On the differential spectrum of a differentially 3-uniform power function

Tingting Pang, Nian Li and Xiangyong Zeng [*]

Abstract: In this paper, we investigate the cardinality, denoted by $(j_1, j_2, j_3, j_4)_2$, of the intersection of $(\mathcal{C}_{j_1}^{(2)} - 1) \cap (\mathcal{C}_{j_2}^{(2)} - 2) \cap (\mathcal{C}_{j_3}^{(2)} - 3) \cap (\mathcal{C}_{j_4}^{(2)} - 4)$ for $j_1, j_2, j_3, j_4 \in \{0, 1\}$, where $\mathcal{C}_0^{(2)}, \mathcal{C}_1^{(2)}$ are the cyclotomic classes of order two over the finite field $\mathbb{F}_{p^n}$, p is an odd prime and n is a positive integer. By making most use of the results on cyclotomic classes of orders two and four as well as the cardinality of the intersection $(\mathcal{C}_{i_1}^{(2)} - 1) \cap (\mathcal{C}_{i_2}^{(2)} - 2) \cap (\mathcal{C}_{i_3}^{(2)} - 3)$, we compute the values of $(j_1, j_2, j_3, j_4)_2$ in the case of $p = 5$, where $i_1, i_2, i_3 \in \{0, 1\}$. As a consequence, the power function $x^{\frac{5^n-1}{2}+2}$ over $\mathbb{F}_{5^n}$ is shown to be differentially 3-uniform and its differential spectrum is also completely determined.

Keywords: Power function, differential spectrum, cyclotomic number.

1 Introduction

Substitution box (S-box for short) is an important nonlinear component of symmetric cryptosystems. The functions used to design S-boxes should have good cryptographic properties in order to resist various kinds of cryptanalytic attacks. Differential attack is one of the most fundamental cryptanalytic approaches targeting symmetric key primitives and the first statistical attack for breaking iterated block ciphers [1].

The differential uniformity of S-boxes, which was introduced by Nyberg in [10], can be used to measure the ability of a given function to resist the differential attack. Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements and $\mathbb{F}_{p^n}^*$ denote its multiplicative group, where p is a prime and n is a positive integer. For a function $F(x)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$, $a \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_{p^n}$, define

$$\delta_F(a, b) = \#\{x \in \mathbb{F}_{p^n} \mid F(x + a) - F(x) = b\}.$$

[*] Tingting Pang is with the School of Mathematics, Shandong University, Jinan, 250100, China. N. Li and X. Zeng are with the Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan, 430062, China. Email: ttingpang@163.com, nian.li@hubu.edu.cn, xzeng@hubu.edu.cn

The differential uniformity of $F(x)$, denoted by Δ_F, is defined as

$$\Delta_F = \max\{\delta_F(a,b) \mid a \in \mathbb{F}_{p^n}^*,\ b \in \mathbb{F}_{p^n}\}.$$

If $\Delta_F = \delta$, then $F(x)$ is called the differentially δ-uniform. A function is called perfect nonlinear (PN for short) if $\Delta_F = 1$ and almost perfect nonlinear (APN for short) if $\Delta_F = 2$.

Power functions with low differential uniformity have been extensively studied in the past decades due to their strong resistance to differential attacks and low implementation cost in hardware. For a power function $F(x) = x^d$, it can be readily verified that $\delta_F(a,b) = \delta_F(1, \frac{b}{a^d})$ for any $a \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_{p^n}$. In order to further investigate the differential properties of power functions, Blondeau et al. defined the differential spectrum of $F(x) = x^d$ as the multiset

$$\mathbb{S} = \{w_0, w_1, \cdots, w_{\Delta_F}\},$$

where $w_i = \#\{b \in \mathbb{F}_{p^n} \mid \delta_F(1,b) = i\}$ and $0 \le i \le \Delta_F$ [2]. It is an interesting topic to obtain the differential spectrum of power functions with low differential uniformity which is useful to analyse the resistance of the cipher to differential attacks. Hence, the study of the differential spectrum of power functions has attracted a lot of attention. However, it is usually a hard work to obtain the differential spectrum for a given power function, and therefore there are only a few classes of power functions with known differential spectrum, see Table 1 for odd characteristics.

Table 1: Power functions $F(x) = x^d$ over $\mathbb{F}_{p^n}$ (p is odd) with known differential spectrum

d	Conditions	Δ_F	References
$2 \cdot 3^{\frac{n-1}{2}} + 1$	$p = 3$, n is odd	4	[5]
$\frac{p^k+1}{2}$	$\gcd(n,k) = e$	$\frac{p^e-1}{2}$ or $p^e + 1$	[4]
$\frac{p^n+1}{p^m+1} + \frac{p^n-1}{2}$	$p \equiv 3 \pmod 4$, $m \mid n$, n is odd	$\frac{p^m+1}{2}$	[4]
$p^{2k} - p^k + 1$	$\gcd(n,k) = e$, $\frac{n}{e}$ is odd	$p^e + 1$	[8,16]
$p^n - 3$	any n	≤ 5	[13,15]
$p^m + 2$	$p > 3$, $n = 2m$	4	[9]
$\frac{5^n-3}{2}$	$p = 5$	4 or 5	[14]
$\frac{5^n-1}{2} + 2$	$p = 5$	3	This paper

Among the study of power functions with low differential uniformity, the differential uniformity of $F(x) = \frac{p^n-1}{2} + 2$ was discussed in [6].

