J. Korean Math. Soc. **55** (2018), No. 6, pp. 1469–1483
https://doi.org/10.4134/JKMS.j170763
pISSN: 0304-9914 / eISSN: 2234-3008

CHARACTERIZATION OF CERTAIN TYPES OF r-PLATEAUED FUNCTIONS

Jong Yoon Hyun, Jungyun Lee, and Yoonjin Lee

Abstract. We study a subclass of p-ary functions in n variables, denoted by $\mathcal{A}_n$, which is a collection of p-ary functions in n variables satisfying a certain condition on the exponents of its monomial terms. Firstly, we completely classify all p-ary $(n-1)$-plateaued functions in n variables by proving that every $(n-1)$-plateaued function should be contained in $\mathcal{A}_n$. Secondly, we prove that if f is a p-ary r-plateaued function contained in $\mathcal{A}_n$ with $\deg f > 1 + \frac{n-r}{4}(p-1)$, then the highest degree term of f is only a single term. Furthermore, we prove that there is no p-ary r-plateaued function in $\mathcal{A}_n$ with maximum degree $(p-1)\frac{n-r}{2}+1$. As application, we partially classify all $(n-2)$-plateaued functions in $\mathcal{A}_n$ when $p = 3, 5$, and 7, and p-ary bent functions in $\mathcal{A}_2$ are completely classified for the cases $p = 3$ and 5.

1. Introduction

Binary plateaued functions (more exactly, r-plateaued functions) are introduced by Zheng and Zhang [12] for designing cryptographic functions. They are important cryptographic functions due to their desirable cryptographic characteristics such as high nonlinearity, resiliency, high algebraic degree and so on (refer to [6, 7] for instance). They also include some Boolean functions such as bent functions, semi-bent functions and partially bent functions; 0-plateaued functions are in fact bent functions. Furthermore, there has been extensive research on p-ary plateaued functions (for example, refer to [1–3, 5, 8–11]).

Received November 25, 2017; Accepted January 30, 2018.
2010 *Mathematics Subject Classification.* 94C10, 94B05.
Key words and phrases. plateaued function, Bent function, cryptographic function.
The first author was supported by the National Research Foundation of Korea(NRF) grant funded by theKorea government(MEST) (NRF-2017R1A2B2004574), the second and third named authors were supported by Basic Science Research Program through the National Re- search Foundation of Korea(NRF) funded by the Ministry of Education(2009-0093827), and the second named author is supported by National Research Foundation of Korea (NRF) grant founded by the Korea government(MEST)(NRF-2017R1A6A3A11030486) and a research grant of Kangwon National University in 2018, and the third named author also by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST)(NRF-2017R1A2B2004574).

According to Hou's result [4, Theorem 4.6], he showed that for a p-ary function f in one variable with p an odd prime, f is bent if and only if the degree of f is two. The key idea for his proof is using the property that if f is a p-ary function with $\deg f \leq \frac{p-1}{2}$, then for any two monomial terms x^u and x^v of f, we have that

$$u + v \leq p - 1.$$

Motivated by Hou's result, Hyun et al. [5, Theorem 11] considered a p-ary plateaued function f in n variables for which every exponent u_i of a monomial term $x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$ of f is at most $\frac{p-1}{2}$. We denote the set of such p-ary plateaued functions by $\mathcal{A}_n$. Hyun et al proved that if f is a p-ary $(n-1)$-plateaued function in $\mathcal{A}_n$ then it can be written as follows:

$$f(\mathbf{x}) = \sum_{i=1}^{n} a_i x_i^2 + \sum_{\mathbf{u} \in \{0,1\}^n} b_{\mathbf{u}} \mathbf{x}^{\mathbf{u}}, \tag{1}$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{x}^{\mathbf{u}} = x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$, a_i and $b_{\mathbf{u}}$ are in $\mathbb{Z}_p^*$. In fact, this result is an extension of Hou's result [5], where he considered $\mathcal{A}_1$.

In this paper, we study a subclass $\mathcal{A}_n$ of p-ary functions in n variables. Firstly, we completely classify all p-ary $(n-1)$-plateaued functions in n variables by proving that every $(n-1)$-plateaued function should be contained in $\mathcal{A}_n$. Secondly, we prove that if f is a p-ary r-plateaued function contained in $\mathcal{A}_n$ with $\deg f > 1 + \frac{n-r}{4}(p-1)$, then the highest degree term of f is a single term (Theorem 4.2). Furthermore, we prove that there is no p-ary r-plateaued function in $\mathcal{A}_n$ with maximum degree $(p-1)\frac{n-r}{2} + 1$ (Corollary 4.4). As application, we partially classify all $(n-2)$-plateaued functions in $\mathcal{A}_n$ when $p = 3, 5$, and 7, and p-ary bent functions in $\mathcal{A}_2$ are completely classified for the cases $p = 3$ and 5 (Section 5).

2. Preliminary

We introduce definitions and notation to be used throughout the paper.

Let $[n]$ be the set of integers from one to n and $\mathbb{Z}_p$ the ring of integers modulo p, where p is an odd prime number, and we denote $\mathbb{Z}_p \setminus \{0\}$ by $\mathbb{Z}_p^*$. We consider a set $\mathbf{U} = \{0, 1, \ldots, p-1\}$ of exponents of all monomials in $\mathbb{Z}_p[x]/(x^p - x)$. We define an operation $\oplus$ of $\mathbf{U}$ as follows: for $u, v \in \mathbf{U}$,

$$x^u x^v = x^{u \oplus v}.$$

From the relation $x^p = x$, we see that $0 \oplus 0 = 0$ and $u \oplus v$ is the modulo $(p-1)$ representative of $u + v$ in $\mathbf{U}$ if u and v are not both 0. We point out that it is not generally true that $u + v = u \oplus v$; it however holds when $u + v$ is contained in $\mathbf{U}$, that is, $u + v \leq p - 1$. We extend $\oplus$ to $\mathbf{U}^n$ which operates component-wise. For $\mathbf{u} \in \mathbf{U}^n$ and $i \in [n]$,

$$\pi_i : \mathbf{U}^n \to \mathbf{U}$$

is a projection mapping from $\mathbf{u}$ to the i-th component of $\mathbf{u}$.

A p-ary function f in n variable is a function from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p$, which is uniquely expressed by

$$f(\mathbf{x}) = \sum_{\mathbf{u}\in\mathbf{U}^n} a_{\mathbf{u}}\mathbf{x}^{\mathbf{u}} = \sum_{\mathbf{u}\in\mathbf{U}^n} a_{\mathbf{u}} x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n},$$

where $\mathbf{x} = (x_1, x_2, \dots, x_n)$, $\mathbf{u} = (u_1, u_2, \dots, u_n) \in \mathbf{U}^n$ and $a_{\mathbf{u}} \in \mathbb{Z}_p$.

