AAECC (2013) 24:461–475
DOI 10.1007/s00200-013-0202-3

ORIGINAL PAPER

On a class of binomial bent functions over the finite fields of odd characteristic

Dabin Zheng · Long Yu · Lei Hu

Received: 14 January 2013 / Revised: 23 July 2013 / Accepted: 26 July 2013 /
Published online: 7 August 2013

Abstract We give a necessary and sufficient condition such that the class of p-ary binomial functions proposed by Jia et al. (IEEE Trans Inf Theory 58(9):6054–6063, 2012) are regular bent functions, and thus settle the open problem raised at the end of that paper. Moreover, we investigate the bentness of the proposed binomials under the case $\gcd(\frac{t}{2}, p^{\frac{n}{2}} + 1) = 1$ for some even integers t and n. Computer experiments show that the new class contains bent functions that are affinely inequivalent to known monomial and binomial ones.

Keywords p-ary bent function · Regular bent function · Exponential sum

Mathematics Subject Classification (2000) 06E75 · 94A60 · 11T23

1 Introduction

Boolean bent functions, introduced by Rothaus [19] in 1976, are maximally nonlinear Boolean functions with even number of variables, that is, they achieve the maximal

D. Zheng (✉) · L. Yu
Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China
e-mail: dzheng@hubu.edu.cn

L. Yu
School of Mathematics and Statistics, Central Normal University, Wuhan 430079, China
e-mail: yulong_math_edu@sina.cn

L. Hu
State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing 100093, China
e-mail: hu@is.ac.cn

Hamming distance to the set of all affine Boolean functions. Besides wide application in cryptography due to their high nonlinearity, they play an important role in sequences and coding theory [2,3,8,16,17,20]. Moreover, they are also interesting combinatorial objects [5,7]. The concept of Boolean bent functions was also generalized to the case of functions over finite fields of odd characteristic by Kumar et al. [13]. People have paid a lot of attention to this topic, however, the complete classification of bent functions is still hopeless. Some research on constructions of bent functions focuses on monomial, binomial and quadratic functions (see [1,4–6,9,10,12,14,18], and references therein).

Let p be an odd prime and n be an even positive integer. Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements and $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$. $\mathrm{Tr}_n(\cdot)$ is the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, i.e. $\mathrm{Tr}_n(x) = \sum_{i=0}^{n-1} x^{p^i}$ for $x \in \mathbb{F}_{p^n}$. Helleseth and Kholosha [9] first characterized the bentness of a class of p-ary Dillon monomial functions by a certain Kloosterman sum. Recently, Jia et al. [12] considered a class of p-ary binomial functions which is the sum of a Dillon monomial and a special monomial as follows,

$$f_{a,b,t}(x) = \mathrm{Tr}_n\left(ax^{t(p^m-1)}\right) + bx^{\frac{p^n-1}{2}}, \quad a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_p, \tag{1}$$

where $n = 2m$ and t is a positive integer such that $\gcd(t, p^m + 1) = 1$. Inspired by the technique proposed in Jia et al. [10] established a relationship between Kloosterman sums and some partial exponential sums (see Proposition 2), and used the result to prove that $f_{a,\pm b,t}(x)$ are both regular bent functions if and only if

$$K_m(a^{p^m+1}) = 1 - \sec\frac{2\pi b}{p},$$

where "sec" denotes the secant function and

$$\sec\frac{2\pi b}{p} = \frac{2}{\omega^b + \omega^{-b}},$$

here $\omega = \exp(2\pi\sqrt{-1}/p)$ is the complex primitive pth root of unity and an element in $\mathbb{F}_p$ is viewed as an integer in $\mathbb{Z}_p$. At the end of Jia e al. [12] the authors improved the above result for the cases $p^m \equiv 3 \bmod 4$ or $p = 3$, and it was left an open problem for the other cases.

The aim of this paper is to complete the improvement of Theorem 1 of [12] and investigate the bentness of the p-ary binomial in (1) under different cases. Following the idea in [12] we first reduce the characterization of bentness of the binomial in (1) to determining a partial exponential sum (see Lemma 3). Based on the relationship (see Proposition 2) between the derived partial exponential sum and Kloosterman sums, and by using some symmetric properties of the derived partial exponential sum, we solve the open problem in [12]. Moreover, we study the bentness of the function $f_{a,b,t}(x)$ under the case $\gcd(\frac{t}{2}, p^m + 1) = 1$ for some even integer t. Computer experiments show that we can obtain bent functions that are affinely inequivalent to all known monomial and binomial ones in this case.

The remainder of the paper is organized as follows. In Sect. 2 we introduce some preliminaries. Section 3 discusses some partial exponential sums. Finally, the bentness of the class of p-ary binomial functions proposed by Jia et al. [12] under two cases is characterized in Sect. 4.

2 Preliminaries

Throughout this paper, let m, n be positive integers with $n = 2m$. Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements. The *Walsh transform and its inverse* of a p-ary function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ are defined by

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{p^n}} \omega^{f(x) - \mathrm{Tr}_n(\lambda x)} \quad \text{and} \quad \omega^{f(x)} = \frac{1}{p^n} \sum_{\lambda \in \mathbb{F}_{p^n}} W_f(\lambda) \omega^{\mathrm{Tr}_n(\lambda x)}.$$

The values $W_f(\lambda), \lambda \in \mathbb{F}_{p^n}$ are called the *Walsh coefficients* of f. The function $f(x)$ is called a *p-ary bent function* (or *generalized bent function*) if $|W_f(\lambda)|^2 = p^n$ for all $\lambda \in \mathbb{F}_{p^n}$. A bent function $f(x)$ is called *regular* if for each $\lambda \in \mathbb{F}_{p^n}$, $W_f(\lambda) = p^{\frac{n}{2}} \omega^{f^*(\lambda)}$ for some p-ary function f^* from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. A bent function $f(x)$ is called *weakly regular* if there is a complex μ with unit magnitude such that $W_f(\lambda) = p^{\frac{n}{2}} \mu \omega^{f^*(\lambda)}$ for all $\lambda \in \mathbb{F}_{p^n}$. The function $f^*(x)$ is called the *dual* of $f(x)$. Furthermore, the dual of a (weakly) regular bent function is again a (weakly) regular bent function [9].

