ON DISTANCES BETWEEN BENT FUNCTIONS, BETWEEN PLATEAUED FUNCTIONS AND BOUNDS ON NONLINEARITIES OF p-ARY FUNCTIONS

FERRUH ÖZBUDAK & VLADIMIR N. POTAPOV

Abstract. We obtain lower bounds on the distance between two different bent functions and between two different s-plateaued functions in odd characteristic. For odd p and $n \geq 2$, we obtain a new explicit upper bound on the nonlinearity of a p-ary function in terms of the cardinality S of its Walsh support. For $S \geq (p-1)^2$, it reduces to $N_f \leq \lfloor (p-1)p^{n-1} - p^{n-1}/\sqrt{S} \rfloor$. For $S < (p-1)^2$, our bound is a strict refinement of this estimate. It gives the sharp inequality $N_f \leq (p-2)p^{n-1}$ when $S = p$. We characterize equality when $S = p^{n-s}$ with $n-s$ even and when $S = p$; the former characterization implies weak regularity.

Keywords: Bent function, plateaued function, Hamming distance, nonlinearity

AMS(2020) Math Sc. Cl. 94A60, 11T71, 94D10

1. Introduction

The Hamming distances between cryptographic functions have been studied in many papers. These distances correspond to code distances of error-correcting codes obtained by using cryptographic functions [1]. The minimum distance between two Boolean bent functions and the number of bent functions at minimum distance from a fixed bent function were established in [3]. Similar problems for regular p-ary bent functions were resolved in [8] when p is an odd prime. Other related questions, such as possible small distances between Boolean bent functions, were studied in [7] and [4]. The minimum distances between two Boolean correlation immune functions and between two plateaued functions were found in [7] and [8].

The nonlinearity of a function is the minimum Hamming distance between the function and the set of affine functions. It is well-known that Boolean bent functions in n variables attain maximum possible nonlinearity if n is even. The nonlinearity of the maximum nonlinear function is equal to the covering radius of the Hadamard code. The asymptotic behaviour of the maximum nonlinearity of q-ary functions was studied in [12]. For an even number of variables, a class of bent functions reaching the maximum nonlinearity was found in [8] only for $q = 3$, see also [10], [11] for arbitrary q. The

Corresponding author: Ferruh Özbudak is with Faculty of Engineering and Natural Sciences, Sabancı University, 34956, Istanbul, Türkiye, e-mail: ferruh.ozbudak@sabanciuniv.edu.

Vladimir N. Potapov is with Faculty of Engineering and Natural Sciences, Sabancı University, 34956, Istanbul, Türkiye, e-mail: quasigroup349@gmail.com.

maximal nonlinearity of Boolean functions with constraints on the Walsh spectrum was studied in [14].

All possible nonlinearities of p-ary bent and plateaued functions were found in [6]. In this paper we obtain lower bounds on the distance between two different bent functions and between two different s-plateaued functions in odd characteristic. In Theorem 4.1, we derive a new explicit upper bound on nonlinearity in terms of Walsh-support cardinality by optimizing the associated affine value distributions. For $S \geq (p-1)^2$, it reduces to $N_f \leq \lfloor (p-1)p^{n-1} - p^{n-1}/\sqrt{S} \rfloor$. For $S < (p-1)^2$, Theorem 4.1 gives a strict refinement of this estimate. It also yields the sharp bound $N_f \leq (p-2)p^{n-1}$ when the support has cardinality p. We give an exact affine value-distribution characterization of equality in the support-p case and an if-and-only-if characterization of equality when $S = p^{n-s}$ and $n-s$ is even. In Section 4, we combine methods of Ryabov (see [10] and [11]) with an extremal estimate for the affine value frequencies.

The Maiorana-McFarland class, which is used in Section 3, consists of the p-ary functions $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ given by $F(x,y) = \mathrm{Tr}(x\pi(y)) + h(y)$, where $\pi : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ is a permutation and $h : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is an arbitrary p-ary function; every such function is bent. We refer to [1] and [5] for this class and to [2] for the generalized Maiorana-McFarland class, which is also used in Section 3.

The rest of the paper is organized as follows. We provide the necessary definitions as well as appropriate forms of Parseval's identity (Theorem 2.1) and the uncertainty principle (Theorem 2.2) in Section 2. We prove a lower bound on the distance between two different bent functions and between two different s-plateaued functions in odd characteristic in Section 3 (Theorem 3.1). Moreover, we indicate the cases when these bounds are tight. We prove an upper bound on the nonlinearity of a function in terms of the cardinality of the support of its Walsh transform in Section 4, including an exact refinement for sparse Walsh support (Theorem 4.1). We prove that the resulting bound for support cardinality p is sharp (Theorem 4.3), characterize equality when $S = p^{n-s}$ and $n-s$ is even (Theorem 4.2), and give the exact affine value-distribution profiles for equality in the support-p bound (Theorem 4.4). Section 5 contains the conclusion.

2. Background

Let p be a prime. Let $n \geq 1$ be an integer. Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements. Any map $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is called a p-ary function.

Let $\epsilon_p = e^{\frac{2\pi\sqrt{-1}}{p}} \in \mathbb{C}$ be a primitive p-th root of unity. The Walsh transform of the p-ary function f is a complex valued function $\hat{f} : \mathbb{F}_{p^n} \to \mathbb{C}$ defined as

$$\hat{f}(\alpha) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{f(x) - \mathrm{Tr}(\alpha x)},$$

where $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the trace map $x \mapsto x + x^p + \cdots + x^{p^{n-1}}$.

We will use the following well-known proposition.

Proposition 2.1. *Let p be a prime number and let $a_0, \ldots, a_{p-1} \in \mathbb{Q}$. If $\sum_{k=0}^{p-1} a_k \epsilon_p^k = 0$, then $a_k = a_0$ for each $k = 1, \ldots, p-1$.*

Proof. It is sufficient to note that the minimal polynomial of ϵ_p over $\mathbb{Q}$ is $T^{p-1} + T^{p-2} + \cdots + T + 1$. □

A p-ary function f is called *bent* if $|\hat{f}(\alpha)| = p^{n/2}$ for all $\alpha \in \mathbb{F}_{p^n}$, where $|\cdot|$ is the absolute value. Throughout this paper we use $|\cdot|$ both for the absolute value of a complex variable, and for the cardinality of a finite set. We hope that its meaning will be clear from the context.

Let $0 \leq s \leq n-1$ be an integer. A p-ary function f is called *s-plateaued* if

$$|\hat{f}(\alpha)| = p^{\frac{n+s}{2}} \text{ or } 0$$

for all $\alpha \in \mathbb{F}_{p^n}$. Note that $s = 0$ is allowed here: by Parseval's identity a 0-plateaued function has $|\hat{f}(\alpha)| = p^{n/2}$ for all $\alpha \in \mathbb{F}_{p^n}$, and hence the 0-plateaued functions are exactly the bent functions. Moreover, if f is s-plateaued, then $|\mathrm{Supp}(\hat{f})| = p^{n-s}$, again by Parseval's identity.

Let $f, g : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be two arbitrary p-ary functions. The Hamming distance $d_{\mathrm{H}}(f, g)$ is the integer defined as the cardinality of the subset $\{x \in \mathbb{F}_{p^n} : f(x) \neq g(x)\} \subseteq \mathbb{F}_{p^n}$.