Theorem 1. ([6, Theorem 3]) *Let p be an odd prime and $F(x) = x^d$, where $d = \frac{p^n-1}{2} + 2$. Then* *the differential uniformity of F satisfies*

$$\Delta_F \leq \begin{cases} 1, & \textit{if } p=3 \textit{ and } n \textit{ is even;} \\ 3, & \textit{if } p\neq 3 \textit{ and } p^n \equiv 1 \pmod 4; \\ 4, & \textit{otherwise.} \end{cases}$$

Clearly, $F(x)=x^{\frac{3^n-1}{2}+2}$ is affine equivalent to $x^{\frac{3^{n-1}+1}{2}}$ due to $\gcd(3^{n-1},3^n-1)=1$. Then the differential spectrum of $x^{\frac{3^n-1}{2}+2}$ has been determined in [4,7]. To the best of our knowledge, except for the case of $p=3$, the differential spectrum of $x^{\frac{p^n-1}{2}+2}$ over $\mathbb{F}_{p^n}$ has not been discussed in other characteristics.

In this paper, we aim to determine the differential spectrum of $x^{\frac{p^n-1}{2}+2}$ for $p=5$. To solve this problem, we study the cardinality, denoted by $(j_1,j_2,j_3,j_4)_2$, of the intersection of $(\mathcal{C}_{j_1}^{(2)}-1)\cap(\mathcal{C}_{j_2}^{(2)}-2)\cap(\mathcal{C}_{j_3}^{(2)}-3)\cap(\mathcal{C}_{j_4}^{(2)}-4)$ for $j_1,j_2,j_3,j_4\in\{0,1\}$, where $\mathcal{C}_0^{(2)},\mathcal{C}_1^{(2)}$ are the cyclotomic classes of order two over $\mathbb{F}_{p^n}$. Consequently, the values of $(j_1,j_2,j_3,j_4)_2$ for $p=5$ are determined by means of the known results on the cyclotomic number of order four and the cardinality of the intersection of $(\mathcal{C}_{i_1}^{(2)}-1)\cap(\mathcal{C}_{i_2}^{(2)}-2)\cap(\mathcal{C}_{i_3}^{(2)}-3)$, where $i_1,i_2,i_3\in\{0,1\}$. With the help of certain techniques over finite fields, we completely determined the differential spectrum of $x^{\frac{5^n-1}{2}+2}$ over $\mathbb{F}_{5^n}$.

2 Preliminaries

In this section, some basic results on the cyclotomic class and cyclotomic number of order four over finite fields are given. Let p be an odd prime, n be a positive integer, and η denote the quadratic multiplicative character over $\mathbb{F}_{p^n}$, i.e., $\eta(x)=1$ if x is a square, $\eta(0)=0$ if $x=0$ and $\eta(x)=-1$ if x is a nonsquare. It is well known that $\eta(-1)=1$ if and only if $p^n\equiv 1 \pmod 4$ and $\eta(2)=1$ if and only if $p^n\equiv \pm1 \pmod 8$.

Let e and h be positive integers such that $eh+1=p^n$ and α be a primitive element of $\mathbb{F}_{p^n}$. The cyclotomic class $\mathcal{C}_i^{(e)}$ in $\mathbb{F}_{p^n}$ is defined as

$$\mathcal{C}_i^{(e)}=\{\alpha^{es+i}\,|\,s=0,1,\cdots,h-1\},$$

where $0\leq i\leq e-1$. The cyclotomic number $(i,j)_e$ is defined as the cardinality of the set

$$\mathcal{C}_{i,j}^{(e)}=\mathcal{C}_i^{(e)}\cap(\mathcal{C}_j^{(e)}-1)=\{x\in\mathbb{F}_{p^n}\,|\,x\in\mathcal{C}_i^{(e)} \text{ and } x+1\in\mathcal{C}_j^{(e)}\},$$

where $0\leq i,j\leq e-1$, the cyclotomic matrix $M^{(e)}$ is defined as the matrix whose entry in position $(i+1,j+1)$ is the constant $(i,j)_e$.

The cyclotomic matrix $M^{(4)}$ is given as below, which will be useful for proving our results.