Let $a \in \mathbb{F}_{p^n}$, the *Kloosterman sum* $K_n(a)$ [15] is defined as

$$K_n(a) = \sum_{x \in \mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_n(x + ax^{-1})},$$

here $x + ax^{-1} = 0$ for $x = 0$.

For an integer $d \in \{0, 1, \ldots, p^n - 1\}$, it has the following p-ary expansion

$$d = \sum_{i=0}^{n-1} d_i p^i, \quad 0 \le d_i \le p - 1.$$

The number $w_p(d) = \sum_{i=0}^{n-1} d_i$ is called the *p-weight* of d. It is well known that each function $f(x)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ can be represented by a univariate polynomial over $\mathbb{F}_{p^n}$, and the algebraic degree of $f(x)$ equals the maximal p-weight of the exponent i of the term $a_i x^i$ in $f(x)$ with $a_i \neq 0$. Note that the maximal algebraic degree of a Boolean bent function on $\mathbb{F}_{2^{2m}}$ is equal to m. However, the algebraic degree of p-ary bent functions has the following upper bound.

Proposition 1 [11] *Let $f(x)$ be a p-ary bent function on $\mathbb{F}_{p^n}$, then its algebraic degree* $\deg(f) \le \frac{(p-1)n}{2} + 1$. *Moreover, if $f(x)$ is a (weakly) regular bent function then* $\deg(f) \le \frac{(p-1)n}{2}$.

Two p-ary functions $f(x)$ and $g(x)$ are called *affinely equivalent* [12] if there exist some linearized permutation $l(x) \in \mathbb{F}_{p^n}[x]$, $a, c \in \mathbb{F}_p$ and $b \in \mathbb{F}_{p^n}$ such that $f(x) = ag(l(x) + b) + c$. It is well known that algebraic degree, the set of absolute values of Walsh coefficients and bentness of a p-ary function are affine invariants. It is an interesting and challenging topic to find p-ary bent functions affinely inequivalent to the known ones.

Let ξ be a primitive element of $\mathbb{F}_{p^n}$. For any ξ^i, $0 \le i \le p^n - 2$, it can be uniquely written as the from $\xi^{(p^m+1)k} \cdot \xi^l$, where $0 \le k \le p^m - 2$ and $0 \le l \le p^m$. As a consequence, we have the following lemma.

Lemma 1 *Let ξ be a primitive element of $\mathbb{F}_{p^n}$. For any element $\alpha \in \mathbb{F}_{p^n}^*$, there exists a unique pair $(x, u) \in \mathbb{F}_{p^m}^* \times \mathcal{U}$ such that $\alpha = xu$, where*

$$\mathcal{U} = \left\{ \xi^i \mid i = 0, 1, \ldots, p^m \right\}. \tag{2}$$

An element α in $\mathbb{F}_{p^n}^*$ is called a *square* if $\alpha = x^2$ for some element $x \in \mathbb{F}_{p^n}^*$. Otherwise, α is called a *non-square*. Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the sets of squares and non-squares in $\mathbb{F}_{p^n}^*$, respectively, and they can be represented as follows:

$$\mathcal{C}_i = \left\{ \xi^{2k+i} \mid k = 0, 1, \ldots, \frac{p^n - 3}{2} \right\}, \quad i = 0, 1.$$

A subset of $\mathcal{C}_0$ is defined as

$$\mathcal{C}_0^+ = \left\{ a \in \mathcal{C}_0 \mid \mathrm{Tr}_m(a^{\frac{p^m+1}{2}}) \neq 0 \right\}. \tag{3}$$

Let $\mathcal{G}$ be the cyclic subgroup of $\mathbb{F}_{p^n}^*$ of order $p^m + 1$ as

$$\mathcal{G} = \left\{ \xi^{i(p^m-1)} \mid i = 0, 1, \ldots, p^m \right\}. \tag{4}$$

Two subsets of $\mathcal{G}$ are defined as follows:

$$\mathcal{G}_0 = \left\{ g \in \mathcal{G} \mid g^{\frac{p^m+1}{2}} = 1 \right\} \quad \text{and} \quad \mathcal{G}_1 = \left\{ g \in \mathcal{G} \mid g^{\frac{p^m+1}{2}} = -1 \right\}. \tag{5}$$

It is clear that $\mathcal{G} = \mathcal{G}_0 \cup \mathcal{G}_1$. The following relationship between Kloosterman sums and some partial exponential sums have been established in Lemma 7 of [12], which is very important for our later discussions.

Proposition 2 [12] *Let $n = 2m$ and $a \in \mathbb{F}_{p^n}^*$. Following the notations as above we have*

$$\sum_{x \in \mathcal{G}_0} \omega^{\mathrm{Tr}_n(ax)} = \begin{cases} R + I\left(\omega^Q - \omega^{-Q}\right), & \text{if } a \in \mathcal{C}_0^+, \\ R, & \text{otherwise,} \end{cases}$$

and

$$\sum_{x\in\mathcal{G}_1}\omega^{\mathrm{Tr}_n(ax)}=\begin{cases}R-I\left(\omega^Q-\omega^{-Q}\right), & \text{if } a\in\mathcal{C}_0^+,\\ R, & \text{otherwise,}\end{cases}$$

where $Q=2\mathrm{Tr}_m(a^{\frac{p^m+1}{2}})$ *and*

$$R=\frac{1-K_m(a^{p^m+1})}{2},\quad I=\begin{cases}\frac{(-1)^{\frac{3m}{2}}}{2}p^{\frac{m}{2}}, & p\equiv 3 \mod 4;\\ \frac{(-1)^m}{2}p^{\frac{m}{2}}, & \text{otherwise.}\end{cases}$$

3 Some partial exponential sums

To investigate the bentness of the functions defined by (1) we first consider the following partial exponential sum.

$$S_{a,b,t}=\sum_{x\in\mathcal{G}}\omega^{\mathrm{Tr}_n(ax^t)+bx^{\frac{p^m+1}{2}}},\quad a\in\mathbb{F}_{p^n}^*, b\in\mathbb{F}_p, \tag{6}$$

where $n=2m$ and $\mathcal{G}$ is the subgroup of $\mathbb{F}_{p^n}^*$ defined by (4).

