy to check that $\mathcal{H}_{400}=-\mathcal{H}_{100}$, $\mathcal{H}_{300}=-\mathcal{H}_{200}$, and $\mathcal{H}_{400}\supset(\mathcal{H}_{300}\setminus\{-1\})$.

Table 3
Related PN and APN functions in $f(x) = x^d$.

Researcher	p, n, and k	d	Class
Coulter [6]	$p = 3$ and k is odd	$d = (3^k + 1)/2$, where $\gcd(n.k) = 1$	PN
Helleseth [7]	$p = 5$	$d = (5^k + 1)/2$, where $\gcd(2n, k) = 1$	APN
Helleseth [7]	$p = 3$ and n is odd $p^n > 7$	$d = (p^n + 1)/4 + (p^n - 1)/2$	APN

It should also be checked that $\mathcal{H}_{100}$ cannot include both y and $-y$. Assume that there exist $x_1, x_2 \in E_{00}$ such that $h_1(x_1) = -h_1(x_2)$. From (29), we have $(p^m + 1)t_1 \equiv \pm(p^m + 1)t_2 + (p^n - 1)/2 \bmod p^n - 1$, which can be rewritten as

$$\left(p^m + 1\right)(t_1 \pm t_2) \equiv \frac{p^n - 1}{2} \bmod p^n - 1. \tag{32}$$

Since $\gcd(p^m + 1, p^n - 1) = 2$ does not divide $(p^n - 1)/2$, (32) cannot be satisfied. Hence we conclude that there exist no $x_1, x_2 \in E_{00}$ such that $h_1(x_1) = -h_1(x_2)$. Consequently, we conclude that $\mathcal{H}_{100} \cap \mathcal{H}_{400} = \emptyset$.

So far, we have investigated the mapping property of $h_i(x)|_{E_{00}}$ and the relationship among the elements in $\mathcal{H}_{i00}$, $1 \leqslant i \leqslant 4$.

Now, we will calculate that $N_f(1, b) = \lambda_1(b) + \lambda_2(b) + \lambda_3(b) + \lambda_4(b)$ for square $b \in \mathbb{F}_{p^n}^*$, which is the sum of the cardinalities of the inverse images in E_{00} of the square element in $\mathbb{F}_{p^n}$, $b^{-(p^m+1)/2}$ in (23). Note that there are $(p^n - 3)/4$ squares in $\mathcal{H}_{100} \cup \mathcal{H}_{400}$ because $\mathcal{H}_{100} \cap \mathcal{H}_{400} = \emptyset$ and $\mathcal{H}_{100} = -\mathcal{H}_{400}$. Since $\mathcal{H}_{100} \supset (\mathcal{H}_{200} \setminus \{1\})$, $\mathcal{H}_{400} \supset (\mathcal{H}_{300} \setminus \{-1\})$, and $\mathcal{H}_{200} = -\mathcal{H}_{300}$, there are $(p^n - p^m)/(2(p^m - 1))$ squares in $(\mathcal{H}_{200} \setminus \{1\}) \cup \mathcal{H}_{300}$, which are also included in $\mathcal{H}_{100} \cup \mathcal{H}_{400}$. We can regard each square in $\mathcal{H}_{100} \cup \mathcal{H}_{200} \cup \mathcal{H}_{300} \cup \mathcal{H}_{400}$ as $b^{-(p^m+1)/2}$ in (23). From Lemma 11, it is easy to check that for each square c in $(\mathcal{H}_{200} \setminus \{1\}) \cup \mathcal{H}_{300}$, $N_f(1, \delta) = (p^m + 1)/2$ and for each square c in $(\mathcal{H}_{100} \cup \mathcal{H}_{400}) \setminus (\mathcal{H}_{200} \cup \mathcal{H}_{300})$, $N_f(1, \delta) = 1$, where δ is a square in $\mathbb{F}_{p^n}$ such that $\delta^{-(p^m+1)/2} = c$. For $b = 1$, from Lemma 11, $N_f(1, b) = (p^m - 3)/4 + 1 = (p^m + 1)/4$. Let n_i denote the number of $b \in \mathbb{F}_{p^n}$, which are squares in $\mathbb{F}_{p^n}$, such that $N_f(1, b) = i$. Then, $n_{(p^m+1)/2} = (p^n - p^m)/(2(p^m - 1))$, $n_{(p^m+1)/4} = 1$, $n_1 = (p^n - 3)/4 - (p^n - p^m)/(2(p^m - 1))$, and $n_0 = (p^n - 1)/2 - n_{(p^m+1)/2} - n_1$.