The *nonlinearity* N_f of a p-ary function f is

$$\min \left\{ d_{\mathrm{H}}(f, \mathrm{Tr}(ax) + b) : a \in \mathbb{F}_{p^n},\ b \in \mathbb{F}_p \right\},$$

where $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the trace map $x \mapsto x + x^p + \cdots + x^{p^{n-1}}$, and $g(x) = \mathrm{Tr}(ax) + b$ is considered as a p-ary affine function.

We use two fundamental results in our proofs. The first fundamental result is known as Parseval's identity, that we state here. We refer, for example, to [1] for a proof.

Theorem 2.1. *Let p be a prime number and $n \geq 1$ be an integer. Let $f, g : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be arbitrary p-ary functions. We have*

$$p^n \sum_{x \in \mathbb{F}_{p^n}} \left| \epsilon_p^{f(x)} - \epsilon_p^{g(x)} \right|^2 = \sum_{\alpha \in \mathbb{F}_{p^n}} \left| \hat{f}(\alpha) - \hat{g}(\alpha) \right|^2.$$

The second fundamental result is known as the uncertainty principle, that we state here. We refer, for example, to [13, formula (1)]. We note that we state a suitable version of the uncertainty principle, which is different from the one in [13], but equivalent to it.

Theorem 2.2. *Let p be a prime number and $n \geq 1$ be an integer. Let $f, g : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be two distinct p-ary functions. We have*

$$|\mathrm{Supp}(f - g)| \cdot |\mathrm{Supp}(\hat{f} - \hat{g})| \geq p^n.$$

Here $\mathrm{Supp}(f-g)$ *and* $\mathrm{Supp}(\hat{f}-\hat{g})$ *are the subsets of* $\mathbb{F}_{p^n}$ *defined as* $\mathrm{Supp}(f-g)=\{x\in\mathbb{F}_{p^n}: f(x)\neq g(x)\}$ *and* $\mathrm{Supp}(\hat{f}-\hat{g})=\{\alpha\in\mathbb{F}_{p^n}:\hat{f}(\alpha)\neq\hat{g}(\alpha)\}$. *Moreover* $\cdot$ *refers to the multiplication in* $\mathbb{Z}$.

Proof. Let $H(x)=\epsilon_p^{f(x)}-\epsilon_p^{g(x)}$ and $\widetilde{H}(\alpha)=\sum_{x\in\mathbb{F}_{p^n}}H(x)\epsilon_p^{-\mathrm{Tr}(\alpha x)}$. By the definition we see that $\mathrm{Supp}(f-g)=\mathrm{Supp}(H)$ and $\mathrm{Supp}(\hat{f}-\hat{g})=\mathrm{Supp}(\widetilde{H})$.

By Theorem 2.1 we obtain that

$$p^n\sum_{x\in\mathbb{F}_{p^n}}|H(x)|^2=\sum_{\alpha\in\mathbb{F}_{p^n}}|\widetilde{H}(\alpha)|^2\leq|\mathrm{Supp}(\widetilde{H})|\max_{\alpha}|\widetilde{H}(\alpha)|^2. \tag{1}$$

By the Cauchy–Schwarz inequality for every $\alpha\in\mathbb{F}_{p^n}$ we have

$$|\widetilde{H}(\alpha)|^2=|\sum_{x\in\mathbb{F}_{p^n}}H(x)\epsilon_p^{-\mathrm{Tr}(\alpha x)}|^2=|\sum_{x\in\mathrm{Supp}(H)}H(x)\epsilon_p^{-\mathrm{Tr}(\alpha x)}|^2\leq|\mathrm{Supp}(H)|\sum_{x\in\mathbb{F}_{p^n}}|H(x)|^2.$$

Therefore

$$\max_{\alpha}|\widetilde{H}(\alpha)|^2\leq|\mathrm{Supp}(H)|\sum_{x\in\mathbb{F}_{p^n}}|H(x)|^2. \tag{2}$$

Combining (1) and (2) we obtain

$$p^n\sum_{x\in\mathbb{F}_{p^n}}|H(x)|^2\leq|\mathrm{Supp}(\widetilde{H})||\mathrm{Supp}(H)|\sum_{x\in\mathbb{F}_{p^n}}|H(x)|^2.$$

Since $f\neq g$, the last sum is positive. Cancelling it gives the asserted inequality. □

The equality case of the product uncertainty principle, recalled in [13], states that equality in Theorem 2.2 holds precisely when H is a constant multiple of an additive character on a coset of an additive subgroup. For odd p, it follows that equality holds if and only if there exist an affine $\mathbb{F}_p$-subspace $V\subseteq\mathbb{F}_{p^n}$, an element $a\in\mathbb{F}_p^*$, an element $\beta\in\mathbb{F}_{p^n}$, and $b\in\mathbb{F}_p$ such that

$$f-g=a\mathbf{1}_V\quad\text{and}\quad g(x)=\mathrm{Tr}(\beta x)+b\quad\text{for every } x\in V.$$

Indeed, constancy of $|H|$ on V first shows that $f-g$ takes values in $\{a,-a\}$ there. If both values occurred, the quotient of the two corresponding factors $\epsilon_p^{f-g}-1$ would be $-\epsilon_p^a$, which is not a p-th root of unity for odd p. Thus $f-g$ is constant on V, and the phase of H then gives the affine condition on g. Conversely, every pair satisfying the two displayed conditions gives equality.

Next we recall the definitions of regular, weakly regular and non-weakly regular bent functions in odd characteristic. Assume that p is an odd prime and $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ is a bent function. Let $\nu\in\mathbb{C}$ be the constant defined as

$$\nu=\begin{cases}1 & \text{if } -1 \text{ has a square root in } \mathbb{F}_{p^n},\\ i & \text{otherwise.}\end{cases}$$

There exists a p-ary function $f^* : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and a function $\delta_f : \mathbb{F}_{p^n} \to \{1, -1\}$ such that

$$\hat{f}(\alpha) = \nu\delta_f(\alpha)p^{\frac{n}{2}}\epsilon_p^{f^*(\alpha)}$$

for all $\alpha \in \mathbb{F}_{p^n}$. If $\nu\delta_f(\alpha) = 1$ for all $\alpha \in \mathbb{F}_{p^n}$, then f is called a *regular* bent function. If $|\mathrm{Im}(\delta_f)| = 1$, then f is called a *weakly regular* bent function. Otherwise, that is if $|\mathrm{Im}(\delta_f)| = 2$, then f is called a *non-weakly regular* bent function.

These notions generalize naturally to s-plateaued functions [5, 6]. Put $\nu_{n+s} = 1$ if $p^{n+s} \equiv 1 \pmod 4$ and $\nu_{n+s} = i$ if $p^{n+s} \equiv 3 \pmod 4$. If f is s-plateaued, then there exist a p-ary function $f^* : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and a function $\delta_f : \mathbb{F}_{p^n} \to \{1, -1\}$ such that

$$\hat{f}(\alpha) = \nu_{n+s}\delta_f(\alpha)p^{\frac{n+s}{2}}\epsilon_p^{f^*(\alpha)}$$

for all $\alpha \in \mathrm{Supp}(\hat{f})$, while $\hat{f}(\alpha) = 0$ for all $\alpha \notin \mathrm{Supp}(\hat{f})$. Here f is called weakly regular if δ_f is constant on $\mathrm{Supp}(\hat{f})$. Note that the amplitude $p^{\frac{n+s}{2}}$ is forced by the definition of an s-plateaued function. We refer to [6] for further related results.

