Cryptography and Communications (2019) 11:1133–1144
https://doi.org/10.1007/s12095-019-0355-4

Regular p-ary bent functions with five terms and Kloosterman sums

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

Received: 2 November 2018 / Accepted: 29 January 2019 / Published online: 2 February 2019

Abstract
Kloosterman sums are vital in the study of bent functions, including regular p-ary bent functions. In this paper, a congruence property for Kloosterman sums is presented first and is used to prove the nonexistence of a class of p-ary bent functions. Further, this paper considers p-ary functions of the form $f(x) = \mathrm{Tr}_1^n(a_1 x^{r_1(q-1)}) + \mathrm{Tr}_1^n\left(c_1 x^{r_1(q-1)+\frac{q^2-1}{2}}\right) + \mathrm{Tr}_1^n\left(a_2 x^{r_2(q-1)}\right) + \mathrm{Tr}_1^n\left(c_2 x^{r_2(q-1)+\frac{q^2-1}{2}}\right) + b x^{\frac{q^2-1}{2}}$. We use Kloosterman sums in the characterization of this class of p-ary bent functions. Finally, an open problem of Jia et al. (IEEE Trans Inf. Theory **58**(9): 6054–6063, 2012) is solved and we prove the nonexistence for a class of regular p-ary bent functions.

Keywords Regular bent functions · Walsh transformation · Kloosterman sums · p-ary functions · Congruence

Mathematics Subject Classification (2010) 06E75 · 94A60 · 11T23

1 Introduction

Introduced by Rothaus [17], Boolean bent functions from $\mathbb{F}_2^n$ or $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ have important applications in cryptography, coding theory, and sequences. As a class of Boolean functions

This article is part of the Topical Collection on *Special Issue on Sequences and Their Applications*

✉ Chunming Tang
tangchunmingmath@163.com

Yanfeng Qi
qiyanfeng07@163.com

Dongmei Huang
huangdmmath@163.com

1 School of Mathematics and Information, China West Normal University, Sichuan Nanchong, 637002, China

2 School of Science, Hangzhou Dianzi University, Hangzhou, Zhejiang, 310018, China

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 present characterization and construction of monomial bent functions, binomial bent functions and quadratic bent functions [1–5, 12, 15, 16, 19, 20]. Boolean bent functions were generalized to the notation of functions over an arbitrary finite field in [11]. It is elusive to completely classify bent functions. The characterization of bent functions over finite fields of odd characteristic is more complicate than that of Boolean bent functions. Several work can be found in [7, 8].

Let p be an odd prime and m be an integer. Let $n = 2m$ and $q = p^m$. Let $\mathrm{Tr}_1^n(\cdot)$ be the trace function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_p$. Helleseth and Kholosha [6] studied monomial functions with Dillon type of the form $f_{a,r}(x) = \mathrm{Tr}_1^n(ax^{r(q-1)})$, 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. [9] considered binomial functions of the form $f_{a,b,r}(x) = \mathrm{Tr}_1^n(ax^{r(q-1)}) + bx^{\frac{q^2-1}{2}}$, where $a \in \mathbb{F}_{q^2}, b \in \mathbb{F}_p$ and $\gcd(r, q+1) = 1$. By Kloosterman sums, they presented the characterization of bentness for $f_{a,b,r}$. For $p = 3$ or $q \equiv 3 \pmod 4$, they proved that $f_{a,b,r}$ is bent if and only if $K_m(a) = 1 - \sec \frac{2\pi b}{p}$. Zheng et al. [21] generalized Jia et al.'s result to the case $q \equiv 1 \pmod 4$, i.e., $f_{a,b,r}$ is bent if and only if $K_m(a) = 1 - \sec \frac{2\pi b}{p}$. Further, when $q \equiv 7 \pmod 8$, r is even and $\gcd(\frac{r}{2}, q+1) = 1$, Zheng et al. proved that $f_{a,b,r}(x) = \mathrm{Tr}_1^n(ax^{r(q-1)}) + bx^{\frac{q^2-1}{2}} (a \in \mathbb{F}_{q^2}, b \in \mathbb{F}_p)$ is not bent. This paper generalizes Zheng et al.'s results, presents the characterization of more regular p-ary bent functions and proves the nonexistence of a class of bent functions. Further, this paper also solves an open problem in the case $q \equiv 3 \pmod 8$ presented by Jia et al. [9] and proves that $f_{a,b,r}$ is not bent.