Consider the case when $b \in C_1$. From (29) and (30), note that $h_1(x)|_{E_{00}} = h_1(x)|_{E_{11}}$, $h_4(x)|_{E_{00}} = h_4(x)|_{E_{11}}$, $h_2(x)|_{E_{00}} = h_3(x)|_{E_{11}}$, and $h_3(x)|_{E_{00}} = h_2(x)|_{E_{11}}$. Since t varies over $\mathcal{T}_1$ for both $x \in E_{00}$ and $x \in E_{11}$, they have the same mapping property, which means that for $b \in C_1$, the distribution of $N_f(1, b)$ is the same as the case when $b \in C_0$. Taking that $N_f(1, b) = 1$ when $b = 0$ into account, it is derived that $\omega_{(p^m+1)/2} = 2n_{(p^m+1)/2} = (p^n - p^m)/(p^m - 1)$, $\omega_{(p^m+1)/4} = 2n_{(p^m+1)/4} = 2$, $\omega_1 = 2n_1 + 1 = (p^n - 1)/2 - (p^n - p^m)/(p^m - 1)$, and $\omega_0 = p^n - \omega_{(p^m+1)/2} - \omega_{(p^m+1)/4} - \omega_1$. □

Corollary 2. *For an odd prime p such that $p \equiv 3 \bmod 4$, odd n, $m|n$, and $d = (p^n + 1)/(p^m + 1) + (p^n - 1)/2$, Δ_f of the function $f(x) = x^d$ in $\mathbb{F}_{p^n}$ is given as $\Delta_f = (p^m + 1)/2$.*

From Sections 3 and 4, we can explain the previously known PN and APN functions as in Table 3. Moreover new power functions which are differential 4-uniform and 6-uniform are also introduced in the following corollaries.

Corollary 3. *Let $d = (p^n + 1)/8 + (p^n - 1)/2$. Then x^d defined on $\mathbb{F}_{p^n}$ is differentially 4-uniform for $p = 7$ and odd n.*

Corollary 4. *Let $d = (p^n + 1)/12 + (p^n - 1)/2$. Then x^d defined on $\mathbb{F}_{p^n}$ is differentially 6-uniform for $p = 11$ and odd n.*

5. Conclusion

In this paper, the differential spectrum of the two power functions $x^{\frac{p^k+1}{2}}$ and $x^{\frac{p^n+1}{p^m+1}+\frac{p^n-1}{2}}$ in $\mathbb{F}_{p^n}$ are derived. The result can be used to determine Δ_f of the two power functions. We believe that it is the first result to compute the differential spectrum of power functions in odd prime characteristic. Some existing PN and APN functions are explained from our results. Two new power functions in $\mathbb{F}_{p^n}$ which are differentially 4-uniform and 6-uniform are also found.

Appendix A

Proof of Lemma 10. *Case* 1). Relationship between $\mathcal{I}_{00}$ and $\mathcal{I}_{10}$.

Note that $g = \gcd(2n, k)$. Assume that there exist $x_1 \in E_{00}$ and $x_2 \in E_{10}$ such that $D_f(x_1) = D_f(x_2)$. Let $t_1 = \theta^{-1}(x_1)$ and $t_2 = \theta^{-1}(x_2)$. From Lemma 3, we have

$$\alpha^{(p^k-1)t_1} + \alpha^{-(p^k-1)t_1} = \delta^{2(p^k-1)t_2} + \delta^{-2(p^k-1)t_2}. \tag{33}$$

Since $\alpha = \beta^{p^n+1}$ and $\delta = \beta^{(p^n-1)/2}$, (33) is satisfied if and only if

$$\left[\left(p^n+1\right)t_1 \pm \left(p^n-1\right)t_2\right]\left(p^k-1\right) \equiv 0 \bmod \left(p^{2n}-1\right). \tag{34}$$

Then (34) can be rewritten as

$$\left(p^n+1\right)t_1 \pm \left(p^n-1\right)t_2 \equiv 0 \bmod \frac{p^{2n}-1}{p^g-1} \tag{35}$$

where $\gcd(p^k-1, p^{2n}-1) = p^g - 1$.