Lemma 1. ([12]) *Let $e = 4$, s and t be integers such that $p^n = s^2 + 4t^2$ and $s \equiv 1 \pmod 4$. Then $p^n \equiv 1 \pmod 4$ and we have the following conditions.*

(i) If h is even, i.e., $p^n \equiv 1 \pmod 8$, then

$$M^{(4)} = \begin{pmatrix} A & B & C & D \\ B & D & E & E \\ C & E & C & E \\ D & E & E & B \end{pmatrix},$$

where $16A = p^n - 11 - 6s$, $16B = p^n - 3 + 2s + 8t$, $16C = p^n - 3 + 2s$, $16D = p^n - 3 + 2s - 8t$ and $16E = p^n + 1 - 2s$.

(ii) If h is odd, i.e., $p^n \equiv 5 \pmod 8$, then

$$M^{(4)} = \begin{pmatrix} A & B & C & D \\ E & E & D & B \\ A & E & A & E \\ E & D & B & E \end{pmatrix},$$

where $16A = p^n - 7 + 2s$, $16B = p^n + 1 + 2s - 8t$, $16C = p^n + 1 - 6s$, $16D = p^n + 1 + 2s + 8t$ and $16E = p^n - 3 - 2s$.

3 On the intersection of some particular cyclotomic classes

Let $(i_1, i_2, i_3)_2$ be defined as the cardinality of the intersection $(\mathcal{C}_{i_1}^{(2)} - 1) \cap (\mathcal{C}_{i_2}^{(2)} - 2) \cap (\mathcal{C}_{i_3}^{(2)} - 3)$, and $(j_1, j_2, j_3, j_4)_2$ denote the cardinality of the intersection $(\mathcal{C}_{j_1}^{(2)} - 1) \cap (\mathcal{C}_{j_2}^{(2)} - 2) \cap (\mathcal{C}_{j_3}^{(2)} - 3) \cap (\mathcal{C}_{j_4}^{(2)} - 4)$, where $i_1, i_2, i_3, j_1, j_2, j_3, j_4 \in \{0, 1\}$. Clearly, we have

$$\begin{aligned} (i_1, i_2, i_3)_2 &= \# \left\{ x \in \mathbb{F}_{p^n} \mid \eta(x + t) = (-1)^{i_t} \text{ for } t = 1, 2, 3 \right\}, \\ (j_1, j_2, j_3, j_4)_2 &= \# \left\{ x \in \mathbb{F}_{p^n} \mid \eta(x + t) = (-1)^{j_t} \text{ for } t = 1, 2, 3, 4 \right\}. \end{aligned}$$

The values of $(i_1, i_2, i_3)_2$ for $i_1, i_2, i_3 \in \{0, 1\}$ are given in the following lemma.

Lemma 2. ([11]) *Let p be an odd prime, n be a positive integer. When $p^n \equiv 1 \pmod 4$, let $p^n = s^2 + 4t^2$, where s and t are integers such that $s \equiv 1 \pmod 4$.*

(i) If $p^n \equiv -1 \pmod 8$, then

$$(0, 0, 0)_2 = (1, 0, 0)_2 = (1, 1, 0)_2 = (1, 1, 1)_2 = \frac{p^n - 7}{8},$$

$$(0, 0, 1)_2 = (0, 1, 0)_2 = (0, 1, 1)_2 = (1, 0, 1)_2 = \frac{p^n + 1}{8}.$$

(ii) If $p^n \equiv 1 \pmod 8$*, then*

$$(0,0,1)_2 = (0,1,0)_2 = (1,0,0)_2 = (1,1,1)_2 = \frac{p^n + 2s - 3}{8},$$

$$(0,1,1)_2 = (1,0,1)_2 = (1,1,0)_2 = (0,0,0)_2 + 2 = \frac{p^n - 2s + 1}{8}.$$

(iii) If $p^n \equiv -3 \,(\bmod 8)$*, then*

$$(0,0,1)_2 = (0,1,0)_2 = (1,0,0)_2 = (1,1,1)_2 = \frac{p^n - 2s - 3}{8},$$

$$(0,1,1)_2 = (1,1,0)_2 = (1,0,1)_2 + 1 = (0,0,0)_2 + 1 = \frac{p^n + 2s + 1}{8}.$$

(iv) If $p^n \equiv 3 \pmod 8$*, then* $(i_1, i_2, i_3)_2 = \frac{p^n-3}{8}$ *for all* $i_1, i_2, i_3 \in \{0, 1\}$*.*

According to Lemma 2 and the cyclotomic number of order four, we can determine the values of $(j_1, j_2, j_3, j_4)_2$ in the case of $p = 5$ as follows.

