A Family of p-ary Binomial Bent Functions

Dabin Zheng[1,2*] Xiangyong Zeng[1] Lei Hu[2]

1 Faculty of Mathematics and Computer Science,
Hubei University, Wuhan 430062, China

2 State Key Laboratory of Information Security,
Graduate School of Chinese Academy of Sciences, Beijing 100049, China

Abstract

For a prime p with $p \equiv 3 \pmod 4$ and an odd number m, the Bentness of the p-ary binomial function $f_{a,b}(x) = \mathrm{Tr}_1^n(ax^{p^m-1}) + \mathrm{Tr}_1^2(bx^{\frac{p^n-1}{4}})$ is characterized, where $n = 2m$, $a \in \mathbb{F}_{p^n}^*$, and $b \in \mathbb{F}_{p^2}^*$. The necessary and sufficient conditions of $f_{a,b}(x)$ being Bent are established respectively by an exponential sum and two sequences related to a and b. For the special case of $p = 3$, we further characterize the Bentness of the ternary function $f_{a,b}(x)$ by the Hamming weight of a sequence.

Key Words p-ary Binomial Bent functions Exponential sum Hamming weight

1 Introduction

Nonlinearity is an important cryptographic criteria for the Boolean functions used in symmetric ciphers [1]. The nonlinearity of a Boolean function is the distance between it and the set of affine functions. Bent functions, introduced by Rothaus [18], are ones of the most famous Boolean functions since they achieve the upper bound on nonlinearity. Highly nonlinear functions including Bent functions have been extensively applied to cryptography, sequences and coding theory [1, 2, 10]. The concept of Bent function is also generalized to more general notations such as generalized Bent functions [2, 6, 9, 12, 13, 19]. People have paid lots of attention to this topic, however, the complete classification of Bent functions is still hopeless. Some research

[*] Corresponding author E-mail address: zhengdabin@mmrc.iss.ac.cn

of Bent functions focuses on monomial functions, binomial functions, and quadratic functions [1, 4, 5, 8, 14].

For a prime p and a positive integer n, let $\mathbb{F}_{p^n}$ be the finite field with p^n elements, $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$, and $\mathrm{Tr}_1^n(\cdot)$ is the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. For $p = 2$ and an even number $n = 2m$, Dillon [7] established that the monomial Boolean function defined by

$$f_a(x) = \mathrm{Tr}_1^n(ax^d), \quad a \in \mathbb{F}_{2^m}$$

is Bent if and only if the Kloosterman sum satisfies $K(\chi_1, a, 0) = -1$, where the exponent is $d = 2^m - 1$, χ_1 is the canonical additive character of $\mathbb{F}_{p^n}$, and the Kloosterman sum [15] is defined as

$$K(\chi, a, b) = \sum_{x \in \mathbb{F}_{p^n}^*} \chi(ax + bx^{-1}), \quad a,\ b \in \mathbb{F}_{p^n}.$$

This result is generalized by Charpin and Gong to $d = r(2^m - 1)$ for any integer r coprime with $2^m + 1$ [3] and by Helleseth and Kholosha to fields of odd characteristic [11].

Recently, Mesnager characterized the Bentness of the binary Boolean function

$$\mathrm{Tr}_1^n(ax^{2^{n/2}-1}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}}),\ \ a \in \mathbb{F}_{2^n},\ \ b \in \mathbb{F}_4 \tag{1}$$

for even n in terms of the Kloosterman sums of the coefficients a and b [17]. Different from most previous constructions, the coefficient b here shall be restricted in a subfield $\mathbb{F}_4$ of $\mathbb{F}_{2^n}$. In this paper, following the line of Mesnager's work, we consider the analogy problem for the odd p-ary function $f_{a,b} : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$ defined by

$$f_{a,b}(x) = \mathrm{Tr}_1^n(ax^{p^m-1}) + \mathrm{Tr}_1^2(bx^{\frac{p^n-1}{4}}),\ \ a \in \mathbb{F}_{p^n}^*,\ \ b \in \mathbb{F}_{p^2}^* \tag{2}$$

where m is odd, $n = 2m$, and p is odd with $p \equiv 3 \pmod 4$. In analogy with the binary case, we first characterize the Bentness of the function (2) in terms of an exponential sum over a subset of $\mathbb{F}_{p^n}$. For a further characterization of the exponential sum, however, the method of Mesnager can not continue to work here since it needs to divide this subset into four parts but the exponential sum can not be evaluated over each part as in [17]. To this end, we characterize the Bentness by two sequences defined by $\mathrm{Tr}_1^n(ax^{p^m-1})$ and $\mathrm{Tr}_1^2(bx^{\frac{p^n-1}{4}})$. Finally, for the special case of $p = 3$, we further characterize the Bentness of the ternary function $f_{a,b}(x)$ by the Hamming weight of a sequence.

