AAECC (2018) 29:529–544
https://doi.org/10.1007/s00200-018-0357-z

ORIGINAL PAPER

Explicit characterization of two classes of regular bent functions

Yanfeng Qi[1] · **Chunming Tang**[2] · **Dongmei Huang**[2]

Received: 7 September 2017 / Revised: 2 January 2018 / Accepted: 31 March 2018 /
Published online: 7 April 2018

Abstract This paper considers two classes of p-ary functions studied by Li et al. (IEEE Trans Inf Theory 59(3):1818–1831, 2013). The first class of p-ary functions is of the form

$$f(x)=Tr_1^n\left(ax^{l(q-1)}+bx^{\left(l+\frac{q+1}{2}\right)(q-1)}\right)+\epsilon x^{\frac{q^2-1}{2}}.$$

Another class of p-ary functions is of the form

$$f(x)=\begin{cases}\sum_{i=0}^{q-1} Tr_1^n(ax^{(ri+s)(q-1)})+\epsilon x^{\frac{q^2-1}{2}}, & x\neq 0,\\ f(0), & x=0.\end{cases}$$

We generalize Li et al.'s results, give necessary conditions for two classes of bent functions, and present more explicit characterization of these regular bent functions for different cases.

Keywords Regular bent function · p-ary function · Walsh transform · Kloosterman sums

Mathematics Subject Classification 06E75 · 94A60 · 11T23

✉ Chunming Tang
tangchunmingmath@163.com

[1] School of Science, Hangzhou Dianzi University, Hangzhou 310018, Zhejiang, China

[2] School of Mathematics and Information, China West Normal University, Nanchong 637002, Sichuan, China

1 Introduction

Introduced by Rothaus, Boolean bent functions as functions from $\mathbb{F}_2^n$ or $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ have important applications in cryptography [2], coding theory [3,6,8] and sequences [21]. As a class of Boolean functions with maximal Hamming distance to the set of all affine functions, bent functions can be used to construct highly nonlinear cryptographic functions and attract much attention. Many research papers focus on the characterization and construction of monomial bent functions, binomial bent functions and quadratic bent functions [1,4,5,7,9,16,19,20,22–24]. Boolean bent functions were generalized to the notation of functions over an arbitrary finite field in [15]. It is elusive to completely classify bent functions. The characterization of bent functions over finite fields of odd characteristic is more complicated than that of Boolean bent functions. Several results can be found in [11,12].

Let p be an odd prime and m be an integer. Let $n = 2m$ and $q = p^m$. Let $Tr_1^n(\cdot)$ be the trace function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_p$. Helleseth and Kholosha [10] studied monomial functions of the form

$$f_{a,r}(x) = Tr_1^n(ax^{r(q-1)}),$$

where $a \in \mathbb{F}_{q^2}$ and $gcd(r, q+1) = 1$. They proved that $f_{a,r}(x)$ is bent if and only if the Kloosterman sum $K_m(a^{q+1})$ on $\mathbb{F}_{p^m}$ is zero.

Jia et al. [13] considered binomial functions of the form

$$f_{a,b,r}(x) = Tr_1^n(ax^{r(q-1)}) + bx^{\frac{q^2-1}{2}}, a \in \mathbb{F}_{q^2}, b \in \mathbb{F}_p,$$

where $gcd(r, q+1) = 1$. By Kloosterman sums, they presented the characterization of bentness for $f_{a,b,r}$. For $p = 3$ or $q \equiv 3 \mod 4$, they proved that $f_{a,b,r}$ is bent if and only if $K_m(a) = 1 - \frac{1}{\cos(\frac{2\pi b}{p})}$. Zheng et al. [25] generalized Jia et al.'s result to the case $q \equiv 1 \mod 4$, i.e., $f_{a,b,r}$ is bent if and only if $K_m(a) = 1 - \frac{1}{\cos(\frac{2\pi b}{p})}$. Further, when $q \equiv 7 \mod 8$, r is even and $gcd(\frac{r}{2}, q+1) = 1$, Zheng et al. proved that $f_{a,b,r}(x) = Tr_1^n(ax^{r(q-1)}) + bx^{\frac{q^2-1}{2}} (a \in \mathbb{F}_{q^2}, b \in \mathbb{F}_p)$ is not bent.

Li et al. [17] considered trinomial functions of the form

$$f(x) = Tr_1^n\left(ax^{l(q-1)} + bx^{\left(l+\frac{q+1}{2}\right)(q-1)}\right) + \epsilon x^{\frac{q^2-1}{2}}, \tag{1}$$

where $a, b \in \mathbb{F}_{q^2}$ and $\epsilon \in \mathbb{F}_p$. When $gcd(l, q+1) = 1$, they presented the relation between the bentness of $f(x)$ and Kloosterman sums $K_m((a+b)^{q+1})$,$K_m((a-b)^{q+1})$ for different $a+b$ and $a-b$. Further, they considered another class of functions with multiple terms of the form

$$f(x) = \begin{cases} \sum_{i=0}^{q-1} Tr_1^n(ax^{(ri+s)(q-1)}) + \epsilon x^{\frac{q^2-1}{2}}, & x \neq 0, \\ f(0), & x = 0, \end{cases} \tag{2}$$

where $a \in \mathbb{F}_{q^2}$,$\epsilon \in \mathbb{F}_p$. When $gcd(r, q+1) = 1$ and $gcd(s-r, q+1) = 1$, they used Kloosterman sums to characterize regular bent function $f(x)$ for different $-a$.

Based on results of Li et al. [17], this paper considers bent functions defined in (1) and (2), studies parameters of these bent functions, and presents more results of the characterization of bent functions in (1) and (2) for more explicit parameters. For bent functions defined in (1), Li et al. [17] gave the characterization for the case $gcd(l, q+1) = 1$. We have some necessary conditions for these bent functions: $gcd(l, q+1) = 1$, or, $gcd(l, q+1) = 2$ and $q \equiv 1 \mod 4$. When $p \geq 5$, $gcd(l, q+1) = 1$ and $a-b, a+b$ are quadratic residues, p-ary functions defined in (1) are not bent. Further, we present explicit characterization of bentness for these functions defined in (1) for the case $gcd(l, q+1) = 1$ and the case $gcd(l, q+1) = 2, q \equiv 1 \mod 4$. For bent functions defined in (2), Li et al. [17] gave the characterization for the case $gcd(r, q+1) = 1$. We study their bentness for cases $gcd(r, q+1) = 1$ and $gcd(r, q+1) = 2$. When $p \geq 5$ and $\epsilon = 0$, $f(x)$ is not bent. When $\epsilon \neq 0$, we give necessary conditions for regular bent functions and present the characterization of these bent functions for the case $gcd(s-r, q+1) = 1$ and the case $gcd(s-r, q+1) = 2, q \equiv 1 \mod 4$. Our work generalizes results of Li et al. [17] and Zheng et al. [25].