Proposition 3 *Let* $a\in\mathbb{F}_{p^n}^*$, $b\in\mathbb{F}_p$. *Let* n, m, t *be positive integers satisfying* $n=2m$ *and* $\gcd(t, p^m+1)=1$. *We have*

$$S_{a,b,t}=\begin{cases}R\left(\omega^b+\omega^{-b}\right)+I\left(\omega^b-\omega^{-b}\right)\left(\omega^Q-\omega^{-Q}\right), & \text{if } a\in\mathcal{C}_0^+,\\ R\left(\omega^b+\omega^{-b}\right), & \text{otherwise,}\end{cases} \tag{7}$$

where Q, R, I *is given in* Proposition 2 *and* $\mathcal{C}_0^+$ *is defined by* (3).

Proof Since $\gcd(t, p^m+1)=1$ we have that t is odd and

$$S_{a,b,t}=\sum_{x\in\mathcal{G}}\omega^{\mathrm{Tr}_n(ax^t)+bx^{\frac{p^m+1}{2}}}=\sum_{x\in\mathcal{G}}\omega^{\mathrm{Tr}_n(ax^t)+bx^{\frac{t(p^m+1)}{2}}}=S_{a,b,1}. \tag{8}$$

Next we determine $S_{a,b,1}$ as follows:

$$\begin{aligned}S_{a,b,1}&=\sum_{x\in\mathcal{G}}\omega^{\mathrm{Tr}_n(ax)+bx^{\frac{p^m+1}{2}}}\\ &=\omega^b\sum_{x\in\mathcal{G}_0}\omega^{\mathrm{Tr}_n(ax)}+\omega^{-b}\sum_{x\in\mathcal{G}_1}\omega^{\mathrm{Tr}_n(ax)}.\end{aligned}$$

By Proposition 2 we know that (7) holds. □

Proposition 4 *Let $a \in \mathbb{F}_{p^n}^*$, $b \in \mathbb{F}_p$. Let n, m be numbers with $n = 2m$, and t be an even number satisfying* $\gcd(\frac{t}{2}, p^m + 1) = 1$. *Let R, Q, I be notations given in* Proposition 2 *and $\mathcal{C}_0^+$ be defined by* (3). *We have*

(1) *If* $p^m \equiv 1 \mod 4$ *then*

$$S_{a,b,t} = \begin{cases} (\omega^b + \omega^{-b})\left(R + I(\omega^Q - \omega^{-Q})\right), & \text{if } a \in \mathcal{C}_0^+, \\ (\omega^b + \omega^{-b})R, & \text{otherwise.} \end{cases}$$

(2) *If* $p^m \equiv 3 \mod 4$ *then*

$$S_{a,b,t} = \omega^b E_0(a) + \omega^{-b} E_1(a),$$

where

$$E_0(a) = \sum_{x \in \mathcal{G}_0} \omega^{\mathrm{Tr}_n(ax^2)}, \quad E_1(a) = \sum_{x \in \mathcal{G}_1} \omega^{\mathrm{Tr}_n(ax^2)}. \tag{9}$$

In particular, when $b = 0$, for two cases above we have

$$S_{a,0,t} = \begin{cases} 2R + 2I(\omega^Q - \omega^{-Q}), & if\ a \in \mathcal{C}_0^+, \\ 2R, & \text{otherwise.} \end{cases}$$

Proof Because $\gcd(\frac{t}{2}, p^m + 1) = 1$, we know that $\frac{t}{2}$ is odd, and the mapping $x \mapsto x^{\frac{t}{2}}$ is a permutation on $\mathcal{G}$. So,

$$S_{a,b,t} = \sum_{x \in \mathcal{G}} \omega^{\mathrm{Tr}_n(ax^t) + bx^{\frac{p^m+1}{2}}} = \sum_{x \in \mathcal{G}} \omega^{\mathrm{Tr}_n\left(a(x^{\frac{t}{2}})^2\right) + bx^{\frac{t}{2}\frac{p^m+1}{2}}} = S_{a,b,2}. \tag{10}$$

Furthermore, one easily has

$$S_{a,b,2} = \sum_{x \in \mathcal{G}} \omega^{\mathrm{Tr}_n(ax^2) + bx^{\frac{p^m+1}{2}}} = \omega^b \sum_{x \in \mathcal{G}_0} \omega^{\mathrm{Tr}_n(ax^2)} + \omega^{-b} \sum_{x \in \mathcal{G}_1} \omega^{\mathrm{Tr}_n(ax^2)}. \tag{11}$$

(1) If $p^m \equiv 1 \mod 4$ then $\gcd(2, \frac{p^m+1}{2}) = 1$, and so the $x \mapsto x^2$ is a bijective mapping from $\mathcal{G}_0$ or $\mathcal{G}_1$ to $\mathcal{G}_0$. By (11) and Proposition 2 we have

$$\begin{aligned} S_{a,b,2} &= (\omega^b + \omega^{-b}) \sum_{x \in \mathcal{G}_0} \omega^{\mathrm{Tr}_n(ax)} \\ &= \begin{cases} (\omega^b + \omega^{-b})\left(R + I(\omega^Q - \omega^{-Q})\right), & \text{if } a \in \mathcal{C}_0^+, \\ (\omega^b + \omega^{-b})R, & \text{otherwise.} \end{cases} \end{aligned}$$

□

(2) By (11) one has

$$S_{a,b,t} = \omega^b E_0(a) + \omega^{-b} E_1(a).$$

When $b = 0$, by (10), (11) and Proposition 2 we have that

$$\begin{aligned} S_{a,0,t} &= E_0(a) + E_1(a) = 2 \sum_{x \in \mathcal{G}_0} \omega^{\mathrm{Tr}_n(ax)} \\ &= \begin{cases} 2R + 2I(\omega^Q - \omega^{-Q}), & \text{if } a \in \mathcal{C}_0^+, \\ 2R, & \text{otherwise.} \end{cases} \end{aligned}$$

□

We also need the following proposition for later usage.