3. Lower bound on the distance between s-plateaued functions

In the Maiorana-McFarland class, we can find a pair of p-ary bent functions in $2m$ variables at distance p^m. Consider bent functions $f, g : \mathbb{F}_{p^{2m}} \to \mathbb{F}_p$ determined by the equations $f(x, y) = \mathrm{Tr}(yx)$ and $g(x, y) = \mathrm{Tr}(yx) + \phi(y)$. It is easy to see that $d_{\mathrm{H}}(f, g) = |\mathrm{Supp}(\phi)|p^m$. So, $d_{\mathrm{H}}(f, g) = p^m$ if ϕ is the indicator function of a point. Similarly, we can find two vectorial bent functions at the same distance. This distance is minimal for the binary case $p = 2$ (see [3], [7]). For odd p, however, the minimum-distance problem is more subtle (see [8] and Proposition 3.1 below).

In this section, we prove a new lower bound on the distance between two different s-plateaued functions in odd characteristic for $0 \le s \le n - 1$, together with a separate bent bound. The expressions inside the ceilings agree for $p = 3$; for $p > 3$, the bent expression is strictly larger.

Theorem 3.1. *Let p be an odd prime and let $n \ge 2$ be an arbitrary integer. Assume that $0 \le s \le n - 1$ is an integer. Assume also that $f, g : \mathbb{F}_{p^n} \to \mathbb{F}_p$ are distinct s-plateaued functions. Then we have*

$$d_{\mathrm{H}}(f, g) \ge \left\lceil p^{\frac{n+s}{2}} \left(\frac{p-1}{2p}\right)^{1/2} \right\rceil, \tag{3}$$

and if $s = 0$ we have

$$d_{\mathrm{H}}(f, g) \ge \left\lceil p^{\frac{n}{2}} \left(\frac{p-2}{p}\right)^{1/2} \right\rceil, \tag{4}$$

where $\lceil \cdot \rceil$ is the ceiling function on $\mathbb{R}$.

Proof. Let $U \subseteq \mathbb{F}_p^*$ be a chosen and fixed subset such that $|U| = \frac{p-1}{2}$ with the property that $a \in U \implies (-a) \notin U$.

Let $x \in \mathbb{F}_{p^n}$. Since ϵ_p is a root of unity we have $\overline{\epsilon_p^a} = \epsilon_p^{-a}$ for every $a \in \mathbb{F}_p$, and therefore

$$\left|\epsilon_p^{f(x)} - \epsilon_p^{g(x)}\right|^2 = \left(\epsilon_p^{f(x)} - \epsilon_p^{g(x)}\right)\left(\epsilon_p^{-f(x)} - \epsilon_p^{-g(x)}\right) = 2 - \epsilon_p^{f(x)-g(x)} - \epsilon_p^{-f(x)+g(x)},$$

where the last equality uses $\epsilon_p^u \epsilon_p^{-u} = \epsilon_p^0 = 1$ for $u \in \mathbb{F}_p$. The product in the following display expands to the same expression:

$$\left(\epsilon_p^{f(x)-g(x)} - 1\right)\left(\epsilon_p^{-f(x)+g(x)} - 1\right) = 2 - \epsilon_p^{f(x)-g(x)} - \epsilon_p^{-f(x)+g(x)}$$

Comparing this with the preceding identity, we obtain

$$\left|\epsilon_p^{f(x)} - \epsilon_p^{g(x)}\right|^2 = \left(\epsilon_p^{f(x)-g(x)} - 1\right)\left(\epsilon_p^{-f(x)+g(x)} - 1\right).$$

As $f(x) - g(x) \in \{0, 1, \ldots, p-1\}$ we conclude that exactly one of the following two cases holds:

- Case 1.1: $\left|\epsilon_p^{f(x)} - \epsilon_p^{g(x)}\right|^2 = 0$.
- Case 1.2: $\left|\epsilon_p^{f(x)} - \epsilon_p^{g(x)}\right|^2 = 2 - \epsilon_p^a - \epsilon_p^{-a}$ for a uniquely determined $a \in U$.

For $a \in U$, let s_a denote the number of $x \in \mathbb{F}_{p^n}$ such that Case 1.2 holds, or equivalently $\left|\epsilon_p^{f(x)} - \epsilon_p^{g(x)}\right|^2 = 2 - \epsilon_p^a - \epsilon_p^{-a}$. Note that it follows from the definition that

$$|\mathrm{Supp}(f-g)| = \sum_{a \in U} s_a. \tag{5}$$

Let $\alpha \in \mathbb{F}_{p^n}$. As f and g are p-ary s-plateaued functions and p is odd, there exist p-ary functions $f^*, g^* : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and functions $\delta_f, \delta_g : \mathbb{F}_{p^n} \to \{1, -1\}$ such that

$$\hat{f}(\alpha) = \nu_{n+s}\delta_f(\alpha) p^{\frac{n+s}{2}} \epsilon_p^{f^*(\alpha)}, \text{ and}$$

$$\hat{g}(\alpha) = \nu_{n+s}\delta_g(\alpha) p^{\frac{n+s}{2}} \epsilon_p^{g^*(\alpha)}$$

for all α in $\mathrm{Supp}(\hat{f})$ and $\mathrm{Supp}(\hat{g})$ respectively, while $\hat{f}$ and $\hat{g}$ vanish outside their supports.

We have

$$\left|\hat{f}(\alpha) - \hat{g}(\alpha)\right|^2 = p^{n+s}\left(\frac{\delta_f(\alpha)}{\delta_g(\alpha)}\epsilon_p^{f^*(\alpha)-g^*(\alpha)} - 1\right)\left(\frac{\delta_f(\alpha)}{\delta_g(\alpha)}\epsilon_p^{-f^*(\alpha)+g^*(\alpha)} - 1\right)$$

for all α lying in both $\mathrm{Supp}(\hat{f})$ and $\mathrm{Supp}(\hat{g})$. Here we use the facts that $\left|\epsilon_p^{g^*(\alpha)}\right| = 1$ and $\delta_f(\alpha), \delta_g(\alpha) \in \{1, -1\}$ for all $\alpha \in \mathbb{F}_{p^n}$. Combining this formula with the vanishing of the transforms outside their supports, we see that exactly one of the following four cases holds for each $\alpha \in \mathbb{F}_{p^n}$:

- Case 2.1: $\hat{f}(\alpha) = \hat{g}(\alpha)$.

- Case 2.2: α lies in both Walsh supports, $\delta_f(\alpha) = \delta_g(\alpha)$, and $f^*(\alpha) - g^*(\alpha) \in \{a, -a\}$ for a uniquely determined $a \in U$. In this case $|\hat{f}(\alpha) - \hat{g}(\alpha)|^2 = p^{n+s}(2 - \epsilon_p^a - \epsilon_p^{-a})$.
- Case 2.3: α lies in both Walsh supports, $\delta_f(\alpha) = -\delta_g(\alpha)$, and $f^*(\alpha) - g^*(\alpha) \in \{a, -a\}$ for a uniquely determined $a \in U \cup \{0\}$. In this case $|\hat{f}(\alpha) - \hat{g}(\alpha)|^2 = p^{n+s}(2 + \epsilon_p^a + \epsilon_p^{-a})$.
- Case 2.4: α lies in exactly one of $\mathrm{Supp}(\hat{f})$ and $\mathrm{Supp}(\hat{g})$. In this case $|\hat{f}(\alpha) - \hat{g}(\alpha)|^2 = p^{n+s}$.