This paper is organized as follows: Sect. 2 introduces some notations and results on exponential sums. Section 3 considers two classes of regular bent functions, gives necessary conditions for these regular bent functions, and characterizes these regular bent functions for different cases. Section 4 makes a conclusion.

2 Preliminaries

2.1 Regular bent functions

Throughout this paper, let p be an odd prime, m, n be positive integers and $n = 2m$. Let $\mathbb{F}_{p^n}$ be a finite field with p^n elements and $\mathbb{F}_{p^n}^*$ be the multiplicative group composed of all nonzero elements in $\mathbb{F}_{p^n}$. Let $k|n$ and Tr_k^n be the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^k}$

$$Tr_k^n(x) = x + x^{p^k} + \cdots + x^{p^{n-k}}.$$

Let $q = p^m$. For any $x \in \mathbb{F}_{q^2}^*$, there exists a unique factorization $x = y * \xi^i$, where $y \in \mathbb{F}_q^*$, ξ is a primitive element of $\mathbb{F}_{q^2}$ and $0 \leq i \leq q$. Let $U = \{\xi^0, \xi^{(q-1)}, \ldots, \xi^{(q-1)q}\}$, $U_0 = U^2 = \{u^2 : u \in U\}$ and $U_1 = U \backslash U_0$. Sets of quadratic residues and quadratic non-residues in $\mathbb{F}_{q^2}^*$ are defined as $\mathcal{C}_0 = \{x^2 : x \in \mathbb{F}_{q^2}^*\}$, $\mathcal{C}_1 = \{\xi x^2 : x \in \mathbb{F}_{q^2}^*\}$ respectively. Then $\mathbb{F}_{q^2}^* = \mathcal{C}_0 \bigcup \mathcal{C}_1$ and $\mathcal{C}_0 \bigcap \mathcal{C}_1 = \emptyset$. Define $\mathcal{C}_0^+ = \{x \in \mathcal{C}_0 : Tr_1^m(x^{\frac{p^m+1}{2}}) \neq 0\}$.

A p-ary function is a map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. The Walsh transform of a p-ary function $f(x)$ over $\mathbb{F}_{p^n}$ is defined by

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{p^n}} w^{f(x) - Tr_1^n(\lambda x)},$$

where $w = e^{2\pi\sqrt{-1}/p}$ and $\lambda \in \mathbb{F}_{p^n}$.

A p-ary function $f(x)$ is called a p-ary bent function if $|W_f(\lambda)|^2 = p^n$ for any $\lambda \in \mathbb{F}_{p^n}$. A p-ary bent function $f(x)$ is regular if there exists some p-ary function $f^*(\lambda)$ satisfying $W_f(\lambda) = p^{\frac{n}{2}} w^{f^*(\lambda)}$ for any $\lambda \in \mathbb{F}_{p^n}$. The function $f^*(\lambda)$ is called the dual of $f(x)$. The dual of a p-ary bent function is also bent.

Let $f(x)$ be a p-ary function with Dillon exponents of the form

$$f(x) = \begin{cases} \sum_{i=0}^{q-1} Tr_1^n(a_i x^{i(q-1)}) + bx^{\frac{q^2-1}{2}}, & x \neq 0, \\ f(0), & x = 0, \end{cases} \tag{3}$$

where $n = 2m$, $q = p^m$, $a_i \in \mathbb{F}_{p^n}$, and $b \in \mathbb{F}_p$. The characterization of bentness for $f(x)$ is given in the following lemma [17, Theorem 1].

Lemma 1 *Let $f(x)$ be a p-ary function defined in (3). Then $f(x)$ is bent if and only if $\Lambda_f = w^{f(0)}$, where*

$$\Lambda_f = \sum_{u \in U} w^{\sum_{i=0}^{q-1} Tr_1^n(a_i u^{q-1}) + bu^{\frac{q+1}{2}}}.$$

Further, if $f(x)$ is bent, then it is also regular bent.

2.2 Exponential sums

For $a \in \mathbb{F}_q$, the Kloosterman sum $K_m(a)$ of a [14,18] is defined by

$$K_m(a) = \sum_{x \in \mathbb{F}_q} w^{Tr_1^m\left(ax + \frac{1}{x}\right)},$$

where $\frac{1}{0} = 0$ for $x = 0$. Since $\overline{K_m(a)} = \sum_{x \in \mathbb{F}_q} w^{-Tr_1^m(ax + \frac{1}{x})} = K_m(a)$, then $K_m(a)$ is a real number. Some notations are defined below.

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

$$Q(a) = 2Tr_1^m\left(a^{\frac{p^m+1}{2}}\right), \quad a \in \mathcal{C}_0;$$

$$R(a) = \frac{1 - K_m(a^{p^m+1})}{2}, \quad a \in \mathbb{F}_{q^2}.$$

Obviously, if $q \equiv 1 \mod 4$, then I is a real number. If $q \equiv 3 \mod 4$, then I is a pure imaginary number.

The following result on exponential sums is useful [13, Lemma 7].

Proposition 1 *Let $a \in \mathbb{F}_{q^2}^*$. Let $S_i(a) = \sum_{u\in U_i} w^{Tr_1^n(au)}(i=0,1)$. Then,*

$$S_0(a) = \sum_{u\in U_0} w^{Tr_1^n(au)} = \begin{cases} R(a) + I(w^{Q(a)} - w^{-Q(a)}), & a \in \mathcal{C}_0^+, \\ R(a), & otherwise, \end{cases}$$

and

$$S_1(a) = \sum_{u\in U_1} w^{Tr_1^n(au)} = \begin{cases} R(a) - I(w^{Q(a)} - w^{-Q(a)}), & a \in \mathcal{C}_0^+, \\ R(a), & otherwise. \end{cases}$$

Remark If $a \in \mathcal{C}_0 \backslash \mathcal{C}_0^+$, then we have $Q(a) = 0$. Hence, Proposition 1 still holds if $\mathcal{C}_0^+$ is replaced by $\mathcal{C}_0$. From Proposition 1, we have $S_i(a) = \sum_{u\in U_i} w^{Tr_1^n(au)}$ is an imaginary number if and only if $q \equiv 1 \mod 4$ and $a \in \mathcal{C}_0^+$.

Some results on $S_i(a)$ are given below.

Proposition 2 *Let $q \equiv 1 \mod 4$, $a \in \mathcal{C}_0$, and $N_j^i(a) = \#\{v \in U_i : Tr_1^m\left(a^{\frac{q+1}{2}}(v + \frac{1}{v})\right) = j\}(i=0,1)$. Then,*

$$N_j^i(a) \equiv \begin{cases} 0 \mod 2, & j \neq Tr_1^m\left(2(-1)^i a^{\frac{q+1}{2}}\right), \\ 1 \mod 2, & j = Tr_1^m\left(2(-1)^i a^{\frac{q+1}{2}}\right). \end{cases}$$

Further, If $a^{\frac{q^2-1}{4}} = 1$, then $S_i(a) = \sum_{i=0}^{p-1} N_j^i(a) w^j$. If $a^{\frac{q^2-1}{4}} = -1$, then $S_i(a) = \sum_{i=0}^{p-1} N_j^{i+1}(a) w^j$.