The rest of this paper is organized as follows. In Section 2, we recall some necessary preliminaries and present the main results. In Section 3, the main theorems are proved and examples of ternary binomial Bent functions are presented.

2 Preliminaries and Main Theorems

For two positive integers k and n with $k\,|\,n$, the *trace function* from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^k}$ [15] is defined as

$$\mathrm{Tr}_k^n(x)=\sum_{i=0}^{n/k-1} x^{p^{ki}},\quad x\in\mathbb{F}_{p^n}.$$

The *Walsh transform* of a function $f:\mathbb{F}_{p^n}\longrightarrow\mathbb{F}_p$ is defined by

$$\hat{f}(\lambda)=\sum_{x\in\mathbb{F}_{p^n}}\omega^{f(x)-\mathrm{Tr}_1^n(\lambda x)},\quad \lambda\in\mathbb{F}_{p^n}$$

where $\omega=e^{\frac{2\pi\sqrt{-1}}{p}}$ is a primitive p-th complex root of unity. For an odd prime p, f is called a *p-ary Bent function* if $|\hat{f}(\lambda)|=p^{\frac{n}{2}}$ for all $\lambda\in\mathbb{F}_{p^n}$ [13]. A Bent function $f(x)$ is called *regular* if for every $\lambda\in\mathbb{F}_{p^n}$ the normalized Walsh coefficients $p^{-\frac{n}{2}}\hat{f}(\lambda)$ equals to a complex p-th root of unity, that is, $p^{-\frac{n}{2}}\hat{f}(\lambda)=\omega^{f^*(\lambda)}$ for some function $f^*:\mathbb{F}_{p^n}\longrightarrow\mathbb{F}_p$. A binary Bent function is always regular. For odd p, a p-ary Bent function $f(x)$ may not be regular, but its Walsh transform coefficients satisfy

$$\hat{f}(\lambda)=\begin{cases}\pm\,\omega^{f^*(\lambda)}p^{\frac{n}{2}}, & \text{if } p^n\equiv 1 \pmod 4,\\ \pm\,\epsilon\,\omega^{f^*(\lambda)}p^{\frac{n}{2}}, & \text{if } p^n\equiv 3 \pmod 4\end{cases}\tag{3}$$

where ϵ is a complex primitive forth root of unity (please see Property 8 of [13]).

Assume $n=2m$ is even. For any $x\in\mathbb{F}_{p^n}$, denote $\bar{x}=x^{p^m}$. Let G be a subgroup of the multiplicative group $\mathbb{F}_{p^n}^*$ defined by

$$G=\Big\{x\in\mathbb{F}_{p^n}:x\bar{x}=1\Big\},$$

i.e., G is the group of elements in $\mathbb{F}_{p^n}$ of order dividing p^m+1. G is sometimes called the unit circle of $\mathbb{F}_{p^n}^*$. Let γ be a primitive element of $\mathbb{F}_{p^n}$. For each $0\le i\le p^n-2$, the element γ^i of $\mathbb{F}_{p^n}^*$ can be written as $\gamma^{(p^m+1)k}\cdot\gamma^l$, where $0\le l\le p^m$ and $0\le k\le p^m-2$. As a consequence, we have the following

Lemma 2.1 *For a prime p, the multiplicative group $\mathbb{F}_{p^n}^*$ can be decomposed to the Cartesian product*

$$\mathbb{F}_{p^n}^* = \mathbb{F}_{p^m}^* \times V$$

where $V = \left\{1, \gamma, \gamma^2, \cdots, \gamma^{p^m}\right\}$ and γ is a primitive element of $\mathbb{F}_{p^n}$.