We define a subset $\mathbf{U}_f$ of $\mathbf{U}^n$ to be

$$\mathbf{U}_f := \{\mathbf{u} \in \mathbf{U}^n \mid a_{\mathbf{u}} \neq 0\}.$$

The *lexicographic order* $\preceq$ on $\mathbf{U}_f$ is defined by $\mathbf{u} \preceq \mathbf{v}$ for $\mathbf{u}, \mathbf{v} \in \mathbf{U}_f$ if $\pi_i(\mathbf{u}) < \pi_i(\mathbf{v})$ for the first i in which $\pi_i(\mathbf{u})$ and $\pi_i(\mathbf{v})$ differ. The degree of f, denoted by $\deg f$ or $\deg(f)$, is $\max\{\sum_{i=1}^n \pi_i(\mathbf{u}) \mid u \in \mathbf{U}_f\}$.

The following lemma whose proof is obvious, plays a crucial role in the paper.

Lemma 2.1. *Let* $\mathbf{u}, \mathbf{v} \in \mathbf{U}^n$. *If* $\pi_i(\mathbf{u}) + \pi_i(\mathbf{v}) \leq p-1$ *for* $i \in [n]$, *then* $\mathbf{u} \oplus \mathbf{v} = \mathbf{u} + \mathbf{v}$ *and* $\deg \mathbf{x}^{\mathbf{u}\oplus\mathbf{v}} = \deg \mathbf{x}^{\mathbf{u}} + \deg \mathbf{x}^{\mathbf{v}}$.

Let d be the degree of a p-ary function f in n variables. A subset $\mathbf{U}_f^d$ of $\mathbf{U}_f$ is defined by

$$\mathbf{U}_f^d = \{\mathbf{u} \in \mathbf{U}_f \mid \sum_{i=1}^n \pi_i(\mathbf{u}) = d\}.$$

Then $\mathbf{U}_f^d$ is written as

$$\mathbf{U}_f^d = \{\mathbf{u}_{k_1}, \mathbf{u}_{k_2}, \dots, \mathbf{u}_{k_s}\},$$

where $\mathbf{u}_{k_1} \prec \cdots \prec \mathbf{u}_{k_{s-1}} \prec \mathbf{u}_{k_s}$.

We define the subclass $\mathcal{A}_n$ of p-ary functions in n variables as follows.

Notation 2.2.

$$\mathcal{A}_n = \{f : \mathbb{Z}_p^n \to \mathbb{Z}_p \mid \pi_i(\mathbf{u}) \leq \frac{p-1}{2}, \forall i \in [n], \forall \mathbf{u} \in \mathbf{U}_f\}.$$

Lemma 2.3. *Let f be a p-ary function in $\mathcal{A}_n$. If $\mathbf{u}, \mathbf{v} \in \mathbf{U}_f$, then*

$$\deg(\mathbf{x}^{\mathbf{u}\oplus\mathbf{v}}) = \sum_{i=1}^n \pi_i(\mathbf{u} \oplus \mathbf{v}) = \sum_{i=1}^n (\pi_i(\mathbf{u}) + \pi_i(\mathbf{v})) = \deg \mathbf{x}^{\mathbf{u}} + \deg \mathbf{x}^{\mathbf{v}}.$$

The complex-valued function S_f of a p-ary function f in n variables, called the *Walsh-Hadamard transform* of f, is defined by

$$S_f(\mathbf{c}) = \sum_{\mathbf{x}\in\mathbb{Z}_p^n} \zeta_p^{f(\mathbf{x}) - \mathbf{c}\cdot\mathbf{x}},$$

where ζ_p is a primitive p-th root of unity. A p-ary function f in n variables is called *r-plateaued* if $|S_f(\mathbf{c})|^2 \in \{0, p^{n+r}\}$ for any $\mathbf{c} \in \mathbb{Z}_p^n$, where r is an integer between 0 and n. We note that a p-ary bent function f in n variables is 0-plateaued. In this case, $|S_f(\mathbf{c})|^2 = p^n$ for any $\mathbf{c} \in \mathbb{Z}_p^n$.

The authors proved in [5] that if f is an r-plateaued function in n variables, then the degree of f is at most

$$(p-1)\frac{n-r}{2}+1, \tag{2}$$

except for the case $p=3$ and $n=1$; we will say that f has *maximum degree* if f is of degree $(p-1)\frac{n-r}{2}+1$. From this bound we see that n-plateaued functions are affine, and they are of the form $a_1x_1+a_2x_2+\cdots+a_nx_n+\epsilon$, where $\epsilon, a_i \in \mathbb{Z}_p$ $(i=1,2,\ldots,n)$.

We say that p-ary functions f and g in n variables are *extended affine equivalent* (for short, *EA-equivalent*) if

$$g(\mathbf{x}) = cf(L(\mathbf{x})+u)+v\cdot\mathbf{x}+e$$

for some $c\in\mathbb{Z}_p^*, e\in\mathbb{Z}_p, u, v\in\mathbb{Z}_p^n$ and a linear bijective function L from $\mathbb{Z}_p^n$ to itself. In particular, f is r-plateaued if and only if g is r-plateaued.

Let $\omega:\mathbb{Z}_p\to\mathbb{F}_p$ be *a Teichmüller character*, where $\mathbb{F}_p$ is the p-adic integer ring and $\omega(x)$ is the unique solution of $\omega(x)^p=\omega(x)$ in $\mathbb{F}_p$ with $\omega(x)\equiv x \pmod p$. The *Gauss sum* $g(t)$ of ω for $t\in\mathbb{Z}/(p-1)\mathbb{Z}$ is defined by

$$g(t) = -\sum_{x\in\mathbb{Z}_p^*}\omega(x)^{-t}\zeta_p^x.$$

We define $G(t)$ for $t\in\mathbb{Z}/(p-1)\mathbb{Z}$ associated with the Gauss sum to be

$$G(t)=\begin{cases}1 & \text{if } t=0,\\ \frac{p}{1-p} & \text{if } t=p-1,\\ \frac{g(t)}{1-p} & \text{if } 0<t<p-1.\end{cases}$$

The following proposition plays an important role in proving our main results.

Proposition 2.4 ([4, Theorem 4.1])**.** *Let p be an odd prime and ϵ a non-negative real number. For a p-ary function $f(\mathbf{x})=\sum_{i=1}^m a_i\mathbf{x}^{\mathbf{u}_i}$ with $a_i\in\mathbb{Z}_p^*$, we define*

$$h_f(\mathbf{u}) = \sum_{\substack{0\le t_i\le p-1\\ t_1\mathbf{u}_1\oplus\cdots\oplus t_m\mathbf{u}_m=\mathbf{u}}} G(t_1)G(t_2)\cdots G(t_m)\omega(a_1^{t_1}a_2^{t_2}\cdots a_m^{t_m}). \tag{3}$$

Then the following conditions are equivalent:

(1) $v_p(S_f(\mathbf{c}))\ge\epsilon$ *for all* $\mathbf{c}\in\mathbb{Z}_p^n$.

(2) $v_p(h_f(\mathbf{u}))\ge\epsilon-n+\frac{1}{p-1}\sum_{i=1}^n\pi_i(\mathbf{u})$ *for all* $\mathbf{u}\in\mathbf{U}^n$,

where v_p denotes by the p-adic valuation.