Proof Note that $a = a^{\frac{q+1}{2}} \cdot a^{-\frac{q-1}{2}}$. Since $a \in \mathcal{C}_0$, then $a^{\frac{q+1}{2}} \in \mathbb{F}_q$ and $a^{-\frac{q-1}{2}} \in U$. We have

$$S_i(a) = \sum_{v\in U_i} w^{Tr_1^n(av)} = \sum_{v\in U_i} w^{Tr_1^n\left(a^{\frac{q+1}{2}} \cdot a^{-\frac{q-1}{2}} v\right)}.$$

If $a^{\frac{q^2-1}{4}} = 1$, then $a^{-\frac{q-1}{2}} \in U_0$. Hence,

$$S_i(a) = \sum_{v\in U_i} w^{Tr_1^n\left(a^{\frac{q+1}{2}} v\right)} = \sum_{v\in U_i} w^{Tr_1^m\left(a^{\frac{q+1}{2}}\left(v + \frac{1}{v}\right)\right)} = \sum_{i=0}^{p-1} N_j^i(a) w^j,$$

where $N_j^i(a) = \#\{v \in U_i : Tr_1^m(a^{\frac{q+1}{2}}(v + \frac{1}{v})) = j\}$. If $v \neq \pm 1$, then both v and $\frac{1}{v}$ lie in $\{v \in U_i : Tr_1^m(a^{\frac{q+1}{2}}(v + \frac{1}{v})) = j\}$ and $v \neq \frac{1}{v}$. Since $q \equiv 1 \mod 4$, then

$-1 \in U_1$, $(-1)^i \in U_i$, and $(-1)^{i+1} \notin U_i$. Hence, we have $N^i_{Tr_1^m(2(-1)^i a^{(q+1)/2})}(a)$ is odd and $N^i_j(a)$ is even for $j \neq Tr_1^m(2(-1)^i a^{\frac{q+1}{2}})$.

If $a^{\frac{q^2-1}{4}} = -1$, then $a^{-\frac{q-1}{2}} \in U_1$ and

$$S_i(a) = \sum_{v \in U_{i+1}} w^{Tr_1^n\left(a^{\frac{q+1}{2}} v\right)} = \sum_{v \in U_{i+1}} w^{Tr_1^m\left(a^{\frac{q+1}{2}}\left(v+\frac{1}{v}\right)\right)} = \sum_{i=0}^{p-1} N_j^{i+1}(a) w^j,$$

where $N_j^{i+1}(a) = \#\{v \in U_{i+1} : Tr_1^m(a^{\frac{q+1}{2}}(v + \frac{1}{v})) = j\}$.

Hence, this proposition follows. □

Remark From Proposition 2, for $q \equiv 1 \mod 4$ and any $a \in \mathcal{C}_0$, there exist non-negative integers c_j satisfying $S_i(a) = c_0 + c_1 w + \cdots + c_{p-1} w^{p-1}$ and $\#\{i : 2 \nmid c_i, i = 0, 1, \ldots, p-1\} = 1$.

From a similar proof as that of Proposition 2, we have the following proposition.

Proposition 3 *Let $q \equiv 3 \mod 4$, $a \in \mathcal{C}_0$, and $N^i_j(a) = \#\{v \in U_i : Tr_1^m(a^{\frac{q+1}{2}}(v + \frac{1}{v})) = j\}$. Then, $S_i(a) = \sum_{i=0}^{p-1} N^i_j(a) w^j$ and $N^1_j(a) \equiv 0 \mod 2$. Further, if $a \in \mathcal{C}_0^+$, then*

$$N^0_j(a) \equiv \begin{cases} 0 \mod 2, & j \neq \pm Tr_1^m\left(2a^{\frac{q+1}{2}}\right), \\ 1 \mod 2, & j = \pm Tr_1^m\left(2a^{\frac{q+1}{2}}\right). \end{cases}$$

If $a \in \mathcal{C}_0 \backslash \mathcal{C}_0^+$, then $N^0_j(a) \equiv 0 \mod 2$.

Further, we can have the following lemma.

Lemma 2 *Let $a \in \mathbb{F}^*_{q^2}$ and $N_j = \#\{u \in U : Tr_1^n(au) = j\}$, then $\sum_{u \in U} w^{Tr_1^n(au)} = \sum_{i=0}^{p-1} N_i w^i$. Further, If $a \notin \mathcal{C}_0^+$, then all N_i are even. If $a \in \mathcal{C}_0^+$, then*

$$N_i \equiv \begin{cases} 0 \mod 2, & i \neq \pm Tr_1^n\left(a^{\frac{q+1}{2}}\right), \\ 1 \mod 2, & i = \pm Tr_1^n\left(a^{\frac{q+1}{2}}\right). \end{cases}$$

The following two lemmas are useful to obtain our results.

Lemma 3 *Let p be an odd prime, and $c'_0, \ldots, c'_{p-1}$ be integers such that $p > \#\{i \in \{0, \ldots, p-1\} : c'_i \neq 0\}$ and $\sum_{i=0}^{p-1} c'_i \in \{1, -1\}$. Then, for any integers $c_i (i = 0, \ldots, p-1)$ and positive integer $d > 1$,*

$$d\left(\sum_{i=0}^{p-1} c_i w^i\right) \neq \sum_{i=0}^{p-1} c'_i w^i.$$

Proof Suppose that $d(\sum_{i=0}^{p-1} c_i w^i) = \sum_{i=0}^{p-1} c_i' w^i$. Then, $\sum_{i=0}^{p-1}(dc_i - c_i')w^i = 0$. The minimal polynomial of w over the rational field is $w^{p-1} + w^{p-2} + \cdots + w + 1 = 0$. Thus, we have

$$dc_0 - c_0' = \cdots = dc_{p-1} - c_{p-1}'.$$

Since $p > \#\{i \in \{0, \ldots, p-1\} : c_i' \neq 0\}$, there exists $i_0 \in \{0, \ldots, p-1\}$ such that $c_{i_0}' = 0$. Thus, $d|c_i'$ for any $i \in \{0, \ldots, p-1\}$. As a result, $d| \sum_{i=0}^{p-1} c_i' = \pm 1$, which conflicts with $d > 1$. It completes the proof. □