Note that

$$\gcd\left(\frac{p^{2n}-1}{p^g-1}, p^n+1\right) = \begin{cases} p^n+1, & \text{if } g = e \\ \frac{p^n+1}{p^e+1}, & \text{if } g = 2e. \end{cases} \tag{36}$$

Consider the case when $g = e$, i.e., k/e is odd. For the solvability of (34), $\pm(p^n-1)t_2$ should be divided by p^n+1. Since $\gcd(p^n+1, p^n-1) = 2$, t_2 should be divided by $(p^n+1)/2$. Since t_2 varies over $[1, (p^n-3)/4]$ for $p^n \equiv 3 \bmod 4$ and $[1, (p^n-1)/4]$ for $p^n \equiv 1 \bmod 4$, t_2 cannot be divided by $(p^n+1)/2$. Hence we conclude that $\mathcal{I}_{00} \cap \mathcal{I}_{10} = \emptyset$ for odd k/e.

Next, consider the case when $g = 2e$, i.e., k/e is even. From (35), $(p^n+1)t_1$ should be divided by $\gcd(p^n-1, (p^{2n}-1)/(p^{2e}-1)) = (p^n-1)/(p^e-1)$. Since $\gcd((p^n-1)/(p^e-1), p^n+1) = 1$, t_1 should be divided by $(p^n-1)/(p^e-1)$, which means that $\mathcal{I}_{00} \cap \mathcal{I}_{10} = \{1\}$ for even k/e.

Case 2). Relationship between $\mathcal{I}_{11}$ and $\mathcal{I}_{10}$.

For the case when $p^n \equiv 3 \bmod 4$ and $p^k \equiv 1 \bmod 4$, we already proved that $\mathcal{I}_{00} = \mathcal{I}_{11}$. Since $g = 2e$, i.e., k/e is even, in the case, we conclude that $\mathcal{I}_{11} \cap \mathcal{I}_{10} = \{1\}$ for even k/e.

Consider the case when $p^n \equiv 3 \bmod 4$ and $p^k \equiv 3 \bmod 4$. Note that $g = e$, i.e., k/e is odd in the case. We can prove this case similar to Case 1). Assume that there exist $x_1 \in E_{11}$ and $x_2 \in E_{10}$ such that $D_f(x_1) = D_f(x_2)$. Let $t_1 = \theta^{-1}(x_1)$ and $t_2 = \theta^{-1}(x_2)$. From Lemma 3, we have

$$\left(p^k-1\right)\left[\left(p^n+1\right)t_1 \pm \left(p^n-1\right)t_2\right] \equiv \frac{p^{2n}-1}{2} \bmod \left(p^{2n}-1\right). \tag{37}$$

Then (37) can be rewritten as

$$\left(p^n+1\right)t_1 \pm \left(p^n-1\right)t_2 \equiv \frac{p^{2n}-1}{2(p^e-1)} \bmod \frac{p^{2n}-1}{p^e-1} \tag{38}$$

where $\gcd(p^k-1,(p^{2n}-1)/2)=p^e-1$. For the solvability of (38), $\pm(p^n-1)t_2$ should be divided by $(p^n+1)/2$. Since $\gcd((p^n+1)/2,p^n-1)=2$, t_2 should be divided by $(p^n+1)/4$. Since t_2 varies over $[1,(p^n-3)/4]$ for $p^n\equiv 3 \bmod 4$, t_2 cannot be divided by $(p^n+1)/4$. Hence we conclude that $\mathcal{I}_{00}\cap\mathcal{I}_{10}=\emptyset$ for odd k/e.

Next, consider the case when $p^n\equiv 1 \bmod 4$ and $p^k\equiv 1 \bmod 4$. Assume that there exist $x_1\in E_{11}$ and $x_2\in E_{10}$ such that $D_f(x_1)=D_f(x_2)$. From Lemma 3 and by setting $\gamma=-\alpha$, we have

$$\left(p^k-1\right)\left[\left(p^n+1\right)t_1\pm\left(p^n-1\right)t_2\right]\equiv-\frac{p^k-1}{2}\left(p^n+1\right)\bmod\left(p^{2n}-1\right). \tag{39}$$

Note that g can be equal to either e or $2e$ in this case. For the case when $g=e$, i.e., k/e is odd, (39) can be rewritten as

$$\frac{p^k-1}{p^e-1}\left[\left(p^n+1\right)t_1\pm\left(p^n-1\right)t_2\right]\equiv-\frac{p^n+1}{2}\cdot\frac{p^k-1}{p^e-1}\bmod\frac{p^{2n}-1}{p^e-1}. \tag{40}$$

From (40), $(p^n-1)t_2$ should be divided by $(p^n+1)/2$. Since $\gcd(p^n-1,(p^n+1)/2)=1$, t_2 should be divided by $(p^n+1)/2$. Note that t_2 varies over $[1,(p^n-1)/4]$. We conclude that $\mathcal{I}_{11}\cap\mathcal{I}_{10}=\emptyset$ for odd k/e.