Remark 2.5. We note that if f is a p-ary r-plateaued function in n variables, then $v_p(S_f(\mathbf{c}))\ge\frac{n+r}{2}$ for all $\mathbf{c}\in\mathbb{Z}_p^n$. Therefore, f satisfies the condition (1) in Proposition 2.4. Furthermore, we have [4] that

$$v_p\Big(G(t_1)G(t_2)\cdots G(t_m)\omega(a_1^{t_1}a_2^{t_2}\cdots a_m^{t_m})\Big)=\frac{t_1+t_2+\cdots+t_m}{p-1}. \tag{4}$$

3. Classification of $(n-1)$-plateaued functions

In this section we completely classify all p-ary $(n-1)$-plateaued functions in n variables (Theorem 3.1). We first prove that if f is a p-ary $(n-1)$-plateaued function in $\mathcal{A}_n$, then it is actually quadratic (Lemma 3.2), and then we show that there is no $(n-1)$-plateaued function which is not contained in $\mathcal{A}_n$ (Lemmas 3.5 and 3.6).

Theorem 3.1. *Let p be an odd prime and f a p-ary $(n-1)$-plateaued function in n variables. Then f is EA-equivalent to ax_1^2 for $a \in \mathbb{Z}_p^*$.*

We provide the proof of Theorem 3.1 at the end of this section.

Claim 1: Any $(n-1)$-plateaued function in $\mathcal{A}_n$ is quadratic

We start with remark that since a p-ary $(n-1)$-plateaued function in n variables has maximum degree $\frac{p+1}{2}$ (see (2)), any term $x_i^{\frac{p+1}{2}}$ for $i \in [n]$ does not appear in f as a monomial if and only if $f \in \mathcal{A}_n$.

Lemma 3.2. *Let p be an odd prime and f a p-ary $(n-1)$-plateaued function in n variables. If any term $x_i^{\frac{p+1}{2}}$ for $i \in [n]$ does not appear in f as a monomial, that is, $f \in \mathcal{A}_n$, then*

$$f(\mathbf{x}) = \sum_{i,j=1}^{n} a_{ij} x_i x_j,$$

where a_{ij}'s are contained in $\mathbb{Z}_p$.

Proof. It follows from (1), we get that

$$f(\mathbf{x}) = \sum_{i=1}^{n} a_i x_i^2 + \sum_{\mathbf{u} \in \{0,1\}^n} b_{\mathbf{u}} \mathbf{x}^{\mathbf{u}},$$

where a_i and $b_{\mathbf{u}}$ belong to $\mathbb{Z}_p^*$. We assume that f is not quadratic, that is, there is $\mathbf{u}_0 \in \{0,1\}^n \cap \mathbf{U}_f$ with $\deg \mathbf{x}^{\mathbf{u}_0} \geq 3$. Without loss of generality, we may set $\mathbf{x}^{\mathbf{u}_0} = x_1 x_2 x_3 \cdots x_d$, where $d = \deg \mathbf{x}^{\mathbf{u}_0}$. We consider a linear bijective function L defined by

$$L(x_1, x_2, x_3, \ldots, x_n) = (x_1, x_1 + x_2, x_3, \ldots, x_n).$$

Then $f \circ L$ is an $(n-1)$-plateaued function and any term $x_i^{\frac{p+1}{2}}$ for i in $[n]$ does not appear in $f \circ L$ as a monomial. Applying (1) to $f \circ L$ leads to a contradiction. This is because L transforms $x_1 x_2 x_3 \cdots x_d$ into $x_1(x_1 + x_2)x_3 \cdots x_d$, so $f \circ L$ contains the monomial $x_1^2 x_3 \cdots x_d$. $\square$

Claim 2: There is no $(n-1)$-plateaued function which does not belong to $\mathcal{A}_n$

We will work on the case that a term $x_i^{\frac{p+1}{2}}$ appears in f as a monomial for some $i \in [n]$. We prove using Lemmas 3.5(iii) and 3.6 that there is no $(n-1)$-plateaued function which is not in $\mathcal{A}_n$.

Lemma 3.3. *Let p be an odd prime and f a p-ary $(n-1)$-plateaued function in n variables. Let at least one of the terms $x_i^{\frac{p+1}{2}}$ for $i \in [n]$ appear in f as a monomial. Then the following statements are true.*

(i) *f is EA-equivalent to $\tilde{f}$ with*

$$\tilde{f}(\mathbf{x}) = ax_1^{\frac{p+1}{2}} + g_2(x_2, \ldots, x_n)x_1^{\frac{p-3}{2}} + \cdots + g_{\frac{p+1}{2}}(x_2, \ldots, x_n),$$

where $g_t \in \mathbb{Z}_p[x_2, \ldots, x_n]$ for $t = 2, 3, \ldots, \frac{p+1}{2}$.

(ii) *For $\mathbf{u}_0 = (\frac{p+1}{2}, 0, \ldots, 0) \in \mathbf{U}_{\tilde{f}}$ and $\mathbf{u} \in \mathbf{U}_{\tilde{f}}$ with $\mathbf{u} \neq \mathbf{u}_0$, we have that $\pi_i(\mathbf{u}) + \pi_i(\mathbf{u}_0) \leq p-1$ $(i = 1, 2, \ldots, n)$, which implies $\mathbf{u} \oplus \mathbf{u}_0 = \mathbf{u} + \mathbf{u}_0$ and $\deg(\mathbf{x}^{\mathbf{u} \oplus \mathbf{u_0}}) = \deg \mathbf{x}^{\mathbf{u}} + \deg \mathbf{x}^{\mathbf{u_0}}$.*

Proof. (i) Without loss of generality, we may assume that f contains $x_1^{\frac{p+1}{2}}$ as a monomial. By expanding f in terms of x_1, we have that

$$\begin{aligned} f(\mathbf{x}) = {} & ax_1^{\frac{p+1}{2}} + h_1(x_2, \ldots, x_n)x_1^{\frac{p-1}{2}} \\ & + h_2(x_2, \ldots, x_n)x_1^{\frac{p-3}{2}} + \cdots + h_{\frac{p+1}{2}}(x_2, \ldots, x_n), \end{aligned}$$

where $a \in \mathbb{Z}_p^*$ and $h_t \in \mathbb{Z}_p[x_2, \ldots, x_n]$ for $t = 1, 2, \ldots, \frac{p+1}{2}$. The degree of h_1 is at most one because $\deg f = \frac{p+1}{2}$. Consider a linear bijective function $\tilde{L}$ defined by

$$\tilde{L}(x_1, x_2, \ldots, x_n) = \left(x_1 - \bar{a}\overline{\frac{p+1}{2}}h_1(x_2, \ldots, x_n), x_2, \ldots, x_n\right),$$

where $\bar{i} \in \mathbb{Z}_p^*$ for $i \in \mathbb{Z}_p^*$ is the unique element such that $\bar{i}i \equiv 1 \pmod{p}$. Then f is equivalent to $f \circ \tilde{L}$, and the first part is proved by putting $\tilde{f} = f \circ \tilde{L}$.