Lemma 4 *Let p be an odd prime, and $c_0, c_0', \ldots, c_{p-1}, c_{p-1}'$ be integers such that $\sum_{i=0}^{p-1} c_i \equiv 0 \pmod 2$ and $\sum_{i=0}^{p-1} c_i' \equiv 1 \pmod 2$. If $p > \#\{i \in \{0, \ldots, p-1\} : c_i \equiv 1 \pmod 2\} + \#\{i \in \{0, \ldots, p-1\} : c_i' \equiv 1 \pmod 2\}$, then $\sum_{i=0}^{p-1} c_i w^i \neq \sum_{i=0}^{p-1} c_i' w^i$.*

Proof Suppose that $\sum_{i=0}^{p-1} c_i w^i = \sum_{i=0}^{p-1} c_i' w^i$. Then, $\sum_{i=0}^{p-1}(c_i - c_i')w^i = 0$. The minimal polynomial of w over the rational field is $w^{p-1} + w^{p-2} + \cdots + w + 1 = 0$. Thus, we have

$$c_0 - c_0' = \cdots = c_{p-1} - c_{p-1}'.$$

Since $p > \#\{i \in \{0, \ldots, p-1\} : c_i \equiv 1 \pmod 2\} + \#\{i \in \{0, \ldots, p-1\} : c_i' \equiv 1 \pmod 2\}$, there exists $i_0 \in \{0, \ldots, p-1\}$ such that $c_{i_0} \equiv c_{i_0}' \equiv 0 \pmod 2$. Thus, $c_i - c_i' \equiv 0 \pmod 2$ for any $i \in \{0, \ldots, p-1\}$. As a result, $\sum_{i=0}^{p-1} c_i - \sum_{i=0}^{p-1} c_i' \equiv 0 \pmod 2$, which conflicts with $\sum_{i=0}^{p-1} c_i \equiv 0 \pmod 2$ and $\sum_{i=0}^{p-1} c_i' \equiv 1 \pmod 2$. It completes the proof. □

Proposition 4 *Let $p \geq 5$. Then for any $\epsilon \in \mathbb{F}_p$, and $\delta, \theta \in \mathcal{C}_0$, $w^\epsilon S_0(\delta) + w^{-\epsilon} S_1(\theta) \neq 1$.*

Proof We first consider the case $q \equiv 1 \mod 4$. From Proposition 2, there exist non-negative integers $c_j(\delta), c_j(\theta)$ $(j = 0, 1, \ldots, p-1)$ such that

$$w^\epsilon S_0(\delta) = \sum_{j=0}^{p-1} c_j(\delta) w^j, \ w^{-\epsilon} S_1(\theta) = \sum_{j=0}^{p-1} c_j(\theta) w^j.$$

Further, the number of odd $c_j(\delta)(j = 0, 1, \ldots, p-1)$ is one, and the number of odd $c_j(\theta)(j = 0, 1, \ldots, p-1)$ is also one. Then, $\sum_{j=0}^{p-1}(c_j(\delta) + c_j(\theta))$ is even and $\#\{j \in \{0, \ldots, p-1\} : c_j(\delta) + c_j(\theta) \equiv 1 \pmod 2\} \leq 2$. By Lemma 4, $w^\epsilon S_0(\delta) + w^{-\epsilon} S_1(\theta) \neq 1$.

If $q \equiv 3 \mod 4$, from Proposition 3, there exist non-negative integers $c_j(\delta), c_j(\theta)$ $(j = 0, 1, \ldots, p-1)$ such that

$$w^\epsilon S_0(\delta) = \sum_{j=0}^{p-1} c_j(\delta) w^j, \ w^{-\epsilon} S_1(\theta) = \sum_{j=0}^{p-1} c_j(\theta) w^j.$$

Further, the number of odd $c_j(\delta)(j = 0, 1, \ldots, p-1)$ is 0 or 2, and $c_j(\theta)(j = 0, 1, \ldots, p-1)$ are even. Thus, we have $\sum_{j=0}^{p-1}(c_j(\delta) + c_j(\theta)) = 0 \mod 2$ and $\#\{j \in \{0, \ldots, p-1\} : c_j(\delta) + c_j(\theta) \equiv 1 \pmod 2\} \leq 2$. By Lemma 4, $w^{\epsilon} S_0(\delta) + w^{-\epsilon} S_1(\theta) \neq 1$.

Hence, this proposition follows. □

Remark Further, we have $w^{\epsilon} S_0(\delta) + w^{-\epsilon} S_0(\theta) \neq 1$. Proposition 4 can be used to prove the nonexistence of some class of bent functions.

3 Characterization of two classes of regular bent functions

In this section, we will consider two classes of p-ary functions in [17], generalize Li et al.'s work, and make more explicit characterization for bentness of these functions.

3.1 The first class of regular bent functions

The first class of p-ary functions is of the form

$$f(x) = Tr_1^n\left(ax^{l(q-1)} + bx^{\left(l+\frac{q+1}{2}\right)(q-1)}\right) + \epsilon x^{\frac{q^2-1}{2}}, \tag{4}$$

where $n = 2m$, $q = p^m$, $a, b \in \mathbb{F}_{q^2}$, and $\epsilon \in \mathbb{F}_p$.

The case $gcd(l, q+1) = 1$ is studied in [17]. We will consider more general cases for these functions.

Theorem 1 *Let $f(x)$ be defined in (4). If $f(x)$ is bent, then $gcd(l, q+1) = 1$, or, $gcd(l, q+1) = 2$ and $q \equiv 1 \mod 4$.*

Proof We first prove that if $f(x)$ is bent, then $gcd(l, \frac{q+1}{2}) = 1$. Suppose that $gcd(l, \frac{q+1}{2}) = d > 1$. Then

$$\begin{aligned}
\Lambda_f &= \sum_{u \in U} w^{Tr_1^n\left(\left(a+bu^{\frac{q+1}{2}}\right)u^l\right)+\epsilon u^{\frac{q+1}{2}}} \\
&= w^{\epsilon} \sum_{v \in U_0} w^{Tr_1^n((a+b)v^l)} + w^{-\epsilon} \sum_{v \in U_1} w^{Tr_1^n((a-b)v^l)} \\
&= d\left(w^{\epsilon} \sum_{v \in U_0^d} w^{Tr_1^n((a+b)v)} + w^{-\epsilon} \sum_{v \in U_1^d} w^{Tr_1^n((a-b)v)}\right),
\end{aligned}$$

where $U_i^d = \{v^d : v \in U_i\}$. From Lemma 1,

$$\Lambda_f = d\left(w^{\epsilon} \sum_{v \in U_0^d} w^{Tr_1^n((a+b)v)} + w^{-\epsilon} \sum_{v \in U_1^d} w^{Tr_1^n((a-b)v)}\right) = w^{f(0)}.$$

From Lemma 3, $d = gcd(l, \frac{q+1}{2}) = 1$, i.e., $gcd(l, q+1) = 1$ or 2. Further, from $gcd(l, q+1) = 2$, $q \equiv 1 \mod 4$. Thus, this theorem follows. □

When $b = 0$ and $\epsilon \neq 0$, Zheng et al. proved in Theorem 3 in [25] that when $q \equiv 3 \mod 8$ and $gcd(l, q+1) = 2$, $f(x)$ is not bent. They left the nonexistence of bent function $f(x)$ as an open problem when $q \equiv 7 \mod 8$. From Theorem 1, $f(x)$ in the case $q \equiv 7 \mod 8$ is not bent. Li et al. [17] studied the characterization of regular bentness of $f(x)$ for the case $gcd(l, q+1) = 1$.