In the sequel, we always assume that p is odd and $n = 2m$ for some integer m such that $p^m > 3$ and $p^m \equiv 3 \pmod 4$, i.e., $p^m > 3$, $p \equiv 3 \pmod 4$, and m is odd. To characterize the Bentness of the function $f_{a,b}(x)$ defined in (2), we define an exponential sum over the subset V as follows:

$$S_{a,b} := \sum_{v \in V} \omega^{f_{a,b}(v)} = \sum_{i=0}^{p^m} \omega^{\mathrm{Tr}_1^n\left(a\gamma^{(p^m-1)i}\right)} \omega^{\mathrm{Tr}_1^2\left(b\gamma^{\frac{p^n-1}{4}i}\right)}. \tag{4}$$

The main theorems are listed below and their proofs will be given in Section 3.

Theorem 2.2 *The binomial function $f_{a,b}(x)$ in (2) is Bent if and only if*

$$S_{a,b} = 1. \tag{5}$$

Moreover, if (5) holds then $f_{a,b}(x)$ is a regular Bent function and the corresponding Walsh transform coefficient of $f_{a,b}(x)$ is equal to

$$\hat{f}_{a,b}(\lambda) = \begin{cases} p^m \omega^{f_{a,b}(v_\lambda)}, & \text{for } \lambda \in \mathbb{F}_{p^n}^*, \\ p^m, & \text{for } \lambda = 0 \end{cases}$$

where $x = v_\lambda$ is the unique solution in V of $\lambda x + \lambda^{p^m} x^{p^m} = 0$ for $\lambda \in \mathbb{F}_{p^n}^*$.

Theorem 2.2 provides a characterization for Bentness of $f_{a,b}(x)$, however, it is still difficult to compute the exponential sum $S_{a,b}$. In order to find an alternative characterization for $S_{a,b} = 1$, from the last expression in (4) we consider two sequences $\{a_i\}_{i=0}^{p^m}$ and $\{b_i\}_{i=0}^{p^m}$ defined by

$$a_i = \mathrm{Tr}_1^n\left(a\gamma^{(p^m-1)i}\right), \ b_i = \mathrm{Tr}_1^2\left(b\gamma^{\frac{p^n-1}{4}i}\right).$$

It is clear that $p^m + 1$ and 4 are their periods respectively. Let

$$\mathcal{I} = \left\{0, 1, 2, \ldots, \frac{p^m-3}{4}\right\}$$

for $p^m \equiv 3 \pmod 8$ and

$$\mathcal{J} = \left\{0, 1, 2, \ldots, \frac{p^m-7}{8}\right\}$$

for $p^m \equiv 7 \pmod 8$, respectively. Then we have

Theorem 2.3 *The following statements hold:*

1. *If* $p^m \equiv 3 \pmod 8$ *then the function* $f_{a,b}(x)$ *in (2) is Bent if and only if*

$$\sum_{i\in\mathcal{I}} \left(cos\frac{2\pi(b_0 + a_{4i})}{p} + cos\frac{2\pi(b_1 + a_{4i+1})}{p} \right) = \frac{1}{2}. \qquad (6)$$

2. *If* $p^m \equiv 7 \pmod 8$ *then the function* $f_{a,b}(x)$ *in (2) is Bent if and only if*

$$\begin{cases} cos\frac{2\pi b_0}{p} \sum\limits_{i\in\mathcal{I}} cos\frac{2\pi a_{2i}}{p} + cos\frac{2\pi b_1}{p} \sum\limits_{i\in\mathcal{I}} cos\frac{2\pi a_{2i+1}}{p} = \frac{1}{2}, \\ sin\frac{2\pi b_0}{p} \sum\limits_{i\in\mathcal{J}} \left(cos\frac{2\pi a_{4i}}{p} - cos\frac{2\pi a_{4i+2}}{p} \right) + \\ \qquad\qquad sin\frac{2\pi b_1}{p} \sum\limits_{i\in\mathcal{J}} \left(cos\frac{2\pi a_{4i+1}}{p} - cos\frac{2\pi a_{4i+3}}{p} \right) = 0. \end{cases} \qquad (7)$$

In the above two cases, the $f_{a,b}(x)$ *in (2) is a regular Bent function.*

By Theorem 2.3, the Bentness of $f_{a,b}(x)$ is completely determined by subsequences of the sequences $\{a_i\}_{i=0}^{p^m}$ and $\{b_i\}_{i=0}^{p^m}$. In particular, for $p = 3$, let

$$s = (b_0 + a_0, b_1 + a_1, b_0 + a_4, b_1 + a_5, \ldots, b_0 + a_{3^m-3}, b_1 + a_{3^m-2}) \in \mathbb{F}_3^{\frac{3^m+1}{2}},$$

that is, s is a subsequence of the sequence $\{a_i + b_i\}_{i=0}^{3^m}$ consisting of its $0, 1, 4, 5, \cdots, 3^m - 3, (3^m - 2)$-th entries. Let $\mathrm{Wt}(s)$ be the Hamming weight of s. Then we have