Proposition 5 [12] *Let $\alpha \in \mathbb{F}_{p^m}$ and $b \in \mathbb{F}_p$. If*

$$K_m(\alpha) = 1 - sec\frac{2\pi b}{p}$$

then α is a non-square or a square with $\mathrm{Tr}_m(\sqrt{\alpha}) = 0$.

4 A class of binomial p-ary bent functions

In this section we discuss the bentness of the p-ary function $f_{a,b,t}$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ as follows:

$$f_{a,b,t} = \mathrm{Tr}_n\left(ax^{t(p^m-1)}\right) + bx^{\frac{p^n-1}{2}}, \quad a \in \mathbb{F}_{p^n}^*, \ b \in \mathbb{F}_p. \tag{12}$$

When $\gcd(t, p^m + 1) = 1$ and $b = 0$, the bentness of the function $f_{a,0,t}(x)$ has been investigated in [9] as follows.

Proposition 6 [9] *Let $n = 2m$ and t be a positive integer with $\gcd(t, p^m + 1) = 1$. For $a \in \mathbb{F}_{p^n}^*$, the p-ary function*

$$f_{a,0,t}(x) = \mathrm{Tr}_n\left(ax^{t(p^m-1)}\right)$$

is a regular bent function if and only if $K_m(a^{p^m+1}) = 0$.

When $\gcd(t, p^m + 1) = 1$ and $b \neq 0$, Jia et al. have discussed the bentness of $f_{a,b,t}(x)$ in Theorem 1 of [12] as follows.

Proposition 7 [12] *Let $n = 2m$ and t be a positive integer with $\gcd(t, p^m + 1) = 1$. For $a \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_p$, the p-ary functions*

$$f_{a,\pm b,t}(x) = \mathrm{Tr}_n\left(ax^{t(p^m-1)}\right) \pm bx^{\frac{p^n-1}{2}}$$

are both regular bent functions if and only if

$$K_m(a^{p^m+1}) = 1 - \sec\frac{2\pi b}{p}.$$

To improve the result of Proposition 7 and investigate the bentness of $f_{a,b,t}(x)$ defined by (12) under the case $\gcd\left(\frac{t}{2}, p^m+1\right) = 1$ for some even integer t, we first give some preliminary lemmas.

Lemma 2 [9] *Let n be a positive integer and $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a regular bent function satisfying $f(x) = f(-x)$ and $f(0) = 0$, then $f^*(0) = 0$ where f^* is the dual function of f.*

Lemma 3 *Let $f_{a,b,t}(x)$ be a p-ary function defined by (12) and $S_{a,b,t}$ be a partial exponential sum given in (6). Then $f_{a,b,t}(x)$ is a regular bent function if and only if $S_{a,b,t} = 1$.*

Proof If $f(x)$ is a regular bent function, by Lemma 2 we have that $W_{f_{a,b,t}}(0) = p^m$. On the other hand,

$$\begin{aligned} W_{f_{a,b,t}}(0) &= \sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_n\left(ax^{t(p^m-1)}\right)+bx^{\frac{p^n-1}{2}}} \\ &= 1 + \sum_{u\in\mathcal{U}} \sum_{y\in\mathbb{F}^*_{p^m}} \omega^{\mathrm{Tr}_n\left(au^{t(p^m-1)}\right)+bu^{\frac{p^n-1}{2}}} \\ &= 1 + (p^m-1)\sum_{x\in\mathcal{G}} \omega^{\mathrm{Tr}_n(ax^t)+bx^{\frac{p^m+1}{2}}} \\ &= 1 + (p^m-1)S_{a,b,t}. \end{aligned} \tag{13}$$

So, we have $S_{a,b,t} = 1$.

Conversely, assume that $S_{a,b,t} = 1$, by (13) we have $W_{f_{a,b,t}}(0) = p^m$. For any $\lambda \in \mathbb{F}^*_{p^n}$, by Lemma 1 we have

$$\begin{aligned} W_{f_{a,b,t}}(\lambda) &= \sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_n\left(ax^{t(p^m-1)}\right)+bx^{\frac{p^n-1}{2}}-\mathrm{Tr}_n(\lambda x)} \\ &= 1 + \sum_{u\in\mathcal{U}} \omega^{\mathrm{Tr}_n\left(au^{t(p^m-1)}\right)+u^{\frac{p^n-1}{2}}} \sum_{y\in\mathbb{F}^*_{p^m}} \omega^{\mathrm{Tr}_m\left(-(\lambda u+(\lambda u)^{p^m})y\right)} \\ &= 1 - S_{a,b,t} + p^m \sum_{u\in\mathcal{U},\lambda u+(\lambda u)^{p^m}=0} \omega^{f(u)} \\ &= p^m\omega^{f_{a,b,t}(u_\lambda)}, \end{aligned} \tag{14}$$

where u_λ is the unique solution of the equation $\lambda u + (\lambda u)^{p^m} = 0$ in $\mathcal{U}$ for any $\lambda \in \mathbb{F}^*_{p^n}$. By (13) and (14), $f_{a,b,t}(x)$ is a regular bent function. □

4.1 p-ary bent functions for $\gcd(t, p^m + 1) = 1$

In this subsection we investigate the bentness of $f_{a,b,t}(x)$ defined by (12) under the condition $\gcd(t, p^m + 1) = 1$, and complete improvement of Theorem 1 in [12].