Theorem 2 *Let $p \geq 5$ and $f(x)$ be a p-ary function defined in (4). Let $gcd(l, q+1) = 1$, $\delta = a+b$, $\theta = a-b$, and $\delta, \theta \in \mathcal{C}_0$. Then $f(x)$ is not bent.*

Proof From [17], $f(x)$ is bent if and only if $w^{\epsilon} S_0(\delta) + w^{-\epsilon} S_1(\theta) = 1$. From Proposition 4, this theorem follows. □

From Theorem 2, if $\delta, \theta \in \mathcal{C}_0$, then $f(x)$ is not bent. Hence, we have the following corollary, which is a straightforward result of Theorem 9 of Li et al. [17].

Corollary 1 *Let $p \geq 5$, and $f(x)$ be a p-ary function defined in (4). Then $f(x)$ is regular bent if and only if*

$$w^{\epsilon} K_m(\delta^{q+1}) + w^{-\epsilon} K_m(\theta^{q+1}) = \begin{cases} 4I\sqrt{-1}w^{\epsilon} \sin \frac{2\pi Q(\delta)}{p} + 2\cos\frac{2\pi\epsilon}{p} - 2, & \delta \in \mathcal{C}_0, \theta \notin \mathcal{C}_0, \\ -4I\sqrt{-1}w^{-\epsilon} \sin \frac{2\pi Q(\theta)}{p} + 2\cos\frac{2\pi\epsilon}{p} - 2, & \delta \notin \mathcal{C}_0, \theta \in \mathcal{C}_0, \\ 2\cos\frac{2\pi\epsilon}{p} - 2, & \delta \notin \mathcal{C}_0, \theta \notin \mathcal{C}_0. \end{cases}$$

We will study the characterization of regular bent functions for the case $gcd(l, q+1) = 2$ and $q \equiv 1 \mod 4$ in Theorem 1.

Theorem 3 *Let $p \geq 5$, $q \equiv 1 \mod 4$, and $f(x)$ be a p-ary function defined in (4). Let $gcd(l, q+1) = 2$, $\delta = a+b$, and $\theta = a-b$. Then, $f(x)$ is regular bent if and only if*

$$w^{\epsilon} K_m(\delta^{q+1}) + w^{-\epsilon} K_m(\theta^{q+1}) = \begin{cases} 4I\sqrt{-1}w^{\epsilon} \sin \frac{2\pi Q(\delta)}{p} + 2\cos\frac{2\pi\epsilon}{p} - 2, & \delta \in \mathcal{C}_0, \theta \notin \mathcal{C}_0, \\ 4I\sqrt{-1}w^{-\epsilon} \sin \frac{2\pi Q(\theta)}{p} + 2\cos\frac{2\pi\epsilon}{p} - 2, & \delta \notin \mathcal{C}_0, \theta \in \mathcal{C}_0, \\ 2\cos\frac{2\pi\epsilon}{p} - 2, & \delta \notin \mathcal{C}_0, \theta \notin \mathcal{C}_0. \end{cases}$$

Proof We have

$$\Lambda_f = w^{\epsilon} \sum_{v \in U_0} w^{Tr_1^n((a+b)v^l)} + w^{-\epsilon} \sum_{v \in U_1} w^{Tr_1^n((a-b)v^l)}.$$

Since $gcd(l, q+1) = 2$ and $q \equiv 1 \mod 4$, then $gcd(l, \frac{q+1}{2}) = 1$ and l is even. Further, $v \longmapsto v^l$ is a permutation of U_0 and also a bijection from U_1 to U_0. Hence,

$$\Lambda_f = w^{\epsilon} \sum_{v \in U_0} w^{Tr_1^n((a+b)v)} + w^{-\epsilon} \sum_{v \in U_0} w^{Tr_1^n((a-b)v)}.$$

From Lemma 1, $f(x)$ is regular bent if and only if

$$w^{\epsilon} S_0(\delta) + w^{-\epsilon} S_0(\theta) = w^{f(0)} = 1.$$

If $\delta, \theta \in \mathcal{C}_0$, then from the remark after Proposition 4, $f(x)$ is not bent. From Proposition 1, this theorem can be obtained. □

3.2 The second class of regular bent functions

The second class of p-ary functions is of the form

$$f(x)=\begin{cases}\sum_{i=0}^{q-1} Tr_1^n(ax^{(ri+s)(q-1)})+\epsilon x^{\frac{q^2-1}{2}}, & x\neq 0,\\ f(0), & x=0,\end{cases} \tag{5}$$

where $n=2m$, $q=p^m$, $a\in\mathbb{F}_{q^2}$, and $\epsilon\in\mathbb{F}_p$.

For simplicity, we first consider $f(x)$ for the case $\epsilon=0$. When $gcd(r,q+1)=1$ or 2, the following theorem gives the nonexistence of bent $f(x)$.

Theorem 4 *Let $p\geq 7$ and $f(x)$ be a p-ary function defined in (5). Let $\epsilon=0$ and $gcd(r,q+1)=1$ or 2. Then $f(x)$ is not bent.*

Proof Suppose that $f(x)$ is bent. We first prove that $gcd(s-r,q+1)=1$.

(1) $gcd(r,q+1)=1$: If $u\in U$, then

$$\sum_{i=0}^{q-1}u^{ri+s}=\begin{cases}-u^{s-r}, & u\neq 1,\\ 0, & u=1.\end{cases}$$

We have

$$\begin{aligned}\Lambda_f&=\sum_{u\in U}w^{\sum_{i=0}^{q-1}Tr_1^n(au^{ri+s})}\\&=1+\sum_{u\in U\setminus\{1\}}w^{Tr_1^n(-au^{s-r})}\\&=1-w^{-Tr_1^n(a)}+\sum_{u\in U}w^{Tr_1^n(-au^{s-r})}\\&=1-w^{-Tr_1^n(a)}+d\sum_{u\in U^d}w^{Tr_1^n(-au)},\end{aligned}$$

where $d=gcd(s-r,q+1)$ and $U^d=\{u^d:u\in U\}$. Since $f(x)$ is bent, from Lemma 1, we have

$$d\sum_{u\in U^d}w^{Tr_1^n(-au)}=-1+w^{Tr_1^n(-a)}+w^{f(0)}.$$

There exist integers $c_i, c_i'(i=0,1,\ldots,p-1)$ such that

$$d\sum_{u\in U^d}w^{Tr_1^n(-au)}=\sum_{i=0}^{p-1}c_iw^i,\quad -1+w^{Tr_1^n(a)}+w^{f(0)}=\sum_{i=0}^{p-1}c_i'w^i.$$

By Lemma 3, we have $d=1=gcd(s-r,q+1)=1$.