Corollary 2.4 *Let* $p = 3$ *and* m *be an odd integer. The function* $f_{a,b}(x)$ *in (2) is Bent if and only if*

$$Wt(s) = 3^{m-1}.$$

In this case, the $f_{a,b}(x)$ *in (2) is a regular Bent function.*

3 The Bentness of p-ary Binomial Functions

In this section, we will finish the proofs of Theorem 2.2 and 2.3.

We first analyze the properties of the function $f_{a,b}(x)$ in (2) and use them to calculate the Walsh spectra of $f_{a,b}(x)$.

By Lemma 2.1, any $x \in \mathbb{F}_{p^n}^*$ can be uniquely expressed as yv for $y \in \mathbb{F}_{p^m}^*$ and $v \in V$. Then we have

$$\begin{aligned}
f_{a,b}(x) &= f_{a,b}(yv) \\
&= \mathrm{Tr}_1^n\left(av^{p^m-1}y^{p^m-1}\right) + \mathrm{Tr}_1^2\left(bv^{\frac{p^n-1}{4}}y^{\frac{p^n-1}{4}}\right) \\
&= \mathrm{Tr}_1^n\left(av^{p^m-1}\right) + \mathrm{Tr}_1^2\left((y^{p^m-1})^{\frac{p^m+1}{4}}bv^{\frac{p^n-1}{4}}\right) \qquad (8) \\
&= \mathrm{Tr}_1^n\left(av^{p^m-1}\right) + \mathrm{Tr}_1^2\left(bv^{\frac{p^n-1}{4}}\right) \\
&= f_{a,b}(v)
\end{aligned}$$

since $p^m \equiv 3 \,(\mathrm{mod}\, 4)$. According to the equality (8), for any $\lambda \in \mathbb{F}_{p^n}$ we have

$$\begin{aligned}
&\hat{f}_{a,b}(\lambda) \\
&= \sum_{x\in\mathbb{F}_{p^n}} \omega^{f_{a,b}(x)-\mathrm{Tr}_1^n(\lambda x)} \\
&= 1 + \sum_{v\in V}\sum_{y\in\mathbb{F}_{p^m}^*} \omega^{f_{a,b}(vy)-\mathrm{Tr}_1^n(\lambda vy)} \\
&= 1 + \sum_{v\in V}\omega^{f_{a,b}(v)} \sum_{y\in\mathbb{F}_{p^m}^*} \omega^{\mathrm{Tr}_1^m\left(-\left(\lambda v+(\lambda v)^{p^m}\right)y\right)} \qquad (9) \\
&= 1 + \sum_{v\in V,\lambda v+(\lambda v)^{p^m}=0} (p^m-1)\omega^{f_{a,b}(v)} - \sum_{v\in V,\lambda v+(\lambda v)^{p^m}\neq 0} \omega^{f_{a,b}(v)} \\
&= 1 + p^m \sum_{v\in V,\lambda v+(\lambda v)^{p^m}=0} \omega^{f_{a,b}(v)} - \sum_{v\in V}\omega^{f_{a,b}(v)}.
\end{aligned}$$

In particular, for $\lambda = 0$ we have

$$\hat{f}_{a,b}(0) = 1 + (p^m-1)S_{a,b}. \qquad (10)$$

For any $\lambda \in \mathbb{F}_{p^n}^*$, we first have

Lemma 3.1 *The equation $\lambda x + \lambda^{p^m}x^{p^m} = 0$ has a unique solution in V.*

Proof Clearly, the mentioned equation has the same nonzero solutions with this equation: $(\lambda x)^{p^m-1} = -1$, whose unique solution is given by $x = \lambda^{-1}\gamma^{(p^m+1)/2}$. □

We denote this solution by v_λ as in Theorem 2.2. By (9), we have

$$\hat{f}_{a,b}(\lambda) = 1 + p^m\omega^{f_{a,b}(v_\lambda)} - S_{a,b}. \qquad (11)$$

Thus, the calculation of $\hat{f}_{a,b}(\lambda)$ is reduced to determining the exponential sum $S_{a,b}$.

With the above preparations, we can prove Theorem 2.2.