Case 2.4 is possible only if $s \neq 0$.

For $a \in U$, let t_a denote the number of $\alpha \in \mathbb{F}_{p^n}$ for which Case 2.2 holds with parameter a.

For $a \in U \cup \{0\}$, let t'_a denote the number of $\alpha \in \mathbb{F}_{p^n}$ for which Case 2.3 holds with parameter a.

Denote by τ the number of $\alpha \in \mathbb{F}_{p^n}$ for which Case 2.4 holds.

Note that it follows from these definitions that

$$|\mathrm{Supp}(\hat{f} - \hat{g})| = \tau + t'_0 + \sum_{a \in U}(t_a + t'_a). \tag{6}$$

Using Parseval's identity in Theorem 2.1 we have

$$p^n \sum_{x \in \mathbb{F}_{p^n}} \left|\epsilon_p^{f(x)} - \epsilon_p^{g(x)}\right|^2 = \sum_{\alpha \in \mathbb{F}_{p^n}} \left|\hat{f}(\alpha) - \hat{g}(\alpha)\right|^2. \tag{7}$$

The arguments above and (7) imply that

$$\sum_{a \in U} p^{-s} s_a \left(2 - \epsilon_p^a - \epsilon_p^{-a}\right) = \tau + 4t'_0 + \sum_{a \in U} \left\{ t_a \left(2 - \epsilon_p^a - \epsilon_p^{-a}\right) + t'_a \left(2 + \epsilon_p^a + \epsilon_p^{-a}\right) \right\}.$$

By rearranging we obtain

$$2 \sum_{a \in U} \left(p^{-s} s_a - t_a - t'_a\right) - \tau - 4t'_0 = \sum_{a \in U} \left(\epsilon_p^a + \epsilon_p^{-a}\right) \left(p^{-s} s_a - t_a + t'_a\right). \tag{8}$$

Put

$$Y = 2 \sum_{a \in U} \left(p^{-s} s_a - t_a - t'_a\right) - \tau - 4t'_0. \tag{9}$$

For $a \in U$, let

$$Y_a = p^{-s} s_a - t_a + t'_a. \tag{10}$$

Using Proposition 2.1 and (8) this implies that

$$Y = -Y_a \text{ for all } a \in U. \tag{11}$$

Hence combining (9), (10) and (11) we conclude that

$$Y = 2 \sum_{a \in U} (-Y - 2t'_a) - \tau - 4t'_0$$

and hence

$$pY = -\tau - 4\left(t'_0 + \sum_{a\in U} t'_a\right). \tag{12}$$

Put $S = \sum_{a\in U} s_a$, $T = \sum_{a\in U} t_a$ and $T' = t'_0 + \sum_{a\in U} t'_a$. Using (5) we have

$$S = |\mathrm{Supp}(f-g)|. \tag{13}$$

Using (6) we have

$$T + T' + \tau = |\mathrm{Supp}(\hat{f} - \hat{g})|. \tag{14}$$

These definitions, (9) and (12) imply that

$$-4T' - \tau = pY = 2p\left(p^{-s}S - T - T' - t'_0 - \tau/2\right). \tag{15}$$

Dividing (15) by $2p$ we obtain

$$p^{-s}S = T + \left(1 - \frac{2}{p}\right)T' + t'_0 + \tau\left(\frac{1}{2} - \frac{1}{2p}\right). \tag{16}$$

Consider the case of bent functions, i. e., $s = 0$ and $\tau = 0$. By (16), we obtain

$$S \geq \left(1 - \frac{2}{p}\right)(T + T'). \tag{17}$$

Combining (13), (14) and (17) we obtain

$$\frac{S^2}{1 - \frac{2}{p}} \geq S\,(T + T') = |\mathrm{Supp}(f-g)| \cdot |\mathrm{Supp}(\hat{f} - \hat{g})|. \tag{18}$$

Consider the case $s > 0$. By (16), we obtain

$$\frac{p^{-s}S}{(\frac{1}{2} - \frac{1}{2p})} \geq (T + T' + \tau) \tag{19}$$

because $1 - \frac{2}{p} \geq \frac{1}{2} - \frac{1}{2p}$ if $p \geq 3$. Combining (13), (14) and (19) we obtain

$$\frac{S^2}{\frac{1}{2} - \frac{1}{2p}} \geq p^s S\,(T + T' + \tau) = p^s |\mathrm{Supp}(f-g)| \cdot |\mathrm{Supp}(\hat{f} - \hat{g})|. \tag{20}$$

By Theorem 2.2 and $S = d_{\mathrm{H}}(f,g) = |\mathrm{Supp}(f-g)|$, (18) gives (4). Since $(p-2)/p \geq (p-1)/(2p)$, this also gives (3) for $s = 0$; for $s > 0$, (20) gives that bound. This completes the proof. □

Remark 3.1. *If $p = 3$ and $s = 0$, then $\frac{p-2}{p} = \frac{p-1}{2p}$, so the lower bounds (3) and (4) coincide. If $p > 3$ and $s = 0$, then $\frac{p-2}{p} > \frac{p-1}{2p}$ and hence the lower bound in (4) without the ceiling function is stronger than the lower bound in (3) without the ceiling function.*

If $p = 3$ and $n + s$ is odd, then $p^{\frac{n+s}{2}}\left(\frac{p-1}{2p}\right)^{1/2}$ is an integer, and the lower bound in (3) is tight [8].

Using some methods of [8] we obtain the following result.

Proposition 3.1. *For any integers $s \geq 0$ and $k \geq 0$, there exist two distinct 3-ary s-plateaued functions in $n = 1 + s + 2k$ variables at distance $3^{\frac{s+n-1}{2}}$.*

Proof. Put $V = \mathbb{F}_3^{s+1}$ and $W = \mathbb{F}_3^k$. We identify $V \times W \times W$ with $\mathbb{F}_3^n$, and hence with the additive group of $\mathbb{F}_{3^n}$, and we write $\langle \cdot, \cdot \rangle$ for the standard inner products on V and on W. We compute the Walsh transform with respect to the resulting nondegenerate bilinear form. Under an $\mathbb{F}_3$-linear identification with $\mathbb{F}_{3^n}$, this differs from the trace pairing only by an invertible linear change of the frequency variable, and therefore does not affect the Walsh amplitudes.

For $u = (u_0, u_1, \ldots, u_s) \in V$ we define the two 3-ary functions

$$\phi_s(u) = u_0^2 \text{ and } \psi_s(u) = u_0 + 2u_0^2.$$

The one variable functions $u_0 \mapsto u_0^2$ and $u_0 \mapsto u_0 + 2u_0^2$ are bent over $\mathbb{F}_3$ and they differ exactly at $u_0 = 1$. Consequently, for every $\xi \in V$ the Walsh coefficient $\widehat{\phi_s}(\xi)$ is 0 unless $\xi_1 = \cdots = \xi_s = 0$, in which case its modulus is $3^s \cdot 3^{1/2} = 3^{s+\frac{1}{2}}$; the same holds for ψ_s. Hence ϕ_s and ψ_s are s-plateaued functions in $s+1$ variables, and

$$d_{\mathrm{H}}(\phi_s, \psi_s) = 3^s.$$

For $a \in W$ we put

$$\theta_a^{(1)} = \phi_s \text{ and } \theta_a^{(2)} = \begin{cases} \psi_s & \text{if } a = 0, \\ \phi_s & \text{if } a \neq 0. \end{cases}$$

Let $\chi : W \to \mathbb{F}_3$ be the indicator function of 0 and, for $i \in \{1, 2\}$, let

$$F_i(u, y, z) = \sum_{a \in W} \chi(z + a) \left(\theta_a^{(i)}(u) + \langle a, y \rangle \right) = \theta_{-z}^{(i)}(u) - \langle z, y \rangle,$$

where $u \in V$ and $y, z \in W$. This is a generalized Maiorana-McFarland construction, see [2] and [9].