(2) $gcd(r, q+1) = 2$: From a similar discussion, we also have $gcd(s-r, q+1) = 1$. From Case (1) and Case (2), we have $gcd(s-r, q+1) = d = 1$. Note that

$$\begin{aligned}\Lambda_f &= \sum_{u \in U} w^{\sum_{i=0}^{q-1} Tr_1^n(au^{ri+s})} \\ &= 2 + \sum_{u \in U \setminus \{\pm 1\}} w^{Tr_1^n(-au^{s-r})} \\ &= 2 - w^{-Tr_1^n(a)} - w^{-Tr_1^n(a(-1)^{s-r})} + \sum_{u \in U} w^{Tr_1^n(-au^{s-r})} \\ &= 2 - w^{-Tr_1^n(a)} - w^{-Tr_1^n(a(-1)^{s-r})} + d \sum_{u \in U^d} w^{Tr_1^n(-au)}.\end{aligned}$$

Note that $\sum_{u \in U} w^{Tr_1^n(-a(-u))} = \sum_{u \in U} w^{Tr_1^n(-au)}$ and $\sum_{u \in U} w^{Tr_1^n(-au)}$ is a real number. From Lemma 1, we have

$$\sum_{u \in U} w^{Tr_1^n(au)} = -1 + w^{Tr_1^n(a)} + w^{-Tr_1^n(a)}.$$

From Lemma 2, there exist integers $c_i\,(i = 0, 1, \ldots, p-1)$ such that

$$\sum_{u \in U} w^{Tr_1^n(au)} = \sum_{i=0}^{p-1} c_i w^i,$$

where $\sum_{i=0}^{p-1} c_i \equiv 0 \mod 2$ and $\#\{i \in \{0, \ldots, p-1\} : c_i \equiv 1 \pmod 2\} \le 2$. By Lemma 4, $\sum_{u \in U} w^{Tr_1^n(au)} \neq -1 + w^{Tr_1^n(a)} + w^{-Tr_1^n(a)}$. Hence, this theorem follows. □

In Theorem 10, Li et al. [17] gave the necessary and sufficient conditions of bent $f(x)$ for the case $\epsilon = 0$ and $gcd(r, q+1) = 1$. Theorem 4 demonstrates that these functions are not bent.

We will consider the case $\epsilon \neq 0$ and study the bentness of $f(x)$. The following proposition gives necessary conditions of bent function $f(x)$ in the case $gcd(r, q+1) = 1$ or 2.

Proposition 5 *Let $p \geq 7$ and $f(x)$ be a p-ary bent function defined in (5). Let $\epsilon \neq 0$ and $gcd(r, q+1) = 1$ or 2. Then, $gcd(s-r, q+1) = 1$, or, $gcd(s-r, q+1) = 2$ and $q \equiv 1 \mod 4$.*

Proof If $u \in U$, then

$$\sum_{i=0}^{q-1} u^{ri+s} = \begin{cases} -u^{s-r}, & a^d \neq 1, \\ 0, & a^d = 1, \end{cases}$$

where $d = gcd(r, q+1)$. We have

$$\begin{aligned}\Lambda_f &= \sum_{u\in U} w^{\sum_{i=0}^{q-1} Tr_1^n(au^{ri+s})+\epsilon u^{\frac{q+1}{2}}}\\ &= \sum_{u\in\{u\in U:u^d=1\}} w^{\epsilon u^{\frac{q+1}{2}}} + \sum_{u\in U\setminus\{u:u^d=1\}} w^{Tr_1^n(-au^{s-r})+\epsilon u^{\frac{q+1}{2}}}\\ &= \sum_{u\in\{u\in U:u^d=1\}} w^{\epsilon u^{\frac{q+1}{2}}} - \sum_{u\in\{u\in U:u^d=1\}} w^{Tr_1^n(-au^{s-r})+\epsilon u^{\frac{q+1}{2}}} + \sum_{u\in U} w^{Tr_1^n(-au^{s-r})+\epsilon u^{\frac{q+1}{2}}}\\ &= \sum_{u\in\{u\in U:u^d=1\}} w^{\epsilon u^{\frac{q+1}{2}}} - \sum_{u\in\{u\in U:u^d=1\}} w^{Tr_1^n(-au^{s-r})+\epsilon u^{\frac{q+1}{2}}} + e\sum_{u\in U^e} w^{Tr_1^n\left(-au^{\frac{s-r}{e}}\right)+\epsilon u^{\frac{q+1}{2e}}},\end{aligned}$$

where $e = gcd(s-r, \frac{q+1}{2})$. From Lemma 1, $f(x)$ is bent if and only if

$$e\sum_{u\in U^e} w^{Tr_1^n\left(-au^{\frac{s-r}{e}}\right)+\epsilon u^{\frac{q+1}{2e}}} = -\sum_{u\in\{u\in U:u^d=1\}} w^{\epsilon u^{\frac{q+1}{2}}} + \sum_{u\in\{u\in U:u^d=1\}} w^{Tr_1^n(-au^{s-r})+\epsilon u^{\frac{q+1}{2}}} + w^{f(0)}.$$

From $\#\{u \in U : u^d = 1\} \le d \le 2$ and Lemma 3, $e = 1$, i.e., $gcd(s-r, \frac{q+1}{2}) = 1$. Hence, $gcd(s-r, q+1) = 1$ or $gcd(s-r, q+1) = 2$, $q \equiv 1 \mod 4$. □

We will present the characterization of bentness of $f(x)$ for different values of $gcd(r, q+1)$ and $gcd(s-r, q+1)$.

Theorem 5 *Let $f(x)$ be a p-ary function defined in (5) and $\epsilon \neq 0$.*

(1) If $p \ge 7$, $gcd(r, q+1) = 1$ and $gcd(r-s, q+1) = 1$, then $f(x)$ is regular bent if and only if $-a \notin \mathcal{C}_0$ and $K_m(a^{q+1}) = 1 - \frac{\rho}{\cos\frac{2\pi\epsilon}{p}}$, where $\rho = w^{f(0)} - w^{\epsilon} + w^{-Tr_1^n(a)+\epsilon}$.