Theorem 2. *Let* $p = 5$*,* s *and* t *be integers such that* $s \equiv 1 \pmod 4$ *and* $p^n = s^2 + 4t^2$*. Then we have the following results.*

(i) If n *is even, then* $(0,0,0,0)_2 = \frac{p^n-10s-39}{16}$*,*

$$(0,0,0,1)_2 = (0,0,1,0)_2 = (0,1,0,0)_2 = (1,0,0,0)_2 = (1,1,1,1)_2 = \frac{p^n + 6s - 7}{16}$$

and $(j_1, j_2, j_3, j_4)_2 = \frac{p^n-2s+1}{16}$ *otherwise.*

(ii) If n *is odd, then* $(0,1,1,0)_2 = \frac{p^n+10s+1}{16}$*,*

$$(0,0,1,0)_2 = (0,1,0,0)_2 = (1,0,0,1)_2 = (0,1,1,1)_2 = (1,1,1,0)_2 = \frac{p^n - 6s + 1}{16}$$

and $(j_1, j_2, j_3, j_4)_2 = \frac{p^n+2s-7}{16}$ *otherwise.*

Proof. (i) If $p = 5$ and n is even, then $\eta(-1) = \eta(2) = \eta(3) = 1$. It can be verified that

$$\begin{aligned}
& \#\{x \in \mathbb{F}_{p^n} \mid \eta(x+1) = (-1)^{j_1},\ \eta(x+2) = (-1)^{j_2},\ \eta(x+3) = (-1)^{j_3},\ \eta(x+4) = (-1)^{j_4}\} \\
= \ & \#\{x \in \mathbb{F}_{p^n} \mid \eta(2x+2) = (-1)^{j_1},\ \eta(2x+4) = (-1)^{j_2},\ \eta(2x+1) = (-1)^{j_3},\ \eta(2x+3) = (-1)^{j_4}\} \\
= \ & \#\{x \in \mathbb{F}_{p^n} \mid \eta(3x+3) = (-1)^{j_1},\ \eta(3x+1) = (-1)^{j_2},\ \eta(3x+4) = (-1)^{j_3},\ \eta(3x+2) = (-1)^{j_4}\} \\
= \ & \#\{x \in \mathbb{F}_{p^n} \mid \eta(4x+4) = (-1)^{j_1},\ \eta(4x+3) = (-1)^{j_2},\ \eta(4x+2) = (-1)^{j_3},\ \eta(4x+1) = (-1)^{j_4}\}
\end{aligned}$$

which implies $(j_1, j_2, j_3, j_4)_2 = (j_3, j_1, j_4, j_2)_2 = (j_2, j_4, j_1, j_3)_2 = (j_4, j_3, j_2, j_1)_2$. More precisely, we have $(0,1,1,0)_2 = (1,0,0,1)_2$ and

$$\begin{aligned}
(0,0,0,1)_2 &= (0,0,1,0)_2 = (0,1,0,0)_2 = (1,0,0,0)_2 \\
(0,0,1,1)_2 &= (1,0,1,0)_2 = (0,1,0,1)_2 = (1,1,0,0)_2 \\
(0,1,1,1)_2 &= (1,0,1,1)_2 = (1,1,0,1)_2 = (1,1,1,0)_2.
\end{aligned}$$

Note that $1 \in (\mathcal{C}_0^{(2)}-1)\cap(\mathcal{C}_0^{(2)}-2)\cap(\mathcal{C}_0^{(2)}-3)$ and $-1 \in (\mathcal{C}_0^{(2)}-2)\cap(\mathcal{C}_0^{(2)}-3)\cap(\mathcal{C}_0^{(2)}-4)$. From the definitions of $(i_1,i_2,i_3)_2$ and $(j_1,j_2,j_3,j_4)_2$, we get the following equalities:

$$\begin{aligned}
(0,0,0)_2 &= (0,0,0,0)_2+(0,0,0,1)_2+1=(0,0,0,0)_2+(1,0,0,0)_2+1\\
(0,0,1)_2 &= (0,0,1,0)_2+(0,0,1,1)_2=(0,0,0,1)_2+(1,0,0,1)_2\\
(0,1,1)_2 &= (0,1,1,0)_2+(0,1,1,1)_2=(0,0,1,1)_2+(1,0,1,1)_2\\
(1,1,1)_2 &= (1,1,1,0)_2+(1,1,1,1)_2=(0,1,1,1)_2+(1,1,1,1)_2,
\end{aligned}$$

which indicates $(0,1,1,0)_2=(0,0,1,1)_2$. By Lemma 2 (ii), we have $(0,0,1)_2=(1,1,1)_2=\frac{p^n+2s-3}{8}$ and $(0,1,1)_2=(0,0,0)_2+2=\frac{p^n-2s+1}{8}$. This leads to $(0,0,0,1)_2=(0,1,1,1)_2+\frac{s-1}{2}$.