Let $(\xi, \beta, \gamma) \in V \times W \times W$. In the Walsh sum, the terms depending on y give $\sum_{y \in W} \epsilon_3^{-\langle z+\beta, y \rangle}$, which vanishes unless $z + \beta = 0$, that is, $z = -\beta$. Therefore

$$\widehat{F_i}(\xi, \beta, \gamma) = 3^k \epsilon_3^{\langle \beta, \gamma \rangle} \widehat{\theta_\beta^{(i)}}(\xi).$$

Since every nonzero Walsh coefficient of ϕ_s and of ψ_s has modulus $3^{s+\frac{1}{2}}$, every nonzero Walsh coefficient of F_i has modulus

$$3^k \cdot 3^{s+\frac{1}{2}} = 3^{\frac{n+s}{2}},$$

as $n = 1 + s + 2k$. Hence F_1 and F_2 are s-plateaued functions in n variables.

Finally, $\theta_{-z}^{(1)}$ and $\theta_{-z}^{(2)}$ differ only for $z = 0$, and for $z = 0$ the variable $y \in W$ is arbitrary. Therefore

$$d_{\mathrm{H}}(F_1, F_2) = 3^k \, d_{\mathrm{H}}(\phi_s, \psi_s) = 3^{k+s} = 3^{\frac{s+n-1}{2}},$$

which completes the proof. □

4. Upper bound on the nonlinearity in terms of the cardinality of the Walsh support

Let p be an odd prime. Let $n \geq 2$ be an integer. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an arbitrary p-ary function. In this section we bound N_f in terms of $S = |\mathrm{Supp}\hat{f}|$ by determining the maximal sum of squares of the affine value frequencies. We also characterize equality when $S = p^{n-s}$ with $n - s$ even and when $S = p$.

We first prove the following theorem.

Theorem 4.1. *Let p be an odd prime and let $n \geq 2$ be an arbitrary integer. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an arbitrary p-ary function, and put $S = |\mathrm{Supp}\hat{f}|$. Define*

$$R_{p,S} = \frac{S+p-1}{pS}, \qquad k_{p,S} = \left\lfloor \frac{pS}{S+p-1} \right\rfloor$$

and

$$\mu_{p,S} = \frac{k_{p,S} + \sqrt{k_{p,S}((k_{p,S}+1)R_{p,S}-1)}}{k_{p,S}(k_{p,S}+1)} - \frac{1}{p}.$$

Then

$$N_f \leq \left\lfloor (p-1)p^{n-1} - p^n \mu_{p,S} \right\rfloor, \tag{21}$$

where $\lfloor \cdot \rfloor$ is the floor function on $\mathbb{R}$. Moreover, $\mu_{p,S} = 1/(p\sqrt{S})$ when $S \geq (p-1)^2$, whereas $\mu_{p,S} > 1/(p\sqrt{S})$ when $S < (p-1)^2$.

Proof. In the proof we use some methods of [10] and [11]. For $\alpha \in \mathbb{F}_{p^n}$ and $b \in \mathbb{F}_p$, let $\ell_{\alpha,b}$ be the affine function defined as $\ell_{\alpha,b}(x) = \mathrm{Tr}(\alpha x) + b$, where $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the trace map. Recall that $d_{\mathrm{H}}(f, \ell_{\alpha,b})$ is the Hamming distance between f and the affine map $\ell_{\alpha,b}$. Let $\delta_f^{\alpha,b} \in \mathbb{Q}$ be the rational number defined as

$$\delta_f^{\alpha,b} = \frac{p-1}{p} - \frac{d_{\mathrm{H}}(f, \ell_{\alpha,b})}{p^n}.$$

It is not difficult to observe that

$$N_f = p^{n-1}(p-1) - p^n \max\left\{ \delta_f^{\alpha,b} : \alpha \in \mathbb{F}_{p^n},\ b \in \mathbb{F}_p \right\}. \tag{22}$$

We use the identity [10, Theorem 3]

$$\sum_{\alpha \in \mathbb{F}_{p^n}} \sum_{b \in \mathbb{F}_p} \left(\delta_f^{\alpha,b} \right)^2 = \frac{p-1}{p}.$$

By Proposition 2.1 we see that if $\hat{f}(\alpha) = 0$, then $\delta_f^{\alpha,b} = 0$ for each $b \in \mathbb{F}_p$. It is easy to see that

$$\sum_{b \in \mathbb{F}_p} \delta_f^{\alpha,b} = p - 1 - \frac{1}{p^n} \sum_{b \in \mathbb{F}_p} d_{\mathrm{H}}(f, \ell_{\alpha,b}) = p - 1 - \frac{1}{p^n} \sum_{x \in \mathbb{F}_{p^n}} (p-1) = 0$$

for any $\alpha \in \mathbb{F}_{p^n}$.

The numbers $\delta_f^{\alpha,b}$ satisfy the following two conditions and, as noted above, vanish whenever $\alpha \notin \mathrm{Supp}(\hat{f})$:

- Cond 1: $\displaystyle\sum_{\alpha\in\mathbb{F}_{p^n}} \sum_{b\in\mathbb{F}_p} \left(\delta_f^{\alpha,b}\right)^2 = \frac{p-1}{p}.$
- Cond 2: $\displaystyle\sum_{b\in\mathbb{F}_p} \delta_f^{\alpha,b} = 0$ for all $\alpha \in \mathrm{Supp}(\hat{f})$.

We seek a lower bound for

$$\max\{\delta_f^{\alpha,b} : \alpha \in \mathrm{Supp}(\hat{f}),\ \ b \in \mathbb{F}_p\}.$$

We first prove an auxiliary inequality. Let A be a nonnegative real number, and let $(\sigma_b : b \in \mathbb{F}_p)$ be real numbers satisfying $\sum_{b\in\mathbb{F}_p} \sigma_b = 0$ and $\sum_{b\in\mathbb{F}_p} \sigma_b^2 = A(p-1)/p$. Then

$$\max_b \sigma_b \geq \frac{\sqrt{A}}{p}. \tag{23}$$

If $A = 0$, all the σ_b are zero and the assertion is clear. Assume that $A > 0$, and put $M = \max_b \sigma_b$ and $P = \sum_{b:\,\sigma_b>0} \sigma_b$. Since the sum of the σ_b is zero, both positive and negative terms occur. There are therefore at most $p-1$ positive terms, each at most M, and hence $P \leq (p-1)M$. Moreover,

$$\sum_{b:\,\sigma_b>0} \sigma_b^2 \leq MP, \qquad \sum_{b:\,\sigma_b<0} \sigma_b^2 \leq \left(\sum_{b:\,\sigma_b<0} (-\sigma_b)\right)^2 = P^2.$$

Consequently,

$$A\frac{p-1}{p} \leq MP + P^2 \leq p(p-1)M^2.$$

This proves (23). When $A > 0$, equality requires equality in all the estimates above. In particular, $P = (p-1)M$, so there must be $p-1$ positive terms, all equal to M. Equality in the estimate for the negative terms requires exactly one negative term, which is then $-P = -(p-1)M$. Thus, for $A > 0$, equality in (23) holds if and only if, up to a permutation,

$$\sigma_c = -\frac{p-1}{p}\sqrt{A} \ \text{ for exactly one } c \in \mathbb{F}_p, \text{ and } \ \sigma_b = \frac{\sqrt{A}}{p} \ \text{ for } b \neq c. \tag{24}$$

The converse follows by direct substitution.