For the case when $g=2e$, i.e., k/e is even, (39) can be rewritten as

$$\frac{p^k-1}{p^g-1}\left[\left(p^n+1\right)t_1\pm\left(p^n-1\right)t_2\right]\equiv-\frac{p^n+1}{2}\cdot\frac{p^k-1}{p^g-1}\bmod\frac{p^{2n}-1}{p^g-1}. \tag{41}$$

From $\gcd((p^{2n}-1)/(p^g-1),(p^n+1)/2)=(p^n+1)/(p^e+1)$ and (41), $(p^n-1)t_2$ should be divided by $(p^n+1)/(p^e+1)$. Since $\gcd(p^n-1,(p^n+1)/(p^e+1))=1$, t_2 should be divided by $(p^n+1)/(p^e+1)$. From Lemma 4, we have $p^e+1\mid p^k-1$. Hence t_2 which is divided by $(p^n+1)/(p^e+1)$ gives $D_f(x)=1$, which means that $\mathcal{I}_{11}\cap\mathcal{I}_{10}=\{1\}$ for even k/e.

The case when $p^n\equiv 1 \bmod 4$ and $p^k\equiv 3 \bmod 4$ can be proved similarly.

Case 3). Relationship between $\mathcal{I}_{00}$ and $\mathcal{I}_{01}$.

We already proved that $\mathcal{I}_{10}\cap\mathcal{I}_{01}=\emptyset$ for $p^e\equiv 3 \bmod 4$ and odd k/e and $\mathcal{I}_{10}=\mathcal{I}_{01}$, otherwise. Hence we only need to consider the case when $p^e\equiv 3 \bmod 4$ and odd k/e in Case 3) and Case 4). Note that $p^k\equiv 3 \bmod 4$ in this case.

First, consider the relationship between $\mathcal{I}_{00}$ and $\mathcal{I}_{01}$. Assume that there exist $x_1\in E_{00}$ and $x_2\in E_{01}$ such that $D_f(x_1)=D_f(x_2)$. Let $t_1=\theta^{-1}(x_1)$ and $t_2=\theta^{-1}(x_2)$. Again, we have

$$\left(p^k-1\right)\left[\left(p^n+1\right)t_1\pm\left(\frac{p^n-1}{2}+\left(p^n-1\right)t_2\right)\right]\equiv 0 \bmod\left(p^{2n}-1\right), \tag{42}$$

which can be rewritten as

$$\frac{p^k-1}{p^e-1}\left[\left(p^n+1\right)t_1\pm\left(\frac{p^n-1}{2}+\left(p^n-1\right)t_2\right)\right]\equiv 0 \bmod\frac{p^{2n}-1}{p^e-1}. \tag{43}$$

For the solvability of (43), $(p^n-1)/2\pm(p^n-1)t_2$ should be divided by p^n+1, which is given as

$$\frac{p^n-1}{2}(1\pm 2t_2)\equiv 0 \bmod\left(p^n+1\right). \tag{44}$$

For $p^n\equiv 3 \bmod 4$, the left-hand side is odd, while the right-hand side is even, which is a contradiction. For $p^n\equiv 1 \bmod 4$, since $\gcd((p^n-1)/2,p^n+1)=2$, $1\pm 2t_2$ should be divided by $(p^n+1)/2$.

Assume that $1 + 2t_2 = (p^n + 1)/2$. Then t_2 should be $(p^n - 1)/4$. However, since t_2 varies over $[0, (p^n - 5)/4]$, it is impossible. Therefore, we conclude that $\mathcal{I}_{00} \cap \mathcal{I}_{01} = \emptyset$.

Case 4). Relationship between $\mathcal{I}_{11}$, and $\mathcal{I}_{01}$.

Next, consider the relationship between $\mathcal{I}_{11}$ and $\mathcal{I}_{01}$. Assume that there exist $x_1 \in E_{11}$ and $x_2 \in E_{01}$ such that $D_f(x_1) = D_f(x_2)$. For the case when $p^n \equiv 3 \bmod 4$, by setting $\gamma = -1$, we have

$$\left(p^k - 1\right)\left[\left(p^n + 1\right)t_1 \pm \left(\frac{p^n - 1}{2} + \left(p^n - 1\right)t_2\right)\right] \equiv \frac{p^{2n} - 1}{2} \bmod \left(p^{2n} - 1\right), \tag{45}$$

which can be rewritten as

$$\frac{p^k - 1}{p^e - 1}\left[\left(p^n + 1\right)t_1 \pm \left(\frac{p^n - 1}{2} + \left(p^n - 1\right)t_2\right)\right] \equiv \frac{p^n + 1}{2} \cdot \frac{p^n - 1}{p^e - 1} \bmod \frac{p^{2n} - 1}{p^e - 1}. \tag{46}$$