Theorem 1 *Let $a \in \mathbb{F}_{p^n}^*$, $b \in \mathbb{F}_p$, and m, n, t be positive integers such that $n = 2m$ and $\gcd(t, p^m + 1) = 1$. The p-ary function*

$$f_{a,b,t}(x) = \mathrm{Tr}_n\left(ax^{(p^m-1)t}\right) + bx^{\frac{p^n-1}{2}}$$

is a regular bent function if and only if

$$K_m(a^{p^m+1}) = 1 - \sec\frac{2\pi b}{p}. \tag{15}$$

Moreover, if $f_{a,b,t}$ is a regular bent function, then its dual function $f^*_{a,b,t}$ is given by

$$f^*_{a,b,t}(\lambda) = \begin{cases} 0, & \text{if } \lambda = 0, \\ f_{a,b,t}(u_\lambda), & \text{otherwise,} \end{cases}$$

where u_λ denotes the unique solution of the equation $\lambda u + \lambda^{p^m} u^{p^m} = 0$ in $\mathcal{U}$ which is defined in (2).

Proof If the condition (15) holds then by Propositions 3 and 5 we have that $S_{a,b,t} = 1$. So, $f_{a,b,t}(x)$ is a regular bent function by Lemma 3. Conversely, if $f_{a,b,t}(x)$ is a regular bent function then $S_{a,b,t} = 1$ by Lemma 3. Next, we show that there is no pair $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_p$ such that $S_{a,b,t} = 1$ for $a \in \mathcal{C}_0^+$, thus by Propositions 3 the condition (15) holds.

First, when $p^m \equiv 3 \mod 4$, i.e., m is odd and $p \equiv 3 \mod 4$, by Proposition 3 we know that $S_{a,b,t}$ is an imaginary number. So there is no pair $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_p$ such that $S_{a,b,t} = 1$.

Second, we consider the case $p^m \equiv 1 \mod 4$, and assume that $a \in \mathcal{C}_0^+$, i.e., a is a square in $\mathbb{F}_{p^n}^*$ and $\mathrm{Tr}_m(a^{\frac{p^m+1}{2}}) \neq 0$. Furthermore, we assume that a is a square, but not a 4th power of an element in $\mathbb{F}_{p^n}^*$. (If a is a 4th power of an element in $\mathbb{F}_{p^n}^*$ then the following proof is similar.) For a such fixed a, $a^{\frac{p^m-1}{2}}x$ runs through the group $\mathcal{G}$ when x runs through $\mathcal{G}$, and so we have

$$\begin{aligned} S_{a,b,t} &= \sum_{x\in\mathcal{G}} \omega^{\mathrm{Tr}_n(ax^t)+bx^{\frac{p^m+1}{2}}} \overset{(8)}{=} \sum_{x\in\mathcal{G}} \omega^{\mathrm{Tr}_n(ax)+bx^{\frac{p^m+1}{2}}} \\ &= \sum_{x\in\mathcal{G}} \omega^{\mathrm{Tr}_n(a^{\frac{p^m+1}{2}}x)+ba^{\frac{p^n-1}{4}}x^{\frac{p^m+1}{2}}} \\ &= \sum_{x\in\mathcal{G}_0} \omega^{\mathrm{Tr}_m(a^{\frac{p^m+1}{2}}(x+x^{-1}))-b} + \sum_{x\in\mathcal{G}_1} \omega^{\mathrm{Tr}_m(a^{\frac{p^m+1}{2}}(x+x^{-1}))+b}, \end{aligned} \tag{16}$$

where $\mathcal{G}_0, \mathcal{G}_1$ are defined by (5). Denote by

$$N_{i,k} = \#\left\{x \in \mathcal{G}_i \mid \mathrm{Tr}_m\left(a^{\frac{p^m+1}{2}}(x+x^{-1})\right) = k,\ k \in \mathbb{F}_p\right\}, \quad i = 0, 1.$$

It is clear that $x \in \mathcal{G}_i$ if and only if $x^{-1} \in \mathcal{G}_i$ for $i \in \{0, 1\}$, and the mapping $x \mapsto x + x^{-1}$ is 2-to-1 except for $x = 1, -1$. Since $p^m \equiv 1 \mod 4$ we have that $1 \in \mathcal{G}_0$ and $-1 \in \mathcal{G}_1$. So, one can verify that $N_{0,Q}$ and $N_{1,-Q}$ are odd numbers, and $N_{0,k}, k \neq Q$ and $N_{1,k}, k \neq -Q$ are even numbers where $Q = 2\mathrm{Tr}_m(a^{\frac{p^m+1}{2}})$ which is viewed as an integer modulo p. Moreover, we have that $N_{0,k} = N_{1,-k}$ for any $k \in \mathbb{F}_p$. By equality (16) we have

$$\begin{aligned} S_{a,b,t} - 1 = {} & N_{0,b} + N_{1,-b} - 1 + \left(N_{0,b+1} + N_{1,-b+1}\right)\omega \\ & + \left(N_{0,b+2} + N_{1,-b+2}\right)\omega^2 + \cdots + \left(N_{0,p-1+b} + N_{1,p-1-b}\right)\omega^{p-1}. \end{aligned}$$

Based on above discussion we have that $N_{0,b} + N_{1,-b} - 1$ always must be an odd number.

If $p \geq 5$ then there exists $i, 0 \leq i \leq 4$ such that $b+i \neq Q$ and $-b+i \neq -Q$, and so we have that $N_{0,b+i} + N_{1,-b+i}$ is an even number. So, all the coefficients of $\omega_i's$ can not be equal. Hence, there is no pair $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_p$ such that $S_{a,b,t} = 1$ since $x^{p-1} + x^{p-2} + \cdots + x + 1$ is the minimal polynomial of ω over the rational numbers.