Proof of theorem 2.2 Sufficiency. Assume $S_{a,b} = 1$. By equalities (10) and (11) we have

$$\hat{f}_{a,b}(\lambda) = \begin{cases} p^m \omega^{f_{a,b}(v_\lambda)}, & \text{for } \lambda \neq 0, \\ p^m, & \text{for } \lambda = 0. \end{cases}$$

Thus $f_{a,b}(x)$ is a regular Bent function.

Conversely, assume $f_{a,b}(x)$ is a Bent function. Then $|\hat{f}_{a,b}(\lambda)| = p^m$ for any $\lambda \in \mathbb{F}_{p^n}$. We choose a $\lambda \neq 0$. By equality (3), we can assume that $\hat{f}_{a,b}(\lambda) = \pm\,\omega^{k_1} p^m$ for some $0 \leq k_1 \leq p-1$. Moreover, let

$$S_{a,b} = \sum_{v \in V} \omega^{f_{a,b}(v)} = \sum_{i=0}^{p-1} N_i \omega^i$$

where $N_i = \sharp\big\{v \in V \,|\, f_{a,b}(v) = i\big\}$ for $0 \leq i \leq p-1$. We want to prove $N_0 - 1 = N_1 = \cdots = N_{p-1} = p^{m-1}$. If this holds then $S_{a,b} = 1$.

First notice that $N_0 + N_1 + \ldots + N_{p-1} = p^m + 1$. Set $k_2 = f_{a,b}(v_\lambda)$. The equality (11) can be rewritten as

$$(N_0 - 1) + N_1\omega + \cdots + N_{p-1}\omega^{p-1} \pm p^m \omega^{k_1} - p^m \omega^{k_2} = 0. \qquad (12)$$

Suppose merging similar items on the left side of (12) gives

$$a_0 + a_1\omega + \cdots + a_{p-1}\omega^{p-1} = 0.$$

Comparing the sequence of nonnegative integers $\{N_0, N_1, \cdots, N_{p-1}\}$ and the sequence of integers $\{a_0, a_1, \cdots, a_{p-1}\}$, we know there are at least $p-3$ indexes $1 \leq i \leq p-1$ with $a_i = N_i$, and

$$a_0 + a_1 + \cdots + a_{p-1} = (N_0 - 1 + N_1 + \cdots + N_{p-1}) \pm p^m - p^m = \pm p^m.$$

Thus $a_0 = a_1 = \cdots = a_{p-1} = \pm p^{m-1}$ since by Eisenstein's criteria, $x^{p-1} + \cdots + x^2 + x + 1$ is irreducible over the rational numbers, and hence it is the minimal polynomial of ω over the field of rational numbers.

Suppose $\hat{f}_{a,b}(\lambda) = -\omega^{k_1} p^m$, namely the above mentioned "$\pm$" is a negative sign. Then $a_0 = a_1 = \cdots = a_{p-1} = -p^{m-1} < 0$, which happens only when $p = 3$ since otherwise there will be a negative N_i, and in this case we must have $N_0 = 1 - p^{m-1} \leq 0$ and $N_1 = N_2 = p^m - p^{m-1}$, this further happens only when $m = 1$.

Suppose $\hat{f}_{a,b}(\lambda) = \omega^{k_1} p^m$. Then $a_0 = a_1 = \cdots = a_{p-1} = p^{m-1}$. By the relation of two sequences $\{N_0, N_1, \cdots, N_{p-1}\}$ and $\{a_0, a_1, \cdots, a_{p-1}\}$, we can easily learn that $k_1 = k_2$ since otherwise there is some i with $a_i \geq N_i - 1 + p^m \geq p^m - 1 > p^{m-1}$, and hence, $a_0 = N_0 - 1$, and $a_i = N_i$ for $1 \leq i \leq p-1$. Thus, $N_0 - 1 = N_1 = \cdots = N_{p-1} = p^{m-1}$. □

To prove Theorem 2.3, we make the following preparations. Since $\gamma^{\frac{p^n-1}{2}} = -1$, we have

$$b_0 = \mathrm{Tr}_1^2(b), \quad b_1 = \mathrm{Tr}_1^2\left(b\gamma^{\frac{p^n-1}{4}}\right), \quad b_2 = -b_0, \quad b_3 = -b_1.$$