Li et al. [13] considered trinomial functions of the form $f_{a,c,b,r}(x) = \mathrm{Tr}_1^n(ax^{r(q-1)}) + \mathrm{Tr}_1^n\left(cx^{r(q-1)+\frac{q^2-1}{2}}\right) + bx^{\frac{q^2-1}{2}}$, where $a, c \in \mathbb{F}_{q^2}, b \in \mathbb{F}_p$, and $\gcd(r, q+1) = 1$. They presented the relation between the bentness of $f_{a,c,b,r}$ and Kloosterman sums $K_m((a+c)^{q+1})$, $K_m((a-c)^{q+1})$.

With similar methods in [9, 13, 21], this paper generalizes their results and considers functions with five terms of the form

$$\begin{aligned} f(x) = &\ \mathrm{Tr}_1^n(a_1x^{r_1(q-1)}) + \mathrm{Tr}_1^n\left(c_1x^{r_1(q-1)+\frac{q^2-1}{2}}\right) \\ &+\mathrm{Tr}_1^n(a_2x^{r_2(q-1)}) + \mathrm{Tr}_1^n\left(c_2x^{r_2(q-1)+\frac{q^2-1}{2}}\right) + bx^{\frac{q^2-1}{2}}, \end{aligned}$$

where $a_1, a_2, c_1, c_2 \in \mathbb{F}_{q^2}$ and $b \in \mathbb{F}_p$. With the help of Kloosterman sums, we characterize the bentness of this class of p-ary functions. A congruence property of Kloosterman sums is deduced first, which is used to prove the nonexistence of some Dillon type bent functions.

This paper is organized as follows: Section 2 introduces some notations and results on character sums. Section 3 presents a congruence property and proves that some Dillon type functions are not bent. Section 4 presents the characterization of bentness for functions with five terms and solves an open problem proposed by Jia et al. [9]. Section 5 makes a conclusion for this paper.

2 Preliminaries

2.1 Regular bent functions

Throughout this paper, let p be an odd prime and m, n be positive integers. Let $q = p^m$, $\mathbb{F}_q$ be a finite field with q elements and $\mathbb{F}_q^*$ the multiplicative group composed of all nonzero elements in $\mathbb{F}_q$. Let $k|m$ and $\mathrm{Tr}_k^m(x) = \sum_{i=0}^{m/k-1} x^{p^{ki}}$ be the trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^k}$. For any $x \in \mathbb{F}_{q^2}^*$, there exists a unique factorization $x = y * \xi^i$, where $y \in \mathbb{F}_q^*$, $0 \le i \le q$, and ξ is a primitive element of $\mathbb{F}_{q^2}$. Let $U = \{\xi^0, \xi^{(q-1)}, \ldots, \xi^{(q-1)q}\}$, $U_0 = U^2 = \{u^2 : u \in U\}$, and $U_1 = U \setminus U_0$. Sets of squares and nonsquares 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 $\mathcal{C}_0^+ = \{x \in \mathcal{C}_0 : \mathrm{Tr}_1^m(x^{\frac{p^m+1}{2}}) \neq 0\}$.

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 $W_f(\lambda) = \sum_{x \in \mathbb{F}_{p^n}} w^{f(x) - \mathrm{Tr}_1^n(\lambda x)}$,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 $f(x)$. And the dual of a regular p-ary bent function is also bent. Let $n = 2m$ for the rest of the paper.

2.2 Exponential sums

For $a \in \mathbb{F}_{p^n}$, the Kloosterman sum $K_n(a)$ [14] of a is defined by $K_n(a) = \sum_{x \in \mathbb{F}_{p^n}} w^{\mathrm{Tr}_1^n(ax + \frac{1}{x})}$, where $\frac{1}{0} = 0$ for $x = 0$. Since $\overline{K_n(a)} = \sum_{x \in \mathbb{F}_{p^n}} w^{-\mathrm{Tr}_1^n(ax + \frac{1}{x})} = K_n(a)$, then $K_n(a)$ is a real number.