(ii) Let $\mathbf{u} \in \mathbf{U}_{\tilde{f}}$ with $\mathbf{u} \neq \mathbf{u}_0 (= (\frac{p+1}{2}, 0, \ldots, 0))$. It follows from the first result of this lemma that $\mathbf{u}_0 = \left(\frac{p+1}{2}, 0 \ldots, 0\right) \in \mathbf{U}_{\tilde{f}}$ and $\pi_1(\mathbf{u}) \leq \frac{p-3}{2}$. We also have that $\pi_i(\mathbf{u}_0) = 0$ and $\pi_i(\mathbf{u}) \leq \frac{p+1}{2}$ for $i = 2, 3, \ldots, n$. From this observation and Lemma 2.1 the second part follows. □

From now on, we work on $\tilde{f}$ defined in Lemma 3.3. Let $\mathbf{U}_{\tilde{f}} = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m\}$. Recall from Preliminary that

$$\mathbf{U}_{\tilde{f}}^{\deg \tilde{f}} = \{\mathbf{u}_{k_1}, \mathbf{u}_{k_2}, \ldots, \mathbf{u}_{k_s}\},$$

where $\mathbf{u}_{k_1} \prec \mathbf{u}_{k_2} \prec \cdots \prec \mathbf{u}_{k_s}$.

Remark 3.4. (i) We point out that $\mathbf{u}_{k_s} = (\frac{p+1}{2}, 0, \ldots, 0)$, $\mathbf{u}_{k_s} \oplus \mathbf{u}_{k_{s-1}} = \mathbf{u}_{k_s} + \mathbf{u}_{k_{s-1}}$ and $\deg(\mathbf{x}^{\mathbf{u}_{k_s} \oplus \mathbf{u}_{k_{s-1}}}) = p+1$ using Lemma 2.1.

(ii) It is easy to verify that if $\mathbf{u}_\alpha \preceq \mathbf{u}_\beta$ and $\mathbf{u}_\gamma \preceq \mathbf{u}_\delta$, then $\mathbf{u}_\alpha + \mathbf{u}_\gamma \preceq \mathbf{u}_\beta + \mathbf{u}_\delta$, and if $\mathbf{u}_\alpha + \mathbf{u}_\beta \preceq \mathbf{2u}_\beta$, then $\mathbf{u}_\alpha \preceq \mathbf{u}_\beta$.

Lemma 3.5. *Let $\tilde{f}$ be a p-ary r-plateaued function in n variables defined in Lemma 3.3. Then the following statements are true.*

(i) *With the previous setting, the equation $\mathbf{u}_{k_s} \oplus \mathbf{u}_{k_{s-1}} = t_1\mathbf{u}_1 \oplus t_2\mathbf{u}_2 \oplus \cdots \oplus t_m\mathbf{u}_m$ satisfying $t_1 + t_2 + \cdots + t_m = 2$ has only one trivial solution as $t_{k_s} = 1 = t_{k_{s-1}}$, that is,*

$$v_p(h_{\tilde{f}}(\mathbf{u}_{k_{s-1}} \oplus \mathbf{u}_{k_s})) = \frac{2}{p-1},$$

which is also true when k_{s-1} is replaced by k_j for $j \neq s$.

(ii) *The highest degree term of $\tilde{f}$ is just a single term $x_1^{\frac{p+1}{2}}$.*

(iii)

$$\tilde{f}(\mathbf{x}) = a x_1^{\frac{p+1}{2}} + h(x_1, x_2, \ldots, x_n),$$

where $a \in \mathbb{Z}_p^*$ and $\deg h \leq 1$.

Proof. Put $\mathbf{U}_{\tilde{f}}^* = \{\mathbf{u} \in \mathbf{U}_{\tilde{f}} \mid \pi_i(\mathbf{u}) \leq \frac{p-1}{2},\ i \in [n]\}$.

(i) Assume that $\mathbf{u}_{k_s} \oplus \mathbf{u}_{k_{s-1}} = \mathbf{u}_\alpha \oplus \mathbf{u}_\beta$ for $1 \leq \alpha \leq \beta \leq m$. It is sufficient to show that $(\alpha, \beta) = (k_{s-1}, k_s)$. The proof is divided into two parts.

Case I: One of $\mathbf{u}_\alpha$ and $\mathbf{u}_\beta$ is not in $\mathbf{U}_{\tilde{f}}^*$.

If $\mathbf{u}_\alpha = \mathbf{u}_{k_s}$, then our claim is obviously true by using Lemma 3.3. Now, we assume that $\mathbf{u}_\alpha = (0, \ldots, \frac{p+1}{2}, \ldots, 0)$. Using $\pi_1(\mathbf{u}_\alpha) = 0$ and Lemma 3.3, we see that

$$\begin{aligned}\frac{p+1}{2} &= \deg \tilde{f} \geq \pi_1(\mathbf{u}_\beta) = \pi_1(\mathbf{u}_\alpha \oplus \mathbf{u}_\beta) \\ &= \pi_1(\mathbf{u}_{k_s} \oplus \mathbf{u}_{k_{s-1}}) \\ &= \pi_1(\mathbf{u}_{k_s} + \mathbf{u}_{k_{s-1}}) = \frac{p+1}{2} + \pi_1(\mathbf{u}_{k_{s-1}}) \geq \frac{p+1}{2},\end{aligned}$$

which implies $\pi_1(\mathbf{u}_\beta) = \frac{p+1}{2}$, and so $\pi_i(\mathbf{u}_\beta) = 0$ for $i = 2, \ldots, n$ due to the degree of $\tilde{f}$. It follows that $\mathbf{u}_\beta = \mathbf{u}_{k_s}$. By the assumption, we have $\mathbf{u}_\alpha = \mathbf{u}_{k_{s-1}}$ and the first case is completed.

Case II: Both $\mathbf{u}_\alpha$ and $\mathbf{u}_\beta$ are in $\mathbf{U}_{\tilde{f}}^*$. In this case, $\mathbf{u}_\alpha \oplus \mathbf{u}_\beta = \mathbf{u}_\alpha + \mathbf{u}_\beta$.

Assume, in contrary, that $(\alpha, \beta) \neq (k_{s-1}, k_s)$. Notice that

$$\deg \mathbf{x}^{\mathbf{u}_\alpha} + \deg \mathbf{x}^{\mathbf{u}_\beta} = \deg(\mathbf{x}^{\mathbf{u}_\alpha \oplus \mathbf{u}_\beta}) = \deg(\mathbf{x}^{\mathbf{u}_{k_s} \oplus \mathbf{u}_{k_{s-1}}}) = p+1.$$

Here, the first equality follows from Lemma 2.1 using $\mathbf{u}_\alpha, \mathbf{u}_\beta \in \mathbf{U}_{\tilde{f}}^*$, and the last equality follows from Remark 3.4. It then follows from $\deg \mathbf{x}^{\mathbf{u}_\alpha}, \deg \mathbf{x}^{\mathbf{u}_\beta} \leq \frac{p+1}{2}$ that $\mathbf{u}_\alpha$ and $\mathbf{u}_\beta$ belong to $\mathbf{U}_{\tilde{f}}^{\frac{p+1}{2}}$, so that $\mathbf{u}_\alpha, \mathbf{u}_\beta \preceq \mathbf{u}_{k_{s-1}}$. Using Remark 3.4, we derive that $\mathbf{u}_{k_{s-1}} + \mathbf{u}_{k_s} = \mathbf{u}_\alpha + \mathbf{u}_\beta \preceq 2\mathbf{u}_{k_{s-1}}$, or $\mathbf{u}_{k_s} \preceq \mathbf{u}_{k_{s-1}}$, which is a contradiction. This proves the first part of (i). The second part follows from (4).