(2) If $p \ge 7$, $q \equiv 1 \mod 4$, $gcd(r, q+1) = 1$ and $gcd(s-r, q+1) = 2$, then $f(x)$ is regular bent if and only if $a \notin \mathcal{C}_0$ and $K_m(a^{q+1}) = 1 - \frac{\rho}{\cos\frac{2\pi\epsilon}{p}}$, where $\rho = -w^{\epsilon} + w^{Tr_1^n(-a)+\epsilon} + w^{f(0)}$.

(3) If $p \ge 11$, $gcd(r, q+1) = 2$, and $gcd(s-r, q+1) = 1$, then $f(x)$ is regular bent if and only if $-a \notin \mathcal{C}_0$ and $K_m(a^{q+1}) = 1 - \frac{\rho}{\cos\frac{2\pi\epsilon}{p}}$, where $\rho = -w^{\epsilon} - w^{\epsilon(-1)^{\frac{q+1}{2}}} + w^{Tr_1^n(-a)+\epsilon} + w^{Tr_1^n(a)+\epsilon(-1)^{\frac{q+1}{2}}} + w^{f(0)}$.

(4) If $p \ge 11$, $q \equiv 1 \mod 4$, $gcd(r, q+1) = 2$, and $gcd(s-r, q+1) = 2$, then $f(x)$ is regular bent if and only if $a \notin \mathcal{C}_0$ and $K_m(a^{q+1}) = 1 - \frac{\rho}{\cos\frac{2\pi\epsilon}{p}}$, where $\rho = -w^{\epsilon} - w^{-\epsilon} + w^{Tr_1^n(-a)+\epsilon} + w^{Tr_1^n(-a)-\epsilon} + w^{f(0)}$.

Proof (1) From Theorem 11 in [17], $f(x)$ is regular bent if and only if

$$w^{\epsilon}S_0(-a) + w^{-\epsilon}S_1(-a) = w^{f(0)} - w^{\epsilon} + w^{-Tr_1^n(a)+\epsilon}.$$

Suppose $-a \in \mathcal{C}_0$. From Propositions 2 and 3, there exist integers $c_i (i = 0, 1, \ldots, p-1)$ such that $w^{\epsilon}S_0(-a) + w^{-\epsilon}S_1(-a) = \sum_{i=0}^{p-1} c_i w^i$, where the number of odd c_i is 0 or 2. By Lemma 4,

$$w^{\epsilon}S_0(-a)+w^{-\epsilon}S_1(-a)\neq w^{f(0)}-w^{\epsilon}+w^{-Tr_1^n(a)+\epsilon},$$

i.e., $f(x)$ is not bent. From Theorem 11 in [17], this result can be obtained.

(2) From Proposition 5, $f(x)$ is bent if and only if

$$\sum_{u\in U}w^{Tr_1^n(-au^{s-r})+\epsilon u^{\frac{q+1}{2}}}=-w^{\epsilon}+w^{Tr_1^n(-a)+\epsilon}+w^{f(0)}.$$

Since $q\equiv 1 \mod 4$ and $gcd(s-r,q+1)=2$, then $u\mapsto u^{s-r}$ is a permutation of U_0 and also a bijection from U_1 to U_0. We have

$$\begin{aligned}\sum_{u\in U}w^{Tr_1^n(-au^{s-r})+\epsilon u^{\frac{q+1}{2}}}&=w^{\epsilon}\sum_{u\in U_0}w^{Tr_1^n(-av)}+w^{-\epsilon}\sum_{u\in U_0}w^{Tr_1^n(-av)}\\&=(w^{\epsilon}+w^{\epsilon})\sum_{u\in U_0}w^{Tr_1^n(-av)}\\&=(w^{\epsilon}+w^{\epsilon})\sum_{u\in U_1}w^{Tr_1^n(av)}\quad(-1\in U_1).\end{aligned}$$

Hence, $f(x)$ is regular bent if and only if

$$(w^{\epsilon}+w^{-\epsilon})\sum_{u\in U_1}w^{Tr_1^n(av)}=-w^{\epsilon}+w^{Tr_1^n(-a)+\epsilon}+w^{f(0)}.$$

From a similar discussion as (1), we have $a\notin\mathcal{C}_0$. When $a\notin\mathcal{C}_0$, from Proposition 1,

$$\sum_{u\in U_1}w^{Tr_1^n(av)}=\frac{1-K_m(a^{q+1})}{2}.$$

Hence, this result follows.

(3) Note that $f(x)$ is bent if and only if

$$\begin{aligned}\sum_{u\in U}w^{Tr_1^n(-au^{s-r})+\epsilon u^{\frac{q+1}{2}}}&=-w^{\epsilon}-w^{\epsilon(-1)^{\frac{q+1}{2}}}+w^{Tr_1^n(-a)+\epsilon}\\&\quad+w^{Tr_1^n(a)+\epsilon(-1)^{\frac{q+1}{2}}}+w^{f(0)}.\end{aligned}$$

Since $gcd(s-r,q+1)=1$, then $u\mapsto u^{s-r}$ is a permutation of U_0 and also a permutation of U_1. We have

$$\sum_{u\in U}w^{Tr_1^n(-au^{s-r})+\epsilon u^{\frac{q+1}{2}}}=w^{\epsilon}\sum_{u\in U_0}w^{Tr_1^n(-av)}+w^{-\epsilon}\sum_{u\in U_1}w^{Tr_1^n(-av)}.$$

Hence, $f(x)$ is regular bent if and only if

$$w^{\epsilon}\sum_{u\in U_0} w^{Tr_1^n(-av)} + w^{-\epsilon}\sum_{u\in U_1} w^{Tr_1^n(-av)} = -w^{\epsilon} - w^{\epsilon(-1)^{\frac{q+1}{2}}} + w^{Tr_1^n(-a)+\epsilon} + w^{Tr_1^n(a)+\epsilon(-1)^{\frac{q+1}{2}}} + w^{f(0)}.$$

From a similar discussion as (1), we have $-a \notin \mathcal{C}_0$. When $-a \notin \mathcal{C}_0$, from Proposition 1,

$$\sum_{u\in U_0} w^{Tr_1^n(-av)} = \sum_{u\in U_1} w^{Tr_1^n(-av)} = \frac{1-K_m(a^{q+1})}{2}.$$

Hence, this result follows.