For $\alpha \in \mathrm{Supp}(\hat{f})$ define A_α by $\sum_{b\in\mathbb{F}_p} (\delta_f^{\alpha,b})^2 = A_\alpha(p-1)/p$. Cond 1 and the vanishing off the Walsh support give $\sum_{\alpha\in\mathrm{Supp}(\hat{f})} A_\alpha = 1$. Since the support has S elements, some $A_\alpha \geq 1/S$, and (23) yields

$$\max\{\delta_f^{\alpha,b} : \alpha \in \mathrm{Supp}(\hat{f}),\ \ b \in \mathbb{F}_p\} \geq \frac{1}{p\sqrt{S}}.$$

To refine this estimate, put

$$L_{\alpha,b} = |\{x \in \mathbb{F}_{p^n} : f(x) - \mathrm{Tr}(\alpha x) = b\}|, \qquad \rho_{\alpha,b} = \frac{L_{\alpha,b}}{p^n}.$$

For each α, the numbers $(\rho_{\alpha,b} : b \in \mathbb{F}_p)$ are nonnegative and $\sum_{b\in\mathbb{F}_p} \rho_{\alpha,b} = 1$. Thus they form a probability vector. We also have $\delta_f^{\alpha,b} = \rho_{\alpha,b} - 1/p$ and

$$\sum_{b\in\mathbb{F}_p} (\delta_f^{\alpha,b})^2 = \sum_{b\in\mathbb{F}_p} \rho_{\alpha,b}^2 - \frac{1}{p}.$$

Let

$$M = \max_{\alpha,b} \delta_f^{\alpha,b}, \qquad U = \frac{1}{p} + M = \max_{\alpha,b} \rho_{\alpha,b}.$$

Cond 1 and the zero row sums imply that $M > 0$, while $\rho_{\alpha,b} \leq 1$ gives $U \leq 1$. Hence $1/p < U \leq 1$.

Consider any p nonnegative real numbers $(r_b : b \in \mathbb{F}_p)$ such that $\sum_{b\in\mathbb{F}_p} r_b = 1$ and $r_b \leq U$ for every b. Put $j = \lfloor 1/U \rfloor$. Thus $j \in \{1, \ldots, p-1\}$ and $jU \leq 1 < (j+1)U$. Consequently, j is the largest possible number of coordinates r_b that can simultaneously equal the upper bound U. We claim that

$$\sum_{b\in\mathbb{F}_p} r_b^2 \leq jU^2 + (1 - jU)^2. \tag{25}$$

Indeed, suppose that two entries $a \geq c$ lie strictly between 0 and U. Replacing them by $a + t$ and $c - t$, where $t = \min\{U - a, c\}$, preserves all the conditions and increases the sum of squares by $2t(a - c) + 2t^2 > 0$. Repeating this operation leaves at most one entry strictly between 0 and U. The resulting vector has, up to a permutation, j entries U, one further entry $1 - jU$ when this is positive, and zeros elsewhere. This proves the claim and also gives the case of equality.

We now define a real function Φ_p on $[1/p, 1]$. Put $\Phi_p(1/p) = 1/p$, and, for $j = 1, \ldots, p-1$, put

$$\Phi_p(U) = jU^2 + (1 - jU)^2 \qquad \text{if} \qquad \frac{1}{j+1} \leq U \leq \frac{1}{j}.$$

The formulas on two adjacent intervals have the same value at their common endpoint. Moreover, in the interior of the j-th interval,

$$\Phi_p'(U) = 2j((j+1)U - 1) > 0.$$

Hence Φ_p is continuous and strictly increasing on $[1/p, 1]$. Since every $\rho_{\alpha,b} \le U$, the preceding estimate gives, for each $\alpha \in \mathrm{Supp}(\hat{f})$,

$$\sum_{b\in\mathbb{F}_p} (\delta_f^{\alpha,b})^2 \le \Phi_p(U) - \frac{1}{p}.$$

Summing over the Walsh support and using Cond 1 and the vanishing outside the support, we obtain

$$\frac{p-1}{p} = \sum_{\alpha\in\mathrm{Supp}(\hat{f})} \sum_{b\in\mathbb{F}_p} (\delta_f^{\alpha,b})^2 \le S\left(\Phi_p(U) - \frac{1}{p}\right), \qquad \text{and hence} \qquad \Phi_p(U) \ge R_{p,S}.$$

Put $k = k_{p,S} = \lfloor 1/R_{p,S} \rfloor$. Then $1/(k+1) < R_{p,S} \le 1/k$. Since Φ_p is strictly increasing, the equation $\Phi_p(u) = R_{p,S}$ has a unique solution in $[1/(k+1), 1/k]$. Solving the corresponding quadratic equation gives

$$u = \frac{k + \sqrt{k((k+1)R_{p,S} - 1)}}{k(k+1)}.$$

Since Φ_p is strictly increasing, $\Phi_p(U) \ge R_{p,S}$ gives $U \ge u$. Therefore $M = U - 1/p \ge \mu_{p,S}$. The bound follows from (22) and the fact that N_f is an integer.

If $S \ge (p-1)^2$, then $k_{p,S} = p-1$, and substitution gives $\mu_{p,S} = 1/(p\sqrt{S})$. For $S < (p-1)^2$, put $U_0 = 1/p + 1/(p\sqrt{S})$. Suppose that $\Phi_p(U_0) \ge R_{p,S}$. Let $q = (1/p : b \in \mathbb{F}_p)$ and put $j_0 = \lfloor 1/U_0 \rfloor$. Choose $r^* = (r_b^* : b \in \mathbb{F}_p)$ with j_0 entries equal to U_0, one entry equal to $1 - j_0 U_0$, and all remaining entries zero. Its entries lie in $[0, U_0]$, sum to one, and $\sum_{b\in\mathbb{F}_p} (r_b^*)^2 = \Phi_p(U_0)$. On the segment $r(t) = (1-t)q + tr^*$, $t \in [0,1]$, all entries are nonnegative and at most U_0, and their sum is one. Since

$$\sum_{b\in\mathbb{F}_p} q_b^2 = \frac{1}{p} < R_{p,S} \le \sum_{b\in\mathbb{F}_p} (r_b^*)^2,$$

continuity gives a point $r = r(t)$ on this segment such that $\sum_{b\in\mathbb{F}_p} r_b^2 = R_{p,S}$. For $\sigma_b = r_b - 1/p$ we then have

$$\sum_{b\in\mathbb{F}_p} \sigma_b^2 = R_{p,S} - \frac{1}{p} = \frac{p-1}{pS}, \qquad \max_b \sigma_b \le U_0 - \frac{1}{p} = \frac{1}{p\sqrt{S}}.$$

Inequality (23), applied with $A = 1/S$, gives $\max_b \sigma_b \ge 1/(p\sqrt{S})$ and therefore forces equality. Consequently (24) gives, for some c, $r_c = 1/p - (p-1)/(p\sqrt{S}) < 0$, where the strict inequality follows from $S < (p-1)^2$. This contradicts $r_c \ge 0$. Hence $\Phi_p(U_0) < R_{p,S}$, and strict monotonicity gives $\mu_{p,S} > 1/(p\sqrt{S})$. □

For $S = 1$, Theorem 4.1 gives $N_f = 0$. For a bent function, $S = p^n$, so the theorem recovers the known bound $N_f \le \lfloor (p-1)p^{n-1} - p^{n/2-1} \rfloor$. For $S \ge (p-1)^2$, the bound in Theorem 4.1 reduces to $N_f \le \lfloor (p-1)p^{n-1} - p^{n-1}/\sqrt{S} \rfloor$. For $S < (p-1)^2$, its explicit general form is a strict refinement of this estimate.