(ii) Assuming, in contrary, we have that there are at least two distinct elements in $\mathbf{U}_{\tilde{f}}^{\frac{p+1}{2}}$, say $\mathbf{u}_{k_{s-1}}$ and $\mathbf{u}_{k_s}$. From Lemma 3.5(i), Proposition 2.4 and Remark 3.4, we see that

$$\begin{aligned}\frac{2}{p-1} &= v_p(h_{\tilde{f}}(\mathbf{u}_{k_{s-1}} \oplus \mathbf{u}_{k_s})) \\ &\geq \frac{2n-1}{2} - n + \frac{1}{p-1}\sum_{i=1}^{n} \pi_i(\mathbf{u}_{k_{s-1}} \oplus \mathbf{u}_{k_s}) = -\frac{1}{2} + \frac{p+1}{p-1},\end{aligned}$$

which is a contradiction.

(iii) It is sufficient to prove that the second highest degree of $\tilde{f}$ is less than or equal to 1. Let $\mathbf{U}_{\tilde{f}} = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$, where $\deg \mathbf{x}^{\mathbf{v}_1} \leq \deg \mathbf{x}^{\mathbf{v}_2} \leq \cdots \leq \deg \mathbf{x}^{\mathbf{v}_m}$. Then $\mathbf{v}_m = (\frac{p+1}{2}, 0, \ldots, 0)$ and $\mathbf{x}^{\mathbf{v}_m}$ is only one monomial term of $\tilde{f}$ with degree $\frac{p+1}{2}$ by (ii). We claim that

$$v_p(h_{\tilde{f}}(\mathbf{v}_m \oplus \mathbf{v}_{m-1})) = \frac{2}{p-1}.$$

As in (i) we show that if $\mathbf{v}_m \oplus \mathbf{v}_{m-1} = \mathbf{v}_\alpha \oplus \mathbf{v}_\beta$ for $1 \leq \alpha \leq \beta \leq m$, then $(\alpha, \beta) = (m-1, m)$. Obviously, if one of $\mathbf{v}_\alpha$ and $\mathbf{v}_\beta$ is not in $\mathbf{U}^*_{\tilde{f}}$, then $(\alpha, \beta) = (m-1, m)$. It remains to consider the case that both $\mathbf{v}_\alpha$ and $\mathbf{v}_\beta$ belong to $\mathbf{U}^*_{\tilde{f}}$. Assume, in contrary, that $(\alpha, \beta) \neq (m-1, m)$. Then $\deg \mathbf{x}^{\mathbf{v}_\alpha}, \deg \mathbf{x}^{\mathbf{v}_\beta} \leq \deg \mathbf{x}^{\mathbf{v}_{m-1}}$. By a similar argument as in (i), we have that

$$\begin{aligned}\deg \mathbf{x}^{\mathbf{v}_m} + \deg \mathbf{x}^{\mathbf{v}_{m-1}} &= \deg(\mathbf{x}^{\mathbf{v}_m \oplus \mathbf{v}_{m-1}}) \\ &= \deg(\mathbf{x}^{\mathbf{v}_\alpha \oplus \mathbf{v}_\beta}) \\ &= \deg \mathbf{x}^{\mathbf{v}_\alpha} + \deg \mathbf{x}^{\mathbf{v}_\beta} \leq 2 \deg \mathbf{x}^{\mathbf{v}_{m-1}},\end{aligned}$$

or $\deg \mathbf{x}^{\mathbf{v}_m} = \deg \mathbf{x}^{\mathbf{v}_{m-1}}$, which contradicts that $\mathbf{x}^{\mathbf{v}_m}$ is only one monomial term of f with degree $\frac{p+1}{2}$. This proves the claim. It thus follows from Proposition 2.4 that

$$\frac{2}{p-1} \geq \frac{2n-1}{2} - n + \frac{1}{p-1}\Big(\frac{p+1}{2} + \deg \mathbf{x}^{\mathbf{v}_{m-1}}\Big),$$

or $\deg \mathbf{x}^{\mathbf{v}_{m-1}} \leq 1$. This completes the proof. □

Lemma 3.6. *Let $p \geq 5$ be a prime. Then a p-ary function f in n variables defined by*

$$f(\mathbf{x}) = a x_1^{\frac{p+1}{2}} + \sum_{i=1}^{n} b_i x_i \quad (a \neq 0, b_i \in \mathbb{Z}_p)$$

cannot be $(n-1)$-plateaued.

Proof. Let j be a primitive root modulo p. Since

$$\mathbb{Z}_p^* = \{x^2 \mid x \in \mathbb{Z}_p^*\} \cup \{jx^2 \mid x \in \mathbb{Z}_p^*\},$$

we get that for $a \in \mathbb{Z}_p^*$,

$$\sum_{x\in\mathbb{Z}_p} \zeta_p^{ax^{\frac{p+1}{2}}-ax} = \frac{1}{2}\Big(\sum_{x\in\mathbb{Z}_p} \zeta_p^{a(x^2)^{\frac{p+1}{2}}-ax^2} + \sum_{x\in\mathbb{Z}_p} \zeta_p^{a(jx^2)^{\frac{p+1}{2}}-ajx^2}\Big).$$

From

$$(x^2)^{\frac{p+1}{2}} \equiv x^2 \pmod p \quad \text{and} \quad j^{\frac{p+1}{2}} \equiv -j \pmod p,$$

we see that

$$\sum_{x\in\mathbb{Z}_p} \zeta_p^{a(x^2)^{\frac{p+1}{2}}-ax^2} = p$$

and

$$\sum_{x\in\mathbb{Z}_p} \zeta_p^{a(jx^2)^{\frac{p+1}{2}}-ajx^2} = \sum_{x\in\mathbb{Z}_p} \zeta_p^{-2jax^2}.$$

It is known that for $a \in \mathbb{Z}_p^*$,

$$\sum_{x\in\mathbb{Z}_p} \zeta_p^{-2jax^2} = \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ \pm\sqrt{-p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

We may assume that $f(\mathbf{x}) = ax_1^{\frac{p+1}{2}}$ for $a \in \mathbb{Z}_p^*$ up to EA-equivalence. Consequently,

we get that

$$S_f(a,0,\ldots,0) = \begin{cases} \frac{1}{2}(p \pm \sqrt{p})p^{n-1} & \text{if } p \equiv 1 \pmod 4, \\ \frac{1}{2}(p \pm \sqrt{-p})p^{n-1} & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{5}$$