(4) Note that $f(x)$ is bent if and only if

$$\sum_{u\in U} w^{Tr_1^n(-au^{s-r})+\epsilon u^{\frac{q+1}{2}}} = -w^{\epsilon} - w^{-\epsilon} + w^{Tr_1^n(-a)+\epsilon} + w^{Tr_1^n(-a)-\epsilon} + w^{f(0)}.$$

Since $q \equiv 1 \mod 4$ and $gcd(s-r, q+1) = 2$, then $u \mapsto u^{s-r}$ is a permutation of U_0 and also a bijection from U_1 to U_0. We have

$$\begin{aligned}\sum_{u\in U} w^{Tr_1^n(-au^{s-r})+\epsilon u^{\frac{q+1}{2}}} &= w^{\epsilon}\sum_{u\in U_0} w^{Tr_1^n(-av)} + w^{-\epsilon}\sum_{u\in U_0} w^{Tr_1^n(-av)} \\ &= (w^{\epsilon}+w^{-\epsilon})\sum_{u\in U_1} w^{Tr_1^n(av)} \quad (-1 \in U_1).\end{aligned}$$

Hence, $f(x)$ is regular bent if and only if

$$(w^{\epsilon}+w^{-\epsilon})\sum_{u\in U_1} w^{Tr_1^n(av)} = -w^{\epsilon} - w^{-\epsilon} + w^{Tr_1^n(-a)+\epsilon} + w^{Tr_1^n(-a)-\epsilon} + w^{f(0)}.$$

From a similar discussion as (1), we have $a \notin \mathcal{C}_0$. When $a \notin \mathcal{C}_0$, from Proposition 1,

$$\sum_{u\in U_1} w^{Tr_1^n(av)} = \frac{1-K_m(a^{q+1})}{2}.$$

Hence, this result follows. □

Remark Theorem 5 is a generalization of Theorem 11 in [17]. Note that there is a minor error in Theorem 11 in [17], where $\rho = w^{f(0)} - w^{\epsilon} + w^{-Tr_1^n(a)}$ should be $\rho = w^{f(0)} - w^{\epsilon} + w^{-Tr_1^n(a)+\epsilon}$.

4 Conclusion

This paper studies two classes of p-ary regular bent functions introduced by Li et al. [17]. The first class of p-ary functions is defined by

$$f(x) = Tr_1^n \left(ax^{l(q-1)} + bx^{\left(l+\frac{q+1}{2}\right)(q-1)} \right) + \epsilon x^{\frac{q^2-1}{2}},$$

where $a, b \in \mathbb{F}_{q^2}$. We prove that when $gcd(l, q+1) = 1$ and both $a+b$ and $a-b$ are quadratic residues, $f(x)$ is not bent. Further, we present the characterization of these regular bent functions for the case $gcd(l, q+1) = 1$ and the case $gcd(l, q+1) = 2$ and $q \equiv 1 \mod 4$. The second class of p-ary functions is defined by

$$f(x) = \begin{cases} \sum_{i=0}^{q-1} Tr_1^n \left(ax^{(ri+s)(q-1)} \right) + \epsilon x^{\frac{q^2-1}{2}}, & x \neq 0, \\ f(0), & x = 0, \end{cases}$$

where $a \in \mathbb{F}_{q^2}$ and $\epsilon \in \mathbb{F}_p$. When $p \geq 7$ and $\epsilon = 0$, $f(x)$ is not bent. Further, we present the concrete characterization for these functions for different values of $gcd(r, q+1)$ and $gcd(s-r, q+1)$. Our work generalizes results in [17].

Acknowledgements The authors are very grateful to the anonymous reviewers and Prof. Teo Mora for their valuable comments and suggestions. This work is supported by the National Natural Science Foundation of China (Grant Nos. 11401480, 11531002, 11701129). C. Tang also acknowledges support from 14E013, CXTD2014-4 and the Meritocracy Research Funds of China West Normal University. Y. Qi also acknowledges support from Zhejiang provincial Natural Science Foundation of China (LQ17A010008, LQ16A010005).

References

1. Canteaut, A., Charpin, P., Kyureghyan, G.M.: 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.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press, Cambridge (2010)
3. Carlet, C., Mesnager, S., Tang, C., Qi, Y.: Euclidean and Hermitian LCD MDS codes. Des. Codes Cryptogr. (2018). https://doi.org/10.1007/s10623-018-0463-8
4. Charpin, P., Kyureghyan, G.M.: Cubic monomial bent functions: a subclass of $\mathcal{M}$. SIAM J. Discrete Math. **22**(2), 650–665 (2008)
5. Charpin, P., Pasalic, E., Tavernier, C.: On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inf. Theory **51**(12), 4286–4298 (2005)
6. Cohen, G., Honkala, I., Litsyn, S., Lobstein, A.: Covering Codes. North Holland, Amsterdam (1997)
7. Dillon J. F.: Elementary Hadamard difference sets. Ph.D. dissertation, University of Maryland, Collage Park (1974)
8. Ding, C., Fan, C., Zhou, Z.: The dimension and minimum distance of two classes of primitive BCH codes. Finite Fields Appl. **45**, 237–263 (2017)
9. Dobbertin, H., Leander, G., Canteaut, A., Carlet, C., Felke, P., Gaborit, P.: Construction of bent functions via Niho power functions. J. Combin. Theory Ser. A **113**(5), 779–798 (2006)
10. 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)
11. Helleseth, T., Kholosha, A.: On generalized bent functions. In: Proceedings of IEEE Information Theory and Applications Workshop, pp. 1–6 (2010)

12. Helleseth, T., Kholosha, A.: Sequences, Bent functions and Jacobsthal sums. SETA **6338**, 416–429 (2010)
13. 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)
14. Kononen, K.P., Rinta-Aho, M.J., Vaananen, K.O.: On integer values of Kloosterman sums. IEEE Trans. Inf. Theory **56**(8), 4011–4013 (2010)
15. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. J. Combin. Theory Ser. A **40**(1), 90–107 (1985)
16. Leander, N.G.: Monomial bent functions. IEEE Trans. Inf. Theory **52**(2), 738–743 (2006)
17. Li, N., Helleseth, T., Tang, X., Kholosha, A.: Several new classes of bent functions from Dillon exponents. IEEE Trans. Inf. Theory **59**(3), 1818–1831 (2013)
18. Lidl, R., Niederreiter, H.: Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge (1994)
19. Mesnager, S.: Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. IEEE Trans. Inf. Theory **57**(9), 5996–6009 (2011)
20. Mesnager, S., Flori, J.P.: Hyperbent functions via Dillon-like exponents. IEEE Trans. Inf. Theory **59**(5), 3215–3232 (2013)
21. Olsen, J., Scholtz, R., Welch, L.: Bent-function sequences. IEEE Trans. Inf. Theory **28**(6), 858–864 (1982)
22. Tang, C., Qi, Y.: Special values of Kloosterman sums and binomial bent functions. Finite Fields Appl. **41**, 113–131 (2016)
23. Wang, B., Tang, C., Qi, Y., Yang, Y., Xu, M.: A new class of hyper-bent Boolean functions in binomial forms. arxiv.org/pdf/1112.0062.pdf
24. Yu, N.Y., Gong, G.: Constructions of quadratic bent functions in polynomial forms. IEEE Trans. Inf. Theory **52**(7), 3291–3299 (2006)
25. Zheng, D., Yu, L., Hu, L.: On a class of binomial bent functions over the finite fields of odd characteristic. Appl. Algebra Eng. Commun. Comput. **24**(6), 461–475 (2013)