Since $p^m \equiv 3 \pmod 4$, we can decompose the sequence $\{a_i\}_{i=0}^{p^m}$ into corresponding four parts according to values of b_i. So the expression (4) becomes

$$\begin{aligned} S_{a,b} &= \sum_{i=0}^{p^m} \omega^{a_i} \cdot \omega^{b_i} \\ &= \omega^{b_0} \sum_{i\in\mathcal{I}} \omega^{a_{4i}} + \omega^{b_1} \sum_{i\in\mathcal{I}} \omega^{a_{4i+1}} + \omega^{-b_0} \sum_{i\in\mathcal{I}} \omega^{a_{4i+2}} + \omega^{-b_1} \sum_{i\in\mathcal{I}} \omega^{a_{4i+3}} \\ &= \omega^{b_0} S_0 + \omega^{b_1} S_1 + \omega^{-b_0} S_2 + \omega^{-b_1} S_3 \end{aligned} \tag{13}$$

where $S_j = \sum_{i\in\mathcal{I}} \omega^{a_{4i+j}}$ for $j \in \{0,1,2,3\}$.

It can be verified that the sequence $\{a_i\}_{i=0}^{p^m}$ satisfies

$$a_i = \mathrm{Tr}_1^n\left(a\gamma^{(p^m-1)i}\right) = -\mathrm{Tr}_1^n\left(a\gamma^{(p^m-1)(i+\frac{p^m+1}{2})}\right) = -a_{i+\frac{p^m+1}{2}} \tag{14}$$

for any i.

Proof of Theorem 2.3 The condition $p^m \equiv 3 \pmod 4$ is divided into two cases $p^m \equiv 3 \pmod 8$ and $p^m \equiv 7 \pmod 8$.

When $p^m \equiv 3 \pmod 8$, we have $\frac{p^m+1}{2} \equiv 2 \pmod 4$. By the equality (14), for $i \in \mathcal{I}$ and $j \in \{0,1\}$, we have $a_{4i+2+j} = -a_{4(i-(p^m-3)/8)+j}$ since $4i+2 = 4(i-(p^m-3)/8) + (p^m+1)/2$. Thus, the terms $\omega^{a_{4i+j}}$ in the expansion of S_j are one-to-one equal to the terms $\omega^{-a_{4i+j}}$ in the expansion of S_{j+2}, and (13) can be rewritten as

$$\begin{aligned} S_{a,b} &= \left(\omega^{b_0} S_0 + \omega^{-b_0} S_2\right) + \left(\omega^{b_1} S_1 + \omega^{-b_1} S_3\right) \\ &= \sum_{i\in\mathcal{I}} \left(\omega^{b_0+a_{4i}} + \omega^{-(b_0+a_{4i})}\right) + \sum_{i\in\mathcal{I}} \left(\omega^{b_1+a_{4i+1}} + \omega^{-(b_1+a_{4i+1})}\right) \\ &= 2\sum_{i\in\mathcal{I}} \left(cos\frac{2\pi(b_0+a_{4i})}{p} + cos\frac{2\pi(b_1+a_{4i+1})}{p}\right). \end{aligned} \tag{15}$$

As a consequence, $S_{a,b} = 1$ if and only if the equality (6) holds. In this case, by Theorem 2.2, $f_{a,b}(x)$ is regular.

When $p^m \equiv 7 \pmod 8$, we have $\frac{p^m+1}{2} \equiv 0 \pmod 4$. By (14), similarly, the terms $\omega^{a_{4i+k}}$ and $\omega^{-a_{4i+k}}$ are one-to-one correspondence in the expansion of S_k for $i \in \mathcal{J}$ and $k \in \{0,1,2,3\}$. So, the equality (13) becomes

$$\begin{aligned}
S_{a,b} &= \omega^{b_0} S_0 + \omega^{b_1} S_1 + \omega^{-b_0} S_2 + \omega^{-b_1} S_3 \\
&= \omega^{b_0} \sum_{i \in \mathcal{J}} \left(\omega^{a_{4i}} + \omega^{-a_{4i}}\right) + \omega^{b_1} \sum_{i \in \mathcal{J}} \left(\omega^{a_{4i+1}} + \omega^{-a_{4i+1}}\right) \\
&+ \omega^{-b_0} \sum_{i \in \mathcal{J}} \left(\omega^{a_{4i+2}} + \omega^{-a_{4i+2}}\right) + \omega^{-b_1} \sum_{i \in \mathcal{J}} \left(\omega^{a_{4i+3}} + \omega^{-a_{4i+3}}\right) \\
&= 2cos\frac{2\pi b_0}{p} \sum_{i \in \mathcal{I}} cos\frac{2\pi a_{2i}}{p} + 2cos\frac{2\pi b_1}{p} \sum_{i \in \mathcal{I}} cos\frac{2\pi a_{2i+1}}{p} \\
&+ 2\left\{ sin\frac{2\pi b_0}{p} \sum_{i \in \mathcal{J}} \left(cos\frac{2\pi a_{4i}}{p} - cos\frac{2\pi a_{4i+2}}{p} \right) \right. \\
&\left. + sin\frac{2\pi b_1}{p} \sum_{i \in \mathcal{J}} \left(cos\frac{2\pi a_{4i+1}}{p} - cos\frac{2\pi a_{4i+3}}{p} \right) \right\} \sqrt{-1}\ .
\end{aligned}$$