We find from (5) that if $p \geq 5$, then

$$|S_f(a,0,\ldots,0)|^2 \neq p^{2n-1}.$$

Thus $f(\mathbf{x}) = ax_1^{\frac{p+1}{2}}$ with $a \in \mathbb{Z}_p^*$ cannot be an $(n-1)$-plateaued function. □

Proof of Theorem 3.1

First of all, the case of $p = 3$ follows from (2). Assume the case of $p \geq 5$. Combining Lemma 3.3(i), Lemma 3.5(iii) and Lemma 3.6, we get that every $(n-1)$-plateaued function f should be contained in $\mathcal{A}_n$. In Lemma 3.2, we proved that any $(n-1)$-plateaued function f in $\mathcal{A}_n$ is

$$f(\mathbf{x}) = \sum_{i,j=1}^{n} a_{ij}x_ix_j,$$

where a_{ij}'s are contained in $\mathbb{Z}_p$. We note that every quadratic form $f(\mathbf{x}) = \sum_{1\leq i\leq j\leq n} a_{ij}x_ix_j$ for a_{ij} in $\mathbb{Z}_p$ is transformed to a diagonal quadratic form $d_1x_1^2 + d_2x_2^2 + \cdots + d_nx_n^2$. Moreover, it follows from Proposition 1 of [3] that every $(n-1)$-plateaued diagonal quadratic form is $d_ix_i^2$, which completes the proof.

4. Properties of r-plateaued functions in $\mathcal{A}_n$

In this section, we prove that if f is a p-ary r-plateaued function in n variables contained in $\mathcal{A}_n$ with $\deg f > 1+\frac{n-r}{4}(p-1)$, then the highest degree term of f is just a single term and the other terms have degree $\leq 2+\frac{n-r}{2}(p-1)-\deg f$.

Lemma 4.1. *Let p be an odd prime, f a p-ary function in $\mathcal{A}_n$ and $\mathbf{U}_f = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$. Then the following statements are true.*

(i) *If $\mathbf{U}_f^{\deg f} = \{\mathbf{u}_{k_1}, \mathbf{u}_{k_2}, \ldots, \mathbf{u}_{k_s}\}$, where $\mathbf{u}_{k_1} \prec \cdots \prec \mathbf{u}_{k_{s-1}} \prec \mathbf{u}_{k_s}$ contains at least two elements, then $v_p(h_f(\mathbf{u}_{k_{s-1}} \oplus \mathbf{u}_{k_s})) = \frac{2}{p-1}$.*

(ii) *If $\mathbf{U}_f^{\deg f}$ contains exactly one element, then $v_p(h_f(\mathbf{v}_{m-1} \oplus \mathbf{v}_m)) = \frac{2}{p-1}$, where $\deg \mathbf{x}^{\mathbf{v}_1} \leq \deg \mathbf{x}^{\mathbf{v}_2} \leq \cdots \leq \deg \mathbf{x}^{\mathbf{v}_m}$.*

Proof. It is proved by similar arguments as in Lemma 3.5. □

Theorem 4.2. *Let p be an odd prime and f a p-ary r-plateaued function in $\mathcal{A}_n$. If $\deg f > 1+\frac{n-r}{4}(p-1)$, then the highest degree term of f is a monomial and the other terms have degree $\leq 2+\frac{n-r}{2}(p-1)-\deg f$. That is,*

$$f(\mathbf{x}) = a\mathbf{x}^{\mathbf{u}} + g(x_1, x_2, \ldots, x_n),$$

where $a \in \mathbb{Z}_p^*$, $\deg \mathbf{x}^{\mathbf{u}} = \deg f$ and $\deg g \leq 2+\frac{n-r}{2}(p-1)-\deg f$.

Proof. Let $\mathbf{U}_f = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m\}$ and $d = \deg f$. Recall from Preliminary that $\mathbf{U}_f^d = \{\mathbf{u}_{k_1}, \mathbf{u}_{k_2}, \ldots, \mathbf{u}_{k_s}\}$, where $\mathbf{u}_{k_1} \prec \mathbf{u}_{k_2} \prec \cdots \prec \mathbf{u}_{k_s}$. First, we prove that $\mathbf{U}_f^d$ contains only one element. Assuming, in contrary, $\mathbf{U}_f^d$ contains at least two distinct elements. It then follows from Lemma 2.3 that

$$\sum_{i=1}^{n} \pi_i(\mathbf{u}_{k_s} \oplus \mathbf{u}_{k_{s-1}}) = \sum_{i=1}^{n} \Big(\pi_i(\mathbf{u}_{k_s}) + \pi_i(\mathbf{u}_{k_{s-1}})\Big) = 2d$$

and from Lemma 4.1(i) that

$$v_p(h_f(\mathbf{u}_{k_s} \oplus \mathbf{u}_{k_{s-1}})) = \frac{2}{p-1}.$$

Proposition 2.4 implies that

$$\frac{2}{p-1} \geq \frac{n+r}{2} - n + \frac{1}{p-1}\sum_{i=1}^{n} \pi_i(\mathbf{u}_{k_s} \oplus \mathbf{u}_{k_{s-1}}) = -\frac{n-r}{2} + \frac{2d}{p-1},$$

which is a contradiction to the condition of $\deg f$, and so the claim is proved. That is, the highest degree term of f is a single monomial.

Now, we prove that the second highest degree is $\leq 2+\frac{n-r}{2}(p-1)-d$. Let $\mathbf{U}_f = \{\mathbf{v}_1, \mathbf{v}_2 \ldots, \mathbf{v}_m\}$, where $\deg \mathbf{x}^{\mathbf{v}_1} \leq \cdots \leq \deg \mathbf{x}^{\mathbf{v}_{m-1}} \leq \deg \mathbf{x}^{\mathbf{v}_m}$. By Lemma 4.1(ii), we have

$$v_p(h_f(\mathbf{v}_m \oplus \mathbf{v}_{m-1})) = \frac{2}{p-1}.$$

Using $\sum_{i=1}^{n} \pi_i(\mathbf{v}_m \oplus \mathbf{v}_{m-1}) = d + \deg \mathbf{x}^{\mathbf{v}_{m-1}}$ (see Lemma 2.3) and from Proposition 2.4 lead to

$$\frac{2}{p-1} \geq \frac{n+r}{2} - n + \frac{1}{p-1}\Big(d + \deg \mathbf{x}^{\mathbf{v}_{m-1}}\Big).$$

The second claim follows from $\deg \mathbf{x}^{\mathbf{v}_{m-1}} = \deg g$, and the proof is completed. $\square$

Recall that every r-plateaued function f in n variables has the degree less than or equal to $\frac{n-r}{2}(p-1)+1$.