If $S = p^{n-s}$ and $n-s$ is positive and even, then $S \geq p^2 > (p-1)^2$, so $\mu_{p,S} = 1/(p\sqrt{S})$. Under this assumption, the next theorem characterizes equality in the bound from Theorem 4.1.

Theorem 4.2. *Let p be an odd prime and let $n \geq 2$ be an arbitrary integer. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a p-ary function and let S be the cardinality $|\mathrm{Supp}\hat{f}|$. Assume further that $S = p^{n-s}$ for an integer $0 \leq s \leq n-1$ with $n-s$ even. Then*

$$N_f = (p-1)p^{n-1} - \frac{p^{n-1}}{p^{(n-s)/2}}$$

if and only if there exists a p-ary function $f^* : \mathrm{Supp}(\hat{f}) \to \mathbb{F}_p$ such that

$$\hat{f}(\alpha) = -p^{\frac{n+s}{2}} \epsilon_p^{f^*(\alpha)} \quad \text{for all } \alpha \in \mathrm{Supp}(\hat{f}). \tag{26}$$

In particular, in this case f is a weakly regular s-plateaued function.

Proof. Using $L_{\alpha,b}$, $\rho_{\alpha,b}$, and A_α from the proof of Theorem 4.1, we have

$$\delta_f^{\alpha,b} = \rho_{\alpha,b} - \frac{1}{p}, \qquad \hat{f}(\alpha) = p^n \sum_{b \in \mathbb{F}_p} \delta_f^{\alpha,b} \epsilon_p^b. \tag{27}$$

Assume first that $N_f = (p-1)p^{n-1} - \frac{p^{n-1}}{S^{1/2}}$. By (22) this means that $\max\{\delta_f^{\alpha,b}\} = \frac{1}{pS^{1/2}}$. Let $\alpha \in \mathrm{Supp}(\hat{f})$ be arbitrary. Using (23) we obtain $\frac{\sqrt{A_\alpha}}{p} \leq \max_b \delta_f^{\alpha,b} \leq \frac{1}{pS^{1/2}}$ and hence $A_\alpha \leq \frac{1}{S}$. As $\sum_{\alpha \in \mathrm{Supp}(\hat{f})} A_\alpha = 1$ and $|\mathrm{Supp}(\hat{f})| = S$, we conclude that $A_\alpha = \frac{1}{S}$ for all $\alpha \in \mathrm{Supp}(\hat{f})$ and that equality holds in (23) for each such α. By (24) there exists a uniquely determined $c(\alpha) \in \mathbb{F}_p$ with

$$\delta_f^{\alpha,c(\alpha)} = -\frac{p-1}{pS^{1/2}} \text{ and } \delta_f^{\alpha,b} = \frac{1}{pS^{1/2}} \text{ for } b \neq c(\alpha).$$

Substituting these values into (27) and using $\sum_{b \in \mathbb{F}_p} \epsilon_p^b = 0$ gives

$$\hat{f}(\alpha) = -\frac{p^n}{S^{1/2}} \epsilon_p^{c(\alpha)} = -p^{\frac{n+s}{2}} \epsilon_p^{c(\alpha)}.$$

This is (26) with $f^* = c$.

Conversely, assume that (26) holds and let $\alpha \in \mathrm{Supp}(\hat{f})$. Combining (26) and (27), and using $p^{\frac{n+s}{2}} = \frac{p^n}{S^{1/2}}$, we obtain $\sum_{b \in \mathbb{F}_p} \left(\delta_f^{\alpha,b} + \frac{1}{S^{1/2}} \lambda_b\right) \epsilon_p^b = 0$, where $\lambda_b = 1$ if $b = f^*(\alpha)$ and $\lambda_b = 0$ otherwise. By Proposition 2.1 all the coefficients are equal to some constant, and summing them over $b \in \mathbb{F}_p$ and using Cond 2 we see that this constant is $\frac{1}{pS^{1/2}}$. Hence $\delta_f^{\alpha,f^*(\alpha)} = -\frac{p-1}{pS^{1/2}}$ and $\delta_f^{\alpha,b} = \frac{1}{pS^{1/2}}$ for $b \neq f^*(\alpha)$. As $\delta_f^{\alpha,b} = 0$ for $\alpha \notin \mathrm{Supp}(\hat{f})$, we obtain $\max\{\delta_f^{\alpha,b}\} = \frac{1}{pS^{1/2}}$, and (22) gives $N_f = (p-1)p^{n-1} - \frac{p^{n-1}}{S^{1/2}}$.

Finally, $n-s$ even implies that $n+s$ is even, and hence $\nu_{n+s} = 1$. Equation (26) shows that $|\hat{f}(\alpha)|$ is either $p^{\frac{n+s}{2}}$ or 0, and that the Walsh sign function δ_f from Section 2 is constant on $\mathrm{Supp}(\hat{f})$. Hence f is a weakly regular s-plateaued function. □

We now consider the case $S = p$, which is not covered by Theorem 4.2.

Theorem 4.3. *Let p be an odd prime and let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ satisfy $|\mathrm{Supp}(\hat{f})| = p$. Then*

$$N_f \le (p-2)p^{n-1}.$$

The bound is best possible and is attained by a quadratic $(n-1)$-plateaued function.

Proof. For $S = p$, the quantities in Theorem 4.1 satisfy $k_{p,p} = (p-1)/2$ and $\mu_{p,p} = 1/p$. The asserted upper bound therefore follows from (21).

For sharpness choose trace-dual $\mathbb{F}_p$-bases and write $\alpha = (\alpha_1, \dots, \alpha_n)$ and $x = (x_1, \dots, x_n)$, so that $\mathrm{Tr}(\alpha x) = \sum_j \alpha_j x_j$. Set $f(x) = x_1^2$. If $G_p = \sum_{t \in \mathbb{F}_p} \epsilon_p^{t^2}$, then separating the variables and completing the square gives

$$\hat{f}(\alpha) = \begin{cases} p^{n-1} G_p \epsilon_p^{-\alpha_1^2/4}, & \text{if } \alpha_2 = \cdots = \alpha_n = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Thus $|\mathrm{Supp}(\hat{f})| = p$ and, since $|G_p| = \sqrt{p}$, the function is $(n-1)$-plateaued.

An affine function involving one of $x_2, \dots, x_n$ agrees with f at exactly p^{n-1} points; otherwise the agreement equation has at most two roots in x_1. The constant function 1 attains $2p^{n-1}$ agreements. Hence

$$N_f = p^n - 2p^{n-1} = (p-2)p^{n-1},$$

as required. □

We also characterize equality in Theorem 4.3.