For the solvability of (46), $(p^n - 1)(1 \pm 2(p^n - 1)t_2)/2$ should be divided by $(p^n + 1)/2$. Since $\gcd((p^n - 1)/2, (p^n + 1)/2) = 1$, $1 \pm 2(p^n - 1)t_2$ should be divided by $(p^n + 1)/2$. Since $(p^n + 1)/2$ is even and $1 \pm 2(p^n - 1)t_2$ is odd, it is a contradiction. Hence we conclude that $\mathcal{I}_{00} \cap \mathcal{I}_{01} = \emptyset$.

For the case when $p^n \equiv 1 \bmod 4$, $(p^n - 1)/2(1 \pm 2t_2)$ should be divided by $(p^n + 1)/2$. Hence $1 \pm 2t_2$ should be divided by $(p^n + 1)/2$. Assume that $1 + 2t_2$ is divided by $(p^n + 1)/2$. Then t_2 should be equal to $(p^n - 1)/4$, which is a contradiction because $t_2 \leqslant (p^n - 5)/4$. Therefore, $\mathcal{I}_{00} \cap \mathcal{I}_{01} = \emptyset$. □

References

[1] L.E. Dickson, Linear Groups with an Exposition of the Galois Field Theory, Dover Publications, New York, 1958.
[2] K. Nyberg, Differentially uniform mappings for cryptography, in: Advances in Cryptography—EUROCRYPTO'93, in: Lecture Notes in Comput. Sci., vol. 765, Springer-Verlag, New York, 1994, pp. 55–64.
[3] C. Blondeau, A. Canteaut, P. Charpin, Differential properties of power functions, Int. J. Inf. Coding Theory 1 (2) (2010) 149–170.
[4] C. Blondeau, A. Canteaut, P. Charpin, Differential properties of power functions, in: Proc. IEEE Int. Symp. Inf. Theory (ISIT 2010), Austin, Texas, Jun. 2010, pp. 2478–2482.
[5] C. Blondeau, A. Canteaut, P. Charpin, Differential properties of $x \mapsto x^{2^t-1}$, IEEE Trans. Inform. Theory 57 (12) (2011) 8127–8137.
[6] R.S. Coulter, R.W. Matthews, Planar functions and planes of Lenz–Barlotti class, II, Des. Codes Cryptogr. 10 (2) (1997) 167–184.
[7] T. Helleseth, C. Rong, D. Sandberg, New families of almost perfect nonlinear power mapping, IEEE Trans. Inform. Theory 45 (2) (1999) 475–485.
[8] H. Dobbertin, D. Mills, E.N. Muller, A.P. Willems, APN functions in odd characteristic, Discrete Math. 267 (2003) 95–112.
[9] T. Helleseth, D. Sandberg, Some power mappings with low differential uniformity, Appl. Algebra Engrg. Comm. Comput. 8 (1997) 363–370.
[10] Z. Zha, X. Wang, Power functions with low uniformity on odd characteristic finite fields, Sci. China Math. 53 (8) (2010) 1931–1940.
[11] Z. Zha, X. Wang, Almost perfect nonlinear power functions in odd characteristic, IEEE Trans. Inform. Theory 57 (7) (2011) 4826–4832.
[12] G.J. Ness, T. Helleseth, A new family of ternary almost perfect nonlinear mappings, IEEE Trans. Inform. Theory 53 (7) (2007) 2581–2586.
[13] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case, IEEE Trans. Inform. Theory 45 (4) (1999) 1271–1275.
[14] T.P. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy, On almost perfect nonlinear functions over F_{2^n}, IEEE Trans. Inform. Theory 52 (9) (2006) 4160–4170.
[15] Y. Edel, G. Kyureghyan, A. Pott, A new APN functions which is not equivalent to a power mapping, IEEE Trans. Inform. Theory 52 (2) (2006) 744–747.
[16] C. Bracken, G. Leander, A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree, Finite Fields Appl. 16 (4) (2010) 231–242.
[17] T. Storer, Cyclotomy and Difference Sets, Lect. Adv. Math., Markham, Chicago, IL, 1967.
[18] S.E. Payne, Greatest common divisors of $a^m \pm 1$ and $a^n \pm 1$, http://math.ucdenver.edu/~spayne/classnotes/rgcd.ps.