It can be readily obtained that

$$\begin{aligned}
&\#\{x\in\mathbb{F}_{p^n}\,|\,\eta((x+1)(x+2)(x+3)(x+4))=-1\}\\
=\;&\#\{x\in\mathbb{F}_{p^n}\,|\,\eta(x^4-1)=-1\}\\
=\;&(0,0,0,1)_2+(0,1,0,0)_2+(0,0,1,0)_2+(1,0,0,0)_2\\
&+(0,1,1,1)_2+(1,1,0,1)_2+(1,0,1,1)_2+(1,1,1,0)_2\\
=\;&8(0,1,1,1)_2+2(s-1).
\end{aligned}$$

Let $y=x^4-1$, from $\eta(y)=-1$, we have $y\in\mathcal{C}_{1,0}^{(4)}\cup\mathcal{C}_{3,0}^{(4)}$. By Lemma 1 (i), one has

$$\#\{x\in\mathbb{F}_{p^n}\,|\,\eta(x^4-1)=-1\}=4((1,0)_4+(3,0)_4)=\frac{p^n+2s-3}{2}$$

due to $\gcd(4,5^n-1)=4$. Therefore, one gets $(0,1,1,1)_2=\frac{p^n-2s+1}{16}$ and $(0,0,0,1)_2=\frac{p^n+6s-7}{16}$. This together with the relationships between $(i_1,i_2,i_3)_2$ and $(j_1,j_2,j_3,j_4)_2$, we further have $(0,0,0,0)_2=\frac{p^n-10s-39}{16}$, $(0,0,1,1)_2=\frac{p^n-2s+1}{16}$ and $(1,1,1,1)_2=\frac{p^n+6s-7}{16}$.

(ii) For odd n, we have $\eta(-1)=1$, $\eta(2)=\eta(3)=-1$ and then

$$(j_1,j_2,j_3,j_4)_2=(\epsilon(j_3),\epsilon(j_1),\epsilon(j_4),\epsilon(j_2))_2=(\epsilon(j_2),\epsilon(j_4),\epsilon(j_1),\epsilon(j_3))_2=(j_4,j_3,j_2,j_1)_2,$$

where $\epsilon(0)=1$ and $\epsilon(1)=0$. This implies $(0,0,0,0)_2=(1,1,1,1)_2$ and

$$\begin{aligned}
(0,0,0,1)_2&=(1,1,0,1)_2=(1,0,1,1)_2=(1,0,0,0)_2\\
(0,0,1,0)_2&=(0,1,1,1)_2=(1,1,1,0)_2=(0,1,0,0)_2\\
(0,0,1,1)_2&=(0,1,0,1)_2=(1,0,1,0)_2=(1,1,0,0)_2.
\end{aligned}$$

Obviously, $1\in(\mathcal{C}_1^{(2)}-1)\cap(\mathcal{C}_1^{(2)}-2)\cap(\mathcal{C}_0^{(2)}-3)$ and $-1\in(\mathcal{C}_0^{(2)}-2)\cap(\mathcal{C}_1^{(2)}-3)\cap(\mathcal{C}_1^{(2)}-4)$.

Similarly as the proof of (i), one has

$$\begin{aligned}(0,0,0)_2 &= (0,0,0,0)_2+(0,0,0,1)_2=(0,0,0,0)_2+(1,0,0,0)_2\\(0,0,1)_2 &= (0,0,1,0)_2+(0,0,1,1)_2=(0,0,0,1)_2+(1,0,0,1)_2\\(0,1,1)_2 &= (0,1,1,0)_2+(0,1,1,1)_2=(0,0,1,1)_2+(1,0,1,1)_2+1\\(1,1,1)_2 &= (1,1,1,0)_2+(1,1,1,1)_2=(0,1,1,1)_2+(1,1,1,1)_2.\end{aligned}$$

From Lemma 2 (iii), we have $(0,0,1)_2=(1,1,1)_2=\frac{p^n-2s-3}{8}$ and $(0,1,1)_2=(0,0,0)_2+1=\frac{p^n+2s+1}{8}$, which leads to $(1,0,1,1)_2=(0,0,1,0)_2+\frac{s-1}{2}$.

By $\gcd(4,5^n-1)=4$ and Lemma 1 (ii), we further have

$$\#\{x\in\mathbb{F}_{p^n}\mid\eta(x^4-1)=-1\}=8(0,0,1,0)_2+2(s-1),$$

which equals $4((1,0)_4+(3,0)_4)=\frac{p^n-2s-3}{2}$. Then $(0,0,1,0)_2=\frac{p^n-6s+1}{16}$ and $(1,0,1,1)_2=\frac{p^n+2s-7}{16}$. From the relationships between $(i_1,i_2,i_3)_2$ and $(j_1,j_2,j_3,j_4)_2$, one has $(0,0,0,0)_2=(0,0,1,1)_2=\frac{p^n+2s-7}{16}$, $(1,0,0,1)_2=\frac{p^n-6s+1}{16}$ and $(0,1,1,0)_2=\frac{p^n+10s+1}{16}$.