If $p = 3$ then Theorem 2 in [12] has proven that there is no pair $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_p$ such that $S_{a,b,t} = 1$. To sum up, $f_{a,b,t}(x)$ is a regular bent function if and only if $K_m(a^{p^m+1}) = 1 - \sec\frac{2\pi b}{p}$. Moreover, if $f_{a,b,t}(x)$ is a regular bent function then its dual can be obtained from Lemma 3. □

Remark 1 When $b = 0$ in Theorem 1, we have that $f_{a,0,t}(x)$ defined by (12) is a regular bent function if and only if $K_m(a^{p^m+1}) = 0$. This is exact Theorem 2 of [9]. It has been verified in [12] that the algebraic degree of $f_{a,b,t}(x)$ is $(p-1)m$.

4.2 p-ary bent functions for $\gcd\left(\frac{t}{2}, p^m + 1\right) = 1$

In this subsection we discuss the bentness of the p-ary function $f_{a,b,t}(x)$ defined by (12) under the condition $\gcd(\frac{t}{2}, p^m + 1) = 1$ for some even integer t.

Theorem 2 *Let $n = 2m$ and t be an even number with $\gcd(\frac{t}{2}, p^m + 1) = 1$. Let $a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_p^*$. If $p^m \equiv 1 \mod 4$ then the p-ary function*

$$f_{a,b,t}(x) = \mathrm{Tr}_n\left(ax^{(p^m-1)t}\right) + bx^{\frac{p^n-1}{2}}, \quad \gcd\left(\frac{t}{2}, p^m + 1\right) = 1,$$

is a regular bent function if and only if

$$K_m(a^{p^m+1}) = 1 - \sec\frac{2\pi b}{p}. \tag{17}$$

Proof When $p^m \equiv 1 \mod 4$, by Proposition 4 we have

$$S_{a,b,t} = \begin{cases} 2\cos\frac{2\pi b}{p}(R + (-1)^{\frac{3m+1}{2}} p^{\frac{m}{2}} \sin\frac{2\pi Q}{p}), & \text{if } a \in \mathcal{C}_0^+,\ p \equiv 3 \mod 4, \\ 2\cos\frac{2\pi b}{p}\left(R + (-1)^{m+\frac{1}{2}} p^{\frac{m}{2}} \sin\frac{2\pi Q}{p}\right), & \text{if } a \in \mathcal{C}_0^+,\ p \equiv 1 \mod 4, \\ 2\cos\frac{2\pi b}{p} R, & \text{otherwise}, \end{cases} \quad (18)$$

where $R = (1 - K_m(a^{p^m+1}))/2$.

If $f_{a,b,t}(x)$ is a regular bent function then $S_{a,b,t} = 1$ by Lemma 3. Since R is a real number, when $p^m \equiv 1 \mod 4$, one can verify that $S_{a,b,t}$ can not be a real number under the first case or the second case in (18). So,

$$1 = S_{a,b,t} = 2\cos\frac{2\pi b}{p} R, \quad i.e.,\ K_m(a^{p^m+1}) = 1 - \sec\frac{2\pi b}{p}.$$

Conversely, if the condition (17) holds then by Proposition 5 we have that a^{p^m+1} is a non-square in $\mathbb{F}_{p^m}^*$ or a square in $\mathbb{F}_{p^m}^*$ with $\mathrm{Tr}_m(a^{\frac{p^m+1}{2}}) = 0$. Note that a^{p^m+1} is a non-square (resp. square) in $\mathbb{F}_{p^m}^*$ if and only if $a \in \mathcal{C}_0$ (resp. $\mathcal{C}_1$). By (3) we have that $a \notin \mathcal{C}_0^+$. From Eq. (18) we have that

$$S_{a,b,t} = 2\cos\frac{2\pi b}{p} R = \cos\frac{2\pi b}{p}\sec\frac{2\pi b}{p} = 1.$$

Therefore, $f_{a,b,t}(x)$ is a regular bent function by Lemma 3. □

Example 1 Let $\mathbb{F}_{3^4}$ be generated by the primitive polynomial $x^4 + x^3 + 2$, and γ be a primitive element of $\mathbb{F}_{3^4}$. By a computer exhaustive search, we have found 30 binomial regular bent functions with the form $f_{a,1,2}(x) = \mathrm{Tr}_4(ax^{2(3^2-1)}) + x^{\frac{3^4-1}{2}}$ where $a \in \mathbb{F}_{3^4}^*$. These functions can be classified into two equivalent classes whose representatives are $f_{\gamma,1,2}(x)$ and $f_{\gamma^4,1,2}(x)$, respectively. It is known that in Example 1 of [12] there are also 30 binomial regular bent functions with the form $f_{a,1,1}(x) = \mathrm{Tr}_4(ax^{3^2-1}) + x^{\frac{3^4-1}{2}}$, which have been classified into two equivalent classes whose representatives are $f_{\gamma,1,1}(x)$ and $f_{\gamma^4,1,1}(x)$, respectively. Moreover, it can be check that $f_{\gamma,1,2}(x)$ is affinely inequivalent to $f_{\gamma,1,1}(x)$, and equivalent to $f_{\gamma^4,1,1}(x)$, and $f_{\gamma^4,1,2}(x)$ is affinely inequivalent to both $f_{\gamma,1,1}(x)$ and $f_{\gamma^4,1,1}(x)$.

Example 2 Let $\mathbb{F}_{5^4}$ be generated by the primitive polynomial $x^4 + x^3 + x + 3$. By help of a computer we have found 208 pairs $(a, b) \in \mathbb{F}_{5^4}^* \times \mathbb{F}_5$ such that (17) holds, that is, there are 208 binomial regular bent monomial functions with the form $\mathrm{Tr}_4(ax^{2(5^2-1)}) + bx^{\frac{5^4-1}{2}}$ where $a \in \mathbb{F}_{5^4}^*, b \in \mathbb{F}_5$.