Thus $S_{a,b} = 1$ if and only if the equality (7) holds. □

Finally, for $p = 3$, we have that $a_i, b_j \in \{0,1,2\}$ for $0 \le i \le 3^m, j \in \{0,1\}$, and ω is a primitive 3-th complex root of unity. It is clear that

$$2cos\frac{2\pi(b_j + a_i)}{3} = \begin{cases} 2, & \text{if } b_j + a_i = 0 \pmod 3, \\ -1, & \text{otherwise.} \end{cases} \tag{16}$$

Let $s = (b_0 + a_0, b_1 + a_1, b_0 + a_4, b_1 + a_5, \ldots, b_0 + a_{3^m-3}, b_1 + a_{3^m-2}) \in \mathbb{F}_3^{\frac{3^m+1}{2}}$. From equalities (16) and (15) we have

$$S_{a,b} = -\mathrm{Wt}(s) + 2 \times \left(\frac{3^m+1}{2} - \mathrm{Wt}(s)\right) = 3^m + 1 - 3\mathrm{Wt}(s)\ .$$

Therefore, $S_{a,b} = 1$ if and only if $\mathrm{Wt}(s) = 3^{m-1}$. This finishes the proof of Corollary 2.4.

Remark 3.2 *If $b = 0$ then $f_{a,b}(x)$ is degraded to a monomial function. According to Corollary 2.4, $f_{a,0}$ is a Bent function if and only if the sequence $(a_0, a_1, a_4, a_5, \ldots, a_{3^m-3}, a_{3^m-2}) \in \mathbb{F}_3^{\frac{3^m+1}{2}}$ has the Hamming weight 3^{m-1}, which is Corollary 1 in [11], here the length of the sequence considered is half of that in Corollary 1 in [11].*

Applying Corollary 2.4, with the help of a computer, we can efficiently determine whether the ternary binomial function $f_{a,b}(x)$ defined in (2) is Bent or not for some suitable values of n. Below are numerical examples by applying Corollary 2.4.

Example 3.3 *(1) For* $p = 3$ *and* $n = 6$*, there are* 1260 *pairs* $(a, b) \in \mathbb{F}_{3^6}^* \times \mathbb{F}_{3^2}^*$ *such that* $f_{a,b}(x)$ *is Bent. An incomplete list of* (a, b) *is as follows:*

a	γ^2	γ^2	γ^2	γ^2	γ^5	γ^{17}	γ^8	γ^{15}
b	θ^4	θ^2	θ^0	θ^6	θ^3	θ^7	θ^1	θ^5

where γ *is a primitive element of* $\mathbb{F}_{3^6}$ *with minimal polynomial* $x^6 + x^5 + 2$ *and* $\theta = \gamma^{\frac{3^6-1}{8}}$ *is a primitive of* $\mathbb{F}_{3^2}$*.*

(2) For $p = 3$ *and* $n = 10$*, there are* 40992 *pairs* $(a, b) \in \mathbb{F}_{3^{10}}^* \times \mathbb{F}_{3^2}^*$ *such that* $f_{a,b}(x)$ *is Bent. An incomplete list of* (a, b) *is as follows:*

a	γ^4	γ^4	γ^4	γ^4	γ^{61}	γ^{52}	γ^{152}	γ^{52}
b	θ^4	θ^2	θ^0	θ^6	θ^7	θ^3	θ^5	θ

where γ *is a primitive element of* $\mathbb{F}_{3^{10}}$ *with minimal polynomial* $x^{10} + x^9 + x^7 + 2$ *and* $\theta = \gamma^{\frac{3^{10}-1}{8}}$ *is a primitive of* $\mathbb{F}_{3^2}$*.*

4 Conclusion

We have characterized the Bentness of a family of p-ary binomial functions $f_{a,b}(x)$ defined by (2) by a specific exponential sum $S_{a,b}$ and by two sequences depending on the coefficients a and b. In the special case of $p = 3$, the Bentness of the ternary binomial functions

$$f_{a,b}(x) = \mathrm{Tr}_1^n(ax^{3^m-1}) + \mathrm{Tr}_1^2(bx^{\frac{3^n-1}{4}})$$

was further characterized by the Hamming weight of a finite sequence of length $\frac{3^m+1}{2}$.