Lemma 4.3. *If a monomial $a\mathbf{x}^{\mathbf{u}}$ for $a \in \mathbb{Z}_p^*$ and $\mathbf{u} \in \mathbf{U}^n$ is an r-plateaued function in $\mathcal{A}_n$, then*

$$\deg \mathbf{x}^{\mathbf{u}} \leq \frac{n-r}{4}(p-1)+1.$$

Proof. Let $f(\mathbf{x}) = a\mathbf{x}^{\mathbf{u}}$. Then we can check that $v_p(h_f(2\mathbf{u})) = \frac{2}{p-1}$ and $\sum_{i=1}^{n} \pi_i(2\mathbf{u}) = 2\sum_{i=1}^{n} \pi_i(\mathbf{u})$. By Proposition 2.4, we see that

$$\frac{2}{p-1} \geq \frac{n+r}{2} - n + \frac{2}{p-1}\deg \mathbf{x}^{\mathbf{u}},$$

and the result follows. $\square$

Using Theorem 4.2 and Lemma 4.3 we prove that there is no r-plateaued function in $\mathcal{A}_n$ with maximum degree.

Corollary 4.4. *Let p be an odd prime, f an r-plateaued function in $\mathcal{A}_n$. Then*

$$\deg f \leq \frac{n-r}{2}(p-1).$$

Proof. Assume that f is an r-plateaued function in $\mathcal{A}_n$ with the degree $\frac{n-r}{2}(p-1)+1$. It follows from Theorem 4.2 that f is written as

$$f(\mathbf{x}) = a\mathbf{x}^{\mathbf{u}} + g(x_1, x_2, \ldots, x_n),$$

where $a \in \mathbb{Z}_p^*$, $\deg \mathbf{x}^{\mathbf{u}} = \frac{n-r}{2}(p-1)+1$ and $\deg g \leq 1$. Thus $a\mathbf{x}^{\mathbf{u}}$ ia also r-plateaued, which is a contradiction to Lemma 4.3. $\square$

We strengthen Theorem 4.2 for r-plateaued functions in $\mathcal{A}_n$ as follows.

Corollary 4.5. *Let p be an odd prime ≥ 5. If f is an r-plateaued function in $\mathcal{A}_n$ with $\deg f \geq 2 + \frac{n-r-1}{2}(p-1)$, then $\deg f > n$. This implies that when $2 + \frac{n-r-1}{2}(p-1) \leq n$, there is no p-ary $(n-1)$-plateaued function in $\mathcal{A}_n$ with its degree between $1 + \frac{n-r-1}{2}(p-1)$ and $n+1$.*

Proof. By Theorem 4.2, we may write f as

$$f(\mathbf{x}) = a\mathbf{x}^{\mathbf{u}} + g(x_1, x_2, \ldots, x_n),$$

where $a \in \mathbb{Z}_p^*$, $\deg g \leq 2 + \frac{n-r}{2}(p-1) - \deg f$ and $\deg \mathbf{x}^{\mathbf{u}} = \deg f$. The *Hamming weight* of u in $\mathbb{Z}_p^*$ is the number of nonzero coordinate positions, denoted by $|u|$.

We claim that (i) $|\mathbf{u}| = n$ and so $\deg f = \deg \mathbf{x}^{\mathbf{u}} \geq n$ and (ii) $\deg f \neq n$. First, we consider $|\mathbf{u}| < n$ to drive a contradiction. Then there is $k \in \{1, 2, \ldots, n\}$ such that $\pi_k(\mathbf{u}) = 0$. For the simplicity of arguments, we assume $\pi_1(\mathbf{u}) \neq 0$ and $k \neq 1$. We consider a linear transform L_1 defined by

$$L_1(x_1, x_2, \ldots, x_n) = (x_1 + x_k, x_2, \ldots, x_n).$$

Then $\mathbf{x}^{\mathbf{u}} = x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$ is transformed by L_1 into

$$\sum_{i=0}^{u_1} \binom{u_1}{i} x_1^{u_1-i} x_k^i x_2^{u_2} \cdots x_{k-1}^{u_{k-1}} x_{k+1}^{u_{k+1}} \cdots x_n^{u_n},$$

which is also in $\mathcal{A}_n$ by noticing that every exponent of

$$x_1^{u_1-i} x_k^i x_2^{u_2} \cdots x_{k-1}^{u_{k-1}} x_{k+1}^{u_{k+1}} \cdots x_n^{u_n}$$

for $i = 0, 1, \ldots, u_1$ is at most $\frac{p-1}{2}$ because f is in $\mathcal{A}_n$. From the degree bounds of f and g we derive that $\deg g \leq \frac{p-1}{2}$. Those two observations imply that $f \circ L_1$ is in $\mathcal{A}_n$, and it has at least two monomials with highest degree, which is a contradiction to Theorem 4.2.

Now we consider $\deg \mathbf{x}^{\mathbf{u}} = n$. By Theorem 4.2, we may write f as

$$f(\mathbf{x}) = a x_1 x_2 \cdots x_n + g(x_1, x_2, \ldots, x_n),$$

where $a \in \mathbb{Z}_p^*$ and $\deg g \leq \frac{p-1}{2}$. We consider a linear transform L_2 defined by

$$L_2(x_1, x_2, \ldots, x_n) = (x_1 + x_2, x_2, \ldots, x_n).$$

We notice that $f \circ L_2 \in \mathcal{A}_n$ whenever $p \geq 5$. The same arguments as above yield a contradiction. This completes the proof. $\square$

Let f be a p-ary function in $\mathcal{A}_n$ with $\mathbf{U}_f = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m\}$. Let us take the maximum value of $\{\pi_j(\mathbf{u}_i)\}_{1 \leq i \leq m, 1 \leq j \leq n}$, say $\pi_\ell(\mathbf{u}_k)$, called *the maximal exponent of* f and denoted it by e_f. Now, we choose a permutation σ in the permutation group S_n sending ℓ to 1. We set

$$\mathbf{U}_{\sigma f}^{\preceq} = \{\mathbf{v}_i \in \mathbf{U}_{\sigma f} \mid i = 1, 2, \ldots, m\}$$

imposed the lexicographic order $\preceq$. We point out that $\pi_1(\mathbf{v}_m) = e_f$. Let $s = \left\lfloor \frac{p-1}{e_f} \right\rfloor$, where $\lfloor t \rfloor$ is the least integer lager than or equal to t. It follows from Lemma 12 in [5] that

$$v_p(h_f(s\mathbf{v}_m)) = \frac{s}{p-1}.$$

Proposition 2.4 implies that

$$v_p(h_f(s\mathbf{v}_m)) = \frac{s}{p-1} \geq -\frac{n-r}{2} + \frac{s}{p-1} \sum_{i=1}^{n} \pi_i(\mathbf{v}_m),$$

or

$$\sum_{i=1}^{n} \pi_i(\mathbf{v}_m) \leq 1 + \frac{n-r}{2} \frac{p-1}{s}.$$

With the previous discussion, we have the following lemma.