The proof is completed. □

Remark 1. *(i) Let s and t be integers such that $s\equiv 1\,(\mathrm{mod}\,4)$ and $p^n=s^2+4t^2$, where p is an odd prime and n is a positive integer. From [3] and [12], we know that the above conditions determine s uniquely, and t up to sign. Similarly as the method used in [14], it can be verified that $s=\sum_{k=0}^{\lfloor\frac{n}{2}\rfloor}(-1)^k\binom{n}{2k}2^{2k}$ for $p=5$.*

(ii) Numerical data show that the number of different values of $(j_1,j_2,j_3,j_4)_2$ is equal to 3 for $p=5$ and no less than 4 or 5 for $p=7,11,13$. Thus we need more equalities to determine the values of $(j_1,j_2,j_2,j_4)_2$ for a general prime $p>5$. Moreover, the calculations in the proof of Theorem 2 rely on the characteristic $p=5$, and therefore new methods should be proposed to compute the values of $(j_1,j_2,j_3,j_4)_2$ in other characteristics.

4 The differential spectrum of $x^{\frac{5^n-1}{2}+2}$ over $\mathbb{F}_{5^n}$

In this section, we determine the differential spectrum of $x^{\frac{5^n-1}{2}+2}$ over $\mathbb{F}_{5^n}$ by making use of the cardinalities of the intersections of some particular cyclotimic classes of order two.

According to the definition of differential spectrum of a power function $F(x)$, we have

$$\sum\nolimits_{i=0}^{\Delta_F}w_i=\sum\nolimits_{i=0}^{\Delta_F}i\cdot w_i=p^n.$$

Then by Lemma 2 and Theorem 2, the differential spectrum of $x^{\frac{5^n-1}{2}+2}$ over $\mathbb{F}_{5^n}$ can be determined as follows.

Theorem 3. *Let $F(x) = x^d$ be a power function over $\mathbb{F}_{5^n}$, where $d = \frac{5^n-1}{2} + 2$. Then the differential spectrum of F is*

$$\{w_0, w_1, w_2, w_3\} = \left\{ \frac{p^n - 2s + 1}{4}, \frac{9p^n + 14s - 7}{16}, \frac{p^n - 2s + 1}{8}, \frac{p^n - 2s + 1}{16} \right\}$$

if n is even, and

$$\{w_0, w_1, w_2, w_3\} = \left\{ \frac{p^n + 2s + 1}{4}, \frac{9p^n - 6s - 7}{16}, \frac{p^n - 6s + 1}{8}, \frac{p^n + 10s + 1}{16} \right\}$$

if n is odd.

Proof. To determine the differential spectrum of $F(x)$, it is sufficient to consider the number of the solutions of

$$(x+1)^d - x^d = b \tag{1}$$

for any $b \in \mathbb{F}_{p^n}$. Clearly, $x = 0$ gives $b = 1$ and $x = -1$ gives $b = -1$ since $d = \frac{5^n-1}{2} + 2$ is even. Suppose $x(x+1) \neq 0$, then (1) becomes

$$(\eta(x+1) - \eta(x))x^2 + 2\eta(x+1)x + \eta(x+1) - b = 0. \tag{2}$$

Note that $\mathbb{F}_{p^n}^* \backslash \{-1\} = \mathcal{C}_{0,0}^{(2)} \cup \mathcal{C}_{0,1}^{(2)} \cup \mathcal{C}_{1,0}^{(2)} \cup \mathcal{C}_{1,1}^{(2)}$. Then we divide the discussions in the following four cases.

Case I: $x \in \mathcal{C}_{0,0}^{(2)}$, i.e., $\eta(x) = \eta(x+1) = 1$. Then (2) becomes $2x + 1 - b = 0$, which leads to $x = \frac{b-1}{2}$. Therefore (2) has at most one solution in $\mathcal{C}_{0,0}^{(2)}$ and $x = \frac{b-1}{2} \in \mathcal{C}_{0,0}^{(2)}$ if b belongs to

$$D_1 = \{b \in \mathbb{F}_{p^n} \mid \eta((b-1)/2) = \eta((b+1)/2) = 1\}.$$

Case II: $x \in \mathcal{C}_{1,1}^{(2)}$, i.e., $\eta(x) = \eta(x+1) = -1$. In this case, (2) can be reduced to $2x+1+b = 0$, which leads to $x = -\frac{b+1}{2}$. Therefore (2) has one solution in $\mathcal{C}_{1,1}^{(2)}$ if b belongs to

$$\begin{aligned} D_2 &= \{b \in \mathbb{F}_{p^n} \mid \eta(-(b+1)/2) = \eta(-(b-1)/2) = -1\} \\ &= \{b \in \mathbb{F}_{p^n} \mid \eta((b-1)/2) = \eta((b+1)/2) = -1\}. \end{aligned}$$