Remark 2 It is easy to verify that the algebraic degree of the function proposed in Theorem 2 is $(p-1)m$. When $b = 0$, by Proposition 4 and Lemma 3 we can get a characterization on a such that $f_{a,0,t}(x)$ is a regular bent function for $\gcd(\frac{t}{2}, p^m + 1) = 1$. However, we can not find such regular bent monomials for $p = 3, 5, 7$ and

$n = 2, 4, 6$, but we find a weakly regular bent monomials as in the following trivial example.

Example 3 Let $\mathbb{F}_{3^2}$ be generated by the primitive polynomial $x^2 + 1$ and α be a primitive element of $\mathbb{F}_{3^2}$. With help of computer we found 6 weakly regular bent monomials with the form $\mathrm{Tr}_2(ax^{2(3-1)})$ for $a \in \{1, \alpha, \alpha^3, \alpha^4, \alpha^5, \alpha^7\}$. Unfortunately, we can not find more examples of weakly regular bent monomials of the form $\mathrm{Tr}_n(ax^{2(p^{n/2}-1)})$ for $p = 3, n = 4, 6$ and $p = 5, 7, 11, n = 2, 4$.

For an odd prime p, some known classes of p-ary binomial bent functions are listed in Table 1, where $a, c \in \mathbb{F}_{p^n}^*$, $b \in \mathbb{F}_p$. Some abbreviation symbols in the Table are explained as follows: 'r" (respectively, "wr") is short for "regular" (respectively, "weakly regular"), "ar." for "arbitrary", "Deg." for "algebraic degree", " H–K" for "Helleseth–Kholosha" and " J–Z–H–L" for "Jia–Zeng–Helleseth–Li". As for known classes of p-ary monomial bent functions, please refer to Table II in [12].

Recall that algebraic degree is one affine invariant. From Table II and Table III in [12] together with Example 1, we claim that there exist bent functions with the form

$$\mathrm{Tr}_n(ax^{t(p^{n/2}-1)}) + x^{\frac{p^n-1}{2}}, \ \gcd\left(\frac{t}{2}, p^{\frac{n}{2}} + 1\right) = 1,$$

which are affinely inequivalent to all known ones listed in Table II and Table III in [12].

To investigate the bentness of $f_{a,b,t}(x)$ in (12) for $\gcd(\frac{t}{2}, p^m + 1) = 1$ and $p^m \equiv 3 \mod 4$, we need to discuss the partial exponential sums $E_0(a)$ and $E_1(a)$ defined in (9).

Lemma 4 *Let $E_0(a)$ and $E_1(a)$ be the partial exponential sums defined by (9), namely,*

$$E_0(a) = \sum_{x \in \mathcal{G}_0} \omega^{\mathrm{Tr}_n(ax^2)}, \quad E_1(a) = \sum_{x \in \mathcal{G}_1} \omega^{\mathrm{Tr}_n(ax^2)}.$$

Then if $p^m \equiv 7 \mod 8$ then $E_0(a)$ and $E_1(a)$ are real numbers.

Table 1 Some known classes of p-ary bent binomials

Bent binomials	p	n	Forms	Deg.	Ref.
Gold (r,wr)	Odd	ar.	$\mathrm{Tr}_n(ax^{p^i+1} + cx^{p^j+1})$, $i \neq j$	2	[9]
H–K (wr)	Odd	4m	$\mathrm{Tr}_n(ax^{p^{3m}+p^{2m}-p^m+1} + x^2)$	$m + 2$	[10]
J–Z–H–L (r)	Suitable	$2m$	$\mathrm{Tr}_n(ax^{t(p^m-1)}) + bx^{\frac{p^n-1}{2}}$ $\gcd(t, p^m + 1) = 1$	$\frac{(p-1)n}{2}$	[12]
This paper (r,wr)	Suitable	$2m$	$\mathrm{Tr}_n(ax^{t(p^m-1)}) + bx^{\frac{p^n-1}{2}}$ $\gcd(\frac{t}{2}, p^m + 1) = 1$	$\frac{(p-1)n}{2}$	Thm.2

Proof (1) Let ξ be a primitive element of $\mathbb{F}_{p^n}$. Then $\xi^{2(p^m-1)}$ is a generator of $\mathcal{G}_0$. If $p^m \equiv 7 \mod 8$ then $\frac{m+1}{2}$ is a multiple of 4 and

$$E_0(a) = \sum_{x \in \mathcal{G}_0} \omega^{\mathrm{Tr}_n(ax^2)} = 2 \sum_{i \in \mathcal{I}} \omega^{\mathrm{Tr}_n(a\xi^{i(p^m-1)})},$$

where

$$\mathcal{I} = \left\{0, 4, \ldots, \frac{p^m+1}{2} - 4, \frac{p^m+1}{2}, \frac{p^m+1}{2} + 4, \ldots, p^m - 3\right\}. \tag{19}$$

So, the terms $\omega^{\mathrm{Tr}_n\left(a\xi^{i(p^m-1)}\right)}$ and $\omega^{\mathrm{Tr}_n\left(a\xi^{(i+\frac{p^m+1}{2})(p^m-1)}\right)}$ are one-to-one correspondence for $i = 0, 4, \ldots, \frac{p^m+1}{2} - 4$, and the sum of the two terms is a real number. Therefore, $E_0(a)$ is a real number. By the same way we know that $E_1(a)$ is also a real number.□

Theorem 3 *Let $n = 2m$ and t be an even number with $\gcd(\frac{t}{2}, p^m + 1) = 1$. Let $a \in \mathbb{F}_{p^n}^*$, $b \in \mathbb{F}_p^*$. If $p^m \equiv 7 \mod 8$ then there is no pair $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_p^*$ such that the function $f_{a,b,t}(x)$ is a regular bent function.*