Theorem 4.4. *Let p be an odd prime and let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ satisfy $|\mathrm{Supp}(\hat{f})| = p$. Equality $N_f = (p-2)p^{n-1}$ holds if and only if, for every $\alpha \in \mathrm{Supp}(\hat{f})$, the multiset $(L_{\alpha,b} : b \in \mathbb{F}_p)$ is*

$$\underbrace{2p^{n-1}, \dots, 2p^{n-1}}_{(p-1)/2}, \quad p^{n-1}, \quad \underbrace{0, \dots, 0}_{(p-1)/2}.$$

Here $L_{\alpha,b}$ is defined in the proof of Theorem 4.1. When $p = 3$, every function attaining equality is $(n-1)$-plateaued.

Proof. Put $m = (p-1)/2$ and retain the notation $\rho_{\alpha,b} = L_{\alpha,b}/p^n$ from the proof of Theorem 4.1. If equality holds, then (22) gives $\max_{\alpha,b} \rho_{\alpha,b} = 2/p$. For each α in the Walsh support, (25), applied with $U = 2/p$ and $j = m$, gives

$$\sum_b \rho_{\alpha,b}^2 \le m \left(\frac{2}{p}\right)^2 + \left(\frac{1}{p}\right)^2 = \frac{2p-1}{p^2}.$$

For a support point, the corresponding contribution to the identity in Cond 1 in the proof of Theorem 4.1 is at most $(2p-1)/p^2 - 1/p = (p-1)/p^2$. Since the p support

points together contribute $(p-1)/p$, equality must hold for every support point. The equality case is, up to a permutation, m entries $2/p$, one entry $1/p$, and m zero entries. Multiplying by p^n gives the stated profile.

Conversely, the stated profiles give $\max_b \rho_{\alpha,b} = 2/p$ on the Walsh support. Off the support, Proposition 2.1 gives $\rho_{\alpha,b} = 1/p$ for every b, and hence $\max_{\alpha,b} \rho_{\alpha,b} = 2/p$. Equation (22) then gives $N_f = (p-2)p^{n-1}$. If $p = 3$, every nonzero Walsh coefficient has the form $3^{n-1}(2\epsilon_3^a + \epsilon_3^b)$ with $a \neq b$. Its modulus is $3^{n-1/2}$, which proves the last assertion. □

Remark 4.1. *None of Theorems 4.1–4.4 assumes plateauedness. Theorems 4.1 and 4.3 give bounds for arbitrary p-ary functions under Walsh-support cardinality conditions, while Theorems 4.2 and 4.4 characterize equality. The rank-one quadratic in Theorem 4.3 is a plateaued sharpness witness. Equality in Theorem 4.2 implies plateauedness; when $p = 3$, the same conclusion holds for equality in Theorem 4.3 by Theorem 4.4.*

For $p \geq 5$, however, support cardinality p does not force plateauedness. Indeed, for any $n \geq 1$, let $L(x_1, \ldots, x_n) = x_1 + \cdots + x_n$ and set $f(x) = L(x)^{p-1}$. This function depends on all n coordinates. In trace-dual bases, as in the proof of Theorem 4.3, its Walsh transform is supported on the one-dimensional frequency subspace

$$(\ker L)^{\perp} = \{t(1, \ldots, 1) : t \in \mathbb{F}_p\},$$

which contains p frequency vectors. On this subspace its values are

$$p^{n-1}(1 + (p-1)\epsilon_p) \quad \textit{at the zero frequency,} \qquad p^{n-1}(1 - \epsilon_p) \quad \textit{elsewhere.}$$

The two magnitudes are different, so f is not plateaued.

5. Conclusion

We obtained a lower bound on the distance between two distinct s-plateaued functions in odd characteristic and a separate bent bound. The expressions inside the ceilings agree for $p = 3$; for $p > 3$, the bent expression is strictly larger. Proposition 3.1 gives equality for the stated ternary family.

Theorem 4.1 gives a new explicit upper bound on the nonlinearity of a p-ary function in terms of the cardinality of its Walsh support. For $S \geq (p-1)^2$, it reduces to $N_f \leq \lfloor (p-1)p^{n-1} - p^{n-1}/\sqrt{S} \rfloor$. For $S < (p-1)^2$, Theorem 4.1 gives a strict refinement of this estimate. For support cardinality p, the sharp consequence is $N_f \leq (p-2)p^{n-1}$. We also characterized equality when the support cardinality is p^{n-s} and $n-s$ is even, and we determined the exact affine value-distribution profiles for equality in the sharp support-p estimate.

Declarations

Availability of data and materials Not applicable.

Competing interests Not applicable.

Funding The research of Ferruh Özbudak is supported by Sabancı University Research Grants (F.A.CF-24-02904 and B.A.CF-24-02881).

Authors' contributions Not applicable.

Acknowledgements The authors thank the handling editor and the anonymous reviewers for their useful comments and suggestions, which helped improve the manuscript.

Authors' information Not applicable.

References

[1] C. Carlet. *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, Cambridge, 2021.

[2] A.Çesmelioğlu, W. Meidl and A. Pott. Generalized Maiorana-McFarland class and normality of p-ary bent functions. *Finite Fields and Their Applications*, vol. 24, pp. 105–117, 2013.

[3] N.A. Kolomeets, "Enumeration of the bent functions of least deviation from a quadratic bent function", *J. Appl. Ind. Math.*, vol.6(3), 2012, pp. 306-317.

[4] N. Kolomeec, "The graph of minimal distances of bent functions and its properties", *Designs, Codes, and Cryptography*, vol.85(3), 2017, pp. 395-410.

[5] S. Mesnager. *Bent Functions. Fundamentals and Results*, Springer International Publishing, 2016.

[6] F. Özbudak, R. M. Pelen, " Duals of non-weakly regular bent functions are not weakly regular and generalization to plateaued functions", Finite Fields Appl. 64 (2020), 101668, 16 pp.

[7] V. N. Potapov, "Cardinality spectra of components of correlation immune functions, bent functions, perfect colorings, and codes", *Problems of Inform. Transmission*, vol.48(1), 2012, pp. 47-55.

[8] V. N. Potapov, "On q-ary bent and plateaued functions", Designs, Codes, and Cryptography, (2020) 88 (10), pp. 2037-2049.

[9] V. N. Potapov, F. Özbudak, Asymptotic bounds on the numbers of certain bent functions, *Cryptography and Communications*, vol.16(6), 2024, pp.1289–1307.

[10] V. G. Ryabov, "Approximation of restrictions of q-valued logic functions to linear manifolds by affine analogues", Diskr. Mat., 32:4 (2020), 89-102; Discrete Math. Appl., 31:6 (2021), 409-419

[11] V. G. Ryabov, "Criteria for maximal nonlinearity of a function over a finite field", Diskr. Mat., 33:3 (2021), 79-91; Discrete Math. Appl., 33:2 (2023), 117-126

[12] K.-U. Schmidt, "Highly nonlinear functions over finite fields", Finite Fields Appl. 63 (2020), 101640, 19 pp.

[13] T. Tao, "An uncertainty principle for cyclic groups of prime order", *Math. Res. Lett.*, vol.12(1), 2005, pp. 121-127.

[14] Y.V. Tarannikov, "Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters", *Sib. Elektron. Mat. Izv.*, vol.11, 2014, pp. 229-245.