Case III: $x \in \mathcal{C}_{0,1}^{(2)}$, i.e., $\eta(x) = 1$ and $\eta(x+1) = -1$. Then (2) is equivalent to

$$2x^2 + 2x + b + 1 = 0. \tag{3}$$

In can be computed that the discriminant of (3) is equal to $\Delta_3 = -4(2b+1)$. If $\Delta_3 = 0$, then $x = -\frac{1}{2} \notin \mathcal{C}_{0,1}^{(2)}$ due to $p = 5$. If $\eta(\Delta_3) = 1$, then (3) has two solutions in $\mathbb{F}_{p^n}^* \backslash \{-1\}$, which can be represented as $x_3, x_3' = \frac{-1 \pm \sqrt{-2b-1}}{2}$. Clearly, $x_3 + 1 = -x_3'$, $x_3' + 1 = -x_3$ and

$x_3(x_3+1) = -\frac{b+1}{2}$. Due to $\eta(-1)=1$, one obtains that $\eta(x_3)=\eta(x_3'+1)$, $\eta(x_3')=\eta(x_3+1)$ and (3) has at most one solution in $\mathcal{C}_{0,1}^{(2)}$. Thus (3) has exactly one solution in $\mathcal{C}_{0,1}^{(2)}$ if $b \in D_3$, where $D_3 = \{b \in \mathbb{F}_{p^n} \mid \eta(\Delta_3)=1,\ \eta(x_3(x_3+1)=-1)\}$ which can also be written as

$$D_3 = \{b \in \mathbb{F}_{p^n} \mid \eta(2b+1)=1,\ \eta((b+1)/2)=-1\}.$$

Case IV: $x \in \mathcal{C}_{1,0}^{(2)}$, i.e., $\eta(x)=-1$ and $\eta(x+1)=1$. In this case, (2) becomes

$$2x^2+2x+1-b=0. \tag{4}$$

Then the discriminant of (4) equals $\Delta_4 = 4(2b-1)$. If $\Delta_4=0$, then $x=\frac{1}{2}\notin \mathcal{C}_{0,1}^{(2)}$ for $p=5$. If $\eta(\Delta_4)=1$, then (4) has two solutions in $\mathbb{F}_{p^n}^*\backslash\{-1\}$, which can be written as $x_4, x_4' = \frac{-1\pm\sqrt{2b-1}}{2}$. Obviously, $x_4+1=-x_4'$, $x_4'+1=-x_4$ and $x_4(x_4+1)=\frac{b-1}{2}$. Due to $\eta(-1)=1$, one obtains that (4) has at most one solution in $\mathcal{C}_{1,0}^{(2)}$, and (4) has exactly one solution in $\mathcal{C}_{1,0}^{(2)}$ if $b\in D_4$, where $D_4=\{b\in\mathbb{F}_{p^n}\mid \eta(\Delta_4)=1,\ \eta(x_4(x_4+1)=-1)\}$. Equivalently,

$$D_4 = \{b \in \mathbb{F}_{p^n} \mid \eta(2b-1)=1,\ \eta((b-1)/2)=-1\}.$$

Clearly, $b=\pm1\notin D_1\cup D_2\cup D_3\cup D_4$, $D_1\cap(D_2\cup D_3\cup D_4)=\emptyset$ and $D_3\cap D_4 = D_2\cap D_3\cap D_4$. Therefore, (2) has at most three solutions in $\mathbb{F}_{p^n}$ and the number of solutions of (1) is

$$\delta_F(1,b) = \begin{cases} 3, & \text{if } b\in D_2\cap D_3\cap D_4;\\ 2, & \text{if } b\in \big((D_2\cap D_3)\cup(D_2\cap D_4)\big)\backslash(D_2\cap D_3\cap D_4);\\ 1, & \text{if } b\in (D_2\cup D_3\cup D_4)\backslash\big((D_2\cap D_3)\cup(D_2\cap D_4)\cup(D_2\cap D_3\cap D_4)\big),\\ & \text{or } b\in D_1,\ \text{or } b=\pm1;\\ 0, & \text{otherwise.}\end{cases}$$

From the definitions of $(i_1,i_2,i_3)_2$ and $(j_2,j_2,j_3,j_4)_2$, we get

$$\begin{aligned}\#(D_2\cap D_3) &= \#\{b\in\mathbb{F}_{p^n}\mid \eta(2b+1)=1,\ \eta((b+1)/2)=\eta((b-1)/2)=-1\}\\ &= \#\{b\in\mathbb{F}_{p^n}\mid \eta(2b+1)=1,\ \eta(2b+2)=\eta(2b+3)=-1\}\\ &= (0,1,1)_2,\end{aligned}$$

$$\begin{aligned}\#(D_2\cap D_4) &= \#\{b\in\mathbb{F}_{p^n}\mid \eta(2b-1)=1,\ \eta((b+1)/2)=\eta((b-1)/2)=-1\}\\ &= \#\{b\in\mathbb{F}_{p^n}\mid \eta(2b+2)=\eta(2b+3)=-1,\ \eta(2b+4)=1\}\\ &= (1,1,0)_2,\end{aligned}$$

$$\begin{aligned}\#(D_2\cap D_3\cap D_4) &= \#\{b\in\mathbb{F}_{p^n}\mid \eta(2b+1)=\eta(2b-1)=1, \eta((b+1)/2)=\eta((b-1)/2)=-1\}\\ &= \#\{b\in\mathbb{F}_{p^n}\mid \eta(2b+1)=\eta(2b+4)=1, \eta(2b+2)=\eta(2b+3)=-1\}\\ &= (0,1,1,0)_2.\end{aligned}$$