Proof By Lemma 3 $f_{a,b,t}(x)$ is a regular bent function if and only if $S_{a,b,t} = 1$. However, according to Proposition 4 we have

$$\begin{aligned} S_{a,b,t} &= \omega^b E_0(a) + \omega^{-b} E_1(a) \\ &= \cos\frac{2\pi b}{p} (E_0(a) + E_1(a)) + i \sin\frac{2\pi b}{p} (E_0(a) - E_1(a)). \end{aligned}$$

By Lemma 4, $E_0(a)$ and $E_1(a)$ are real numbers, and so $f_{a,b,t}(x)$ is a regular bent function if and only if

$$E_0(a) = E_1(a) \quad \text{and} \quad \cos\frac{2\pi b}{p} (E_0(a) + E_1(a)) = 1. \tag{20}$$

Next we show that there is no pair $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_p^*$ such that (20) holds. Assume that there exists a pair (a, b) satisfying (20), then we have

$$(\omega^b + \omega^{-b}) E_0(a) = 1. \tag{21}$$

Denote by

$$N_{a,k} = \sharp \left\{ i \in \mathcal{I} \mid \mathrm{Tr}_n(a\xi^{i(p^m-1)}) = k,\ 0 \le k \le p-1 \right\},$$

where $\mathcal{I}$ is defined by (19). The equality (21) can be rewritten as

$$\begin{aligned} &\left(N_{a,p-b} + N_{a,b} - \frac{1}{2}\right) + (N_{a,p-b+1} + N_{a,b+1})\omega \\ &\quad + \cdots + (N_{a,p-1-b} + N_{a,b-1})\omega^{p-1} = 0. \end{aligned}$$

Then the coefficients in the equality above satisfy

$$N_{a,-b} + N_{a,b} - \frac{1}{2} = N_{a,b-1} + N_{a,b+1} = \cdots = N_{a,p-1-b} + N_{a,b-1},$$

since $x^{p-1} + x^{p-2} + \cdots + x + 1$ is the minimal polynomial of ω over the rational numbers. But this is impossible since all $N'_{a,k}s$ are integers, and so there is no pair $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_p^*$ such that (20) holds. □

Remark 3 When $p^m \equiv 3 \mod 8$ we can not find a concise characterization on the pair $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_p^*$ such that $f_{a,b,t}(x)$ for $\gcd(\frac{t}{2}, p^m + 1) = 1$ is a regular bent function. However, we also can not find such regular bent functions for small p and n, except find only one weakly regular bent binomial which is given in the following trivial example.

Example 4 Let $\mathbb{F}_{3^2}$ be generated by the primitive polynomial $x^2 + 2x + 2$, and α be a primitive element of $\mathbb{F}_{3^2}$. By help of computer we found that 10 weakly regular bent binomials over $\mathbb{F}_{3^2}$ with the form $\mathrm{Tr}_2(ax^{2(3-1)}) + bx^{\frac{3^2-1}{2}}$.

Acknowledgments The authors wish to thank Xiangyong Zeng, Xiwang Cao and two anonymous referees for their helpful comments. The work of D. Zheng was supported by National Natural Science Foundation of China (NSFC) under Grant 11101131. The work of L. Hu was supported by the NSFC (61070172 and 10990011), and the National Basic Research Program of China (2013CB834203).

References

1. Canteaut, A., Charpin, P., Kyureghyan, G.: A new class of monomial bent functions. Finite Fields Appl. **14**(1), 221–241 (2008)
2. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P. (eds.) The Monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press, Cambridge (2010)
3. Carlet, C., Ding, C.: Highly nonlinear mappings. J. Complex. **20**(2–3), 205–244 (2004)
4. Charpin, P., Kyureghyan, G.: Cubic monomial bent functions: a subclass of $\mathcal{M}$. SIAM. J. Discret. Math. **22**(2), 650–665 (2008)
5. Dillon, J.F.: Elementary Hadamard difference sets. Ph. D. these, University Maryland, Collage Park (1974)
6. Dobbertin, H., Leander, G., Canteaut, A., Gabort, P.: Construction of bent functions via Niho power functions. J. Comb. Theory Ser. **113**, 779–798 (2006)
7. Ding, C., Yuan, J.: A family of skew Hadamard difference sets. J. Comb. Theory Ser. A **113**, 1526–1535 (2006)
8. Golomb, S.W., Gong, G.: Signal Designs With Good Correlation: For Wireless Communications. Cryptography and Radar Applications. Cambridge University Press, Cambridge (2005)
9. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(5), 2018–2032 (2006)
10. Helleseth, T., Kholosha, A.: New binomial bent functions over finite fields of odd characteristic. IEEE Trans. Inf. Theory **56**(9), 4646–4652 (2010)
11. Hou, X.D.: p-ary and q-ary versions of certain results about bent functions and resilient functions. Finite Fields Appl. **10**(4), 566–582 (2004)
12. Jia, W., Zeng, X., Helleseth, T., Li, C.: A class of binomial bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **58**(9), 6054–6063 (2012)
13. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. J. Comb. Theory Ser. A **40**, 90–107 (1985)

14. Leander, G.: Monomial bent functions. IEEE Trans. Inf. Theory **52**(2), 738–743 (2006)
15. Lidl, R., Niederreiter, H.: Finite fields ser. In: Encyclopedia of Mathematics and its Applications. Addison-Wesley, Amsterdam (1983)
16. Liu, S.C., Komo, J.J.: Nonbinary Kasami sequence over GF(p). IEEE Trans. Inf. Theory **38**(4), 1409–1412 (1983)
17. MacWilliams, F.J., Sloane, N.J.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
18. Mesnager, S.: Bent and hyper-bent functions in polynomial form their link with some exponential sums and Dickson polynomials. IEEE Trans. Inf. Theory **57**(9), 5996–6009 (2011)
19. Rothaus, O.S.: On bent functions. J. Comb. Theory Ser. A **20**, 300–305 (1976)
20. Xiang, Q.: Maximally nonlinear functions and bent functions. Des. Codes Cryptogr. **17**, 211–218 (1999)