Our work is motivated by a recent work given by Mesnager [17], who studied the class of functions defined in (1). Another possible way to extend Mesnager's work is to discuss the Bentness of the following functions

$$g_{a,b}(x) = \mathrm{Tr}_1^n(ax^{p^m-1}) + \mathrm{Tr}_1^2(bx^{\frac{p^n-1}{p^2-1}}), \;\; a \in \mathbb{F}_{p^n}^*, \;\; b \in \mathbb{F}_{p^2},$$

which have slight different expression from $f_{a,b}(x)$. When $p = 2$, $g_{a,b}(x)$ is exactly the function considered in [17].

References

[1] C. Carlet, Boolean functions for cryptography and error correcting codes, in: Y. Crama, P. Hammer (Eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, U.K. (in press).

[2] C. Carlet, C. Ding, Highly nonlinear mappings. J. Complexity 20(2-3): 205–244, 2004.

[3] P. Charpin, G. Gong, Hyperbent functions, Kloosterman sums, and Dickson polynomials. IEEE Trans. Inform. Theory, **54**(9), 4230–4238, 2008.

[4] P. Charpin and G. Kyureghyan. Cubic monomial Bent functions: A subclass of $\mathcal{M}$. SIAM. J. Discr. Math., **22**(2), 650–665, 2008.

[5] A. Canteaut, P. Charpin and G. Kyureghyan. A new class of monomial Bent functions. Finite Fields Appl., **14**(1), 221–241, 2008.

[6] R.S. Coulter and R.W. Matthews, Planar functions and planes of Lenz-Barlotti class II, Des. Codes Cryptogr. 10, 167–184, 1997.

[7] J.F. Dillon, Elementary Hadamard difference sets, Ph. D. these, University Maryland, Collage Park, 1974.

[8] H. Dobbertin G. Leander, A. Canteaut, C. Carlet and P. Gabort, Construction of Bent functions via Niho power functions. J. Combin. Theory, Ser. A, **113**, 779–798, 2006.

[9] C. Ding and J. Yuan, A family of skew Hadamard difference sets. J. Combin. Theory, Ser. A, **113**, 1526–1535, 2006.

[10] S.W. Golomb and G. Gong, Signal Designs With Good Correlation: For Wireless Communications, Cryptography and Radar Applications. Cambridge, U.K.: Cambridge University Press, 2005.

[11] Tor Helleseth and Alexander Kholosha, Monomial and quadratic Bent functions over the finite fields of odd characteristic, IEEE Trans. Inform. Theory, 52(5), 2018–2032, 2006.

[12] X.D. Hou, p-ary and q-ary versions of certain results about Bent functions and resilient functions. Finite Fields Appl., **10**(4), 566–582, 2004.

[13] P.V. Kumar, R. A. Scholtz and L. R. Welch, Generalized Bent functions and their properties. J. Combin. Theory, Ser. A, **40**, 90–107, 1985.

[14] G. Leander, Monomial Bent functions. IEEE Trans. Inform. Theory, **52**(2), 738–743, 2006.

[15] R. Lidl and H. Niederreiter, Finite Fields. Ser. Encyclopedia of Mathematics and its Applications, Amsterdam, The Netherlands: Addison-Wesley, 1983.

[16] F.J. MacWilliams, N.J. Sloane, The Theory of Error-Correcting Codes. Amsterdam, the Netherlands: North-Holland, 1977.

[17] S. Mesnager, A new class of Bent functions in polynomial forms. Avaible: http://eprint.iacr.org/2008/512.

[18] O.S. Rothaus, On Bent functions. J. Combin. Theory, Ser. A, **20**, 300–305, 1976.

[19] Q. Xiang, Maximally nonlinear functions and Bent functions. Des., Codes Cryptogr. 17, 211–218, 1999.