By Lemma 2 and Theorem 2, we have $w_3 = (0,1,1,0)_2 = \frac{p^n-2s+1}{16}$ (resp. $\frac{p^n+10s+1}{16}$) if n is even (resp. n is odd) and $w_2 = (0,1,1)_2 + (1,1,0)_2 - 2(0,1,1,0)_2 = \frac{p^n-2s+1}{8}$ (resp. $\frac{p^n-6s+1}{8}$) if n is even (resp. n is odd). Then the results follow from $w_0 + w_1 + w_2 + w_3 = w_1 + 2w_2 + 3w_3 = p^n$.

The proof is completed. □

5 Conclusions

In this paper, we completely determined the differential spectrum of $x^{\frac{p^n-1}{2}+2}$ for $p = 5$ by means of the cardinalities of the intersection of $(\mathcal{C}_{i_1}^{(2)} - 1) \cap (\mathcal{C}_{i_2}^{(2)} - 2) \cap (\mathcal{C}_{i_3}^{(2)} - 3)$ and the intersection of $(\mathcal{C}_{j_1}^{(2)} - 1) \cap (\mathcal{C}_{j_2}^{(2)} - 2) \cap (\mathcal{C}_{j_3}^{(2)} - 3) \cap (\mathcal{C}_{j_4}^{(2)} - 4)$ for $i_1, i_2, i_3, j_1, j_2, j_3, j_4 \in \{0, 1\}$, where $\mathcal{C}_0^{(2)}, \mathcal{C}_1^{(2)}$ are the cyclotomic classes of order two over $\mathbb{F}_{p^n}$. For a general prime $p > 5$, new approaches will be needed for investigating the differential spectrum of $x^{\frac{p^n-1}{2}+2}$ over $\mathbb{F}_{p^n}$.

References

[1] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, J. Cryptology, 4(1) (1991), 3-72.

[2] C. Blondeau, A. Canteaut, P. Charpin, Differential properties of power functions, Int. J. Inf. Coding Theory, 1(2) (2010), 149-170.

[3] L. Carlitz, Pairs of quadratic equations in a finite fields, Amer. J. Math. 76 (1954), 137-154.

[4] S. T. Choi, S. Hong, J. S. No, H. Chung, Differential spectrum of some power functions in odd prime characteristic, Finite Fields Appl., 21 (2013), 11-29.

[5] H. Dobbertin, T. Helleseth, P. V. Kumar, H. Martinsen, Ternary m-sequences with three-valued cross-correlation function: New decimations of Welch and Niho type, IEEE Trans. Inf. Theory, 47(4) (2001), 1473-1481.

[6] T. Helleseth, D. Sandberg, Some power mapping with low differential uniformity, Appl Algebra Engrg Comm Comput., 8(5) (1997), 363-370.

[7] S. Jiang, K. Li, Y. Li, L. Qu, Differential and boomerang spectrums of some power permutations, Cryptogr. Commun., 14 (2022), 371-393.

[8] L. Lei, W. Ren, C. Fan, The differential spectrum of a class of power functions over finite fields, Adv. Math. Commun., 15(3) (2021), 525-537.

[9] Y. Man, Y. Xia, C. Li, T. Helleseth, On the differential properties of the power mapping x^{p^m+2}, arXiv: 2204.08118.

[10] K. Nyberg, Differentially uniform mappings for cryptography, In: T. Helleseth (eds.), Advances in Cryptology-EUROCRYPT'93, 765 (1994), 55-64.

[11] T. Pang, N. Li, X. Zeng, H. Zhu, A note on the c-differential spectrum of an APcN function, Submitted.

[12] T. Storer, Cyclotomy and Difference Sets, Lect. Adv. Math., Markham, Chicago, IL, 1967.

[13] Y. Xia, X. Zhang, C. Li, T. Helleseth, The differential spectrum of a ternary power mapping, Finite Fields Appl., 64 (2020), 101660.

[14] H. Yan, C. Li, Differential spectra of a class of power permutations with characteristic 5, Des. Codes Cryptogr., 89 (2021), 1181-1191.

[15] H. Yan, Y. Xia, C. Li, T. Helleseth, J. Luo, The differential spectrum of the power mapping x^{p^n-3}, arXiv:2108.03088.

[16] H. Yan, Z. Zhou, J. Weng, J. Wen, T. Helleseth, Q. Wang, Differential spectrum of Kasami power permutations over odd characteristic finite fields, IEEE Trans. Inf. Theory, 65(10) (2019), 6819-6826.