Lemma 4.6. *Let p be an odd prime, f a p-ary r-plateaued function in n variables and $s = \left\lfloor \frac{p-1}{e_f} \right\rfloor$. Let $\mathbf{u} \in \mathbf{U}_f$ with $\pi_1(\mathbf{u}) = e_f$ be the maximal element of $\mathbf{U}_f$ which is imposed the lexicographic order $\preceq$. Then*

$$\sum_{i=1}^{n} \pi_i(\mathbf{u}) \leq 1 + \frac{n-r}{2}\frac{p-1}{s}.$$

5. Application: partial classification of $(n-2)$-plateaued functions

In this section, we partially classify all $(n-2)$-plateaued functions in $\mathcal{A}_n$ when $p = 3, 5$ and 7, and p-ary bent functions in $\mathcal{A}_2$ are completely classified for the cases $p = 3$ and 5.

Proposition 5.1. *The following statements are true.*

(i) *Every ternary $(n-2)$-plateaued function in $\mathcal{A}_n$ is quadratic.*

(ii) *The degree of every 5-ary $(n-2)$-plateaued function in $\mathcal{A}_n$ is at most three. In particular, every bent function in $\mathcal{A}_2$ is quadratic.*

(iii) *The degree of every 7-ary $(n-2)$-plateaued function $\mathcal{A}_n$ is at most five. In particular, the degree of every bent function in $\mathcal{A}_2$ is at most four.*

Proof. (i) It is a direct consequence of Corollary 4.4.

(ii) Let f be a 5-ary $(n-2)$-plateaued function in $\mathcal{A}_n$. Using Corollary 4.4, the degree of f is at most four. If f is of degree four, then we get from Corollary 4.5 that $n < 4$. We thus obtain the following table: For $a \in \mathbb{Z}_5^*$ and $\deg g \leq 2$

n	$f \in \mathcal{A}_n$ with degree 4	$\mathbf{u}$ maximal element of $\mathbf{U}_f$
2	$ax_1^2x_2^2 + g(x_1, x_2)$	$(2, 2)$
3	$ax_1^2x_2x_3 + g(x_1, x_2, x_3)$	$(2, 1, 1)$

By Lemma 4.6 with $\pi_1(\mathbf{u}) = e_f = 2$ in both cases of the table, we have that $4 = \sum_{i=1}^{n} \pi_i(\mathbf{u}) \leq 3$, which is a contradiction. This proves the first part of (ii). The second part of (ii) follows by using *Mathematica* program.

(iii) Let f be a 7-ary $(n-2)$-plateaued function in $\mathcal{A}_n$. Using Corollary 4.4, the degree of f is at most six. If f is of degree six, then we find from Corollary 4.5 that $n < 6$. Hence, we obtain the following table: For $a \in \mathbb{Z}_7^*$ and $\deg g \leq 2$

n	$f \in \mathcal{A}_n$ with degree 6	$\mathbf{u}$ maximal element of $\mathbf{U}_f$
2	$ax_1^3x_2^3 + g(x_1, x_2)$	$(3, 3)$
3	$ax_1^2x_2^2x_3^2 + g(x_1, x_2, x_3)$	$(2, 2, 2)$
3	$ax_1^3x_2^2x_3 + g(x_1, x_2, x_3)$	$(3, 2, 1)$
4	$ax_1^2x_2^2x_3x_4 + g(x_1, x_2, x_3, x_4)$	$(2, 2, 1, 1)$
4	$ax_1^3x_2x_3x_4 + g(x_1, x_2, x_3, x_4)$	$(3, 1, 1, 1)$
5	$ax_1^2x_2x_3x_4x_5 + g(x_1, x_2, x_3, x_4, x_5)$	$(2, 1, 1, 1, 1)$

By Lemma 4.6 with $\pi_1(\mathbf{u}) = e_f = 2$ (respectively, 3) in the table, we have that $6 = \sum_{i=1}^n \pi_i(\mathbf{u}) \leq 3$ (respectively, ≤ 4) which is a contradiction. This proves the first part of (iii).

Now we prove that the degree of every bent function in $\mathcal{A}_2$ is at most four. Let f be a 7-ary bent function in $\mathcal{A}_2$ with degree five. Then by Theorem 4.2, it is written as

$$f(\mathbf{x}) = ax^3y^2 + g(x, y),$$

where $a \in \mathbb{Z}_7{}^*$ and $\deg g \leq 3$. By Lemma 4.6 with $\pi_1(\mathbf{u}) = e_f = 3$ for the maximal element $\mathbf{u} \in \mathbf{U}_f$, we have that $5 = \sum_{i=1}^2 \pi_i(\mathbf{u}) \leq 4$, which is a contraction, and the proof is completed. □

References

[1] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes in Boolean Methods and Models*, Cambridge University Press, Cambridge, 2010.

[2] C. Carlet and E. Prouff, *On plateaued functions and their constructions*, Proceedings of Fast Software Encryption 2003, Lecture Notes in Computer Science, 2887, Springer, Berlin, 54–73, 2003.

[3] A. Çeşmelioğlu and W. Meidl, *A construction of bent functions from plateaued functions*, Des. Codes Cryptogr. **66** (2013), no. 1-3, 231–242.

[4] X.-D. Hou, *p-ary and q-ary versions of certain results about bent functions and resilient functions*, Finite Fields Appl. **10** (2004), no. 4, 566–582.

[5] J. Y. Hyun, J. Lee, and Y. Lee, *Explicit criteria for construction of plateaued functions*, IEEE Trans. Inform. Theory **62** (2016), no. 12, 7555–7565.

[6] M. Matsui, *Linear cryptananalysis method for DES cipher*, in Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science, **765**, (1994), 386–397.

[7] W. Meier and O. Staffelbach, *Fast correlation attacks on stream ciphers*, in Advances in Cryptology, EUROCRYPT'88, Lecture Notes in Computer Science, **330**, (1988), 301–314.

[8] S. Mesnager, *Characterizations of plateaued and bent functions in characteristic p*, in Sequences and their applications—SETA 2014, 72–82, Lecture Notes in Comput. Sci., 8865, Springer, Cham, 2014.

[9] ———, *On semi-bent functions and related plateaued functions over the Galois field* $\mathbb{F}_{2^n}$, in Open problems in mathematics and computational science, 243–273, Springer, Cham, 2014.

[10] ———, *Characterizations of plateaued and bent functions in characteristic p*, in Sequences and their applications—SETA 2014, 72–82, Lecture Notes in Comput. Sci., 8865, Springer, Cham, 2014.

[11] S. Mesnager, F. Ozbudak, and A. Sinak, *Characterizations of plateaued functions in arbitrary characteristic*, Proceedings of ICCC 2015, Algers, 2015.

[12] Y. Zheng and X. M. Zhang, *Plateaued functions*, Advances in Cryptology-ICICS'99, Lecture Notes in Computer Science, Heidelberg, Ed., Springer-Verlag, **1726**, (1999), 284–300.

Jong Yoon Hyun
Korea Institute for Advanced Study (KIAS)
Seoul 02455, Korea
Email address: hyun33@kias.re.kr

Jungyun Lee
Department of Mathematics Education
Kangwon National University
Chuncheon 24341, Korea
Email address: lee9311@kangwon.ac.kr

Yoonjin Lee
Department of Mathematics
Ewha Womans University
Seoul 03760, Korea
Email address: yoonjinl@ewha.ac.kr