Some notations are defined below.

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

$$Q(a) = 2\mathrm{Tr}_1^m\left(a^{\frac{p^m+1}{2}}\right), a \in \mathcal{C}_0^+;$$

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

Obviously, when $q \equiv 1 \pmod 4$, I is a real number.

The following result on exponential sums is useful [9].

Proposition 1 *Let $a \in \mathbb{F}_{q^2}^*$, then*

$$\sum_{u \in U_0} w^{\mathrm{Tr}_1^n(au)} = \begin{cases} R(a) + I(w^{Q(a)} - w^{-Q(a)}), & a \in \mathcal{C}_0^+, \\ R(a), & otherwise, \end{cases}$$

and

$$\sum_{u \in U_1} w^{\mathrm{Tr}_1^n(au)} = \begin{cases} R(a) - I(w^{Q(a)} - w^{-Q(a)}), & a \in \mathcal{C}_0^+, \\ R(a), & otherwise. \end{cases}$$

3 A congruence property of Kloosterman sums and its application

Lemma 1 *Let $a, x \in \mathbb{F}_q^*$, and $y \in \mathbb{F}_q$.*

(1) *If $y^2 - 4a$ is not a quadratic residue in $\mathbb{F}_q$, then $ax + x^{-1} = y$ has no solution.*
(2) *If $y^2 - 4a = 0$, then $ax + x^{-1} = y$ has only a solution.*
(3) *If $y^2 - 4a$ is a quadratic residue in $\mathbb{F}_q$, then $ax + x^{-1} = y$ has two solutions.*

Proof The equation $ax + x^{-1} = y$ can be transformed into $ax^2 - yx + 1 = 0$. And $\Delta = y^2 - 4a$ is the discriminant for $ax^2 - yx + 1 = 0$. Hence, Results (1), (2), and (3) are obviously obtained. □

Proposition 2 *Let w be a primitive p-th root of unity and $Q(w)$ be the p-th cyclotomic field over rational field Q. Let $\mathfrak{R}$ be a prime ideal lying above 2 in $Q(w)$ and $a \in \mathbb{F}_q^*$, then*

(1) $K_m(a) \equiv 1 \pmod{\mathfrak{R}}$ *if and only if a is a nonsquare or a is a square satisfying* $\mathrm{Tr}_1^m(\sqrt{a}) = 0$.
(2) $K_m(a) \equiv 1 + w^t + w^{-t} \pmod{\mathfrak{R}} (1 \le t \le p-1)$ *if and only if a is a square and* $\mathrm{Tr}_1^m(2\sqrt{a}) = \pm t$.

Proof We first prove that when $1 \le t \le p-1$, $1 + w^t + w^{-t} \not\equiv 1 \pmod{\mathfrak{R}}$, and when $1 \le t_2 < t_1 \le \frac{p-1}{2}$, $1 + w^{t_1} + w^{-t_1} \not\equiv 1 + w^{t_2} + w^{-t_2} \pmod{\mathfrak{R}}$. Note that $w \not\equiv 1 \pmod{\mathfrak{R}}$, i,e, $w \pmod{\mathfrak{R}}$ is also a primitive p-th root of unity. If $1 + w^t + w^{-t} \equiv 1 \pmod{\mathfrak{R}}$, then $w^t + w^{-t} \equiv 0 \pmod{\mathfrak{R}}$, i,e, $w^{2t} \equiv 1 \pmod{\mathfrak{R}}$. Then $t \equiv 0 \pmod{p}$, which makes a contradiction with the supposition of t. Hence, $1 + w^t + w^{-t} \not\equiv 1 \pmod{\mathfrak{R}}$. If $1 + w^{t_1} + w^{-t_1} \equiv 1 + w^{t_2} + w^{-t_2} \pmod{\mathfrak{R}}$, then $(w^{t_1+t_2} + 1)(w^{t_1-t_2} + 1) \equiv 0 \pmod{\mathfrak{R}}$. From the supposition of t_1, t_2, $w^{t_1+t_2} \not\equiv 1 \pmod{\mathfrak{R}}$, $w^{t_1-t_2} \not\equiv 1 \pmod{\mathfrak{R}}$. Then it makes a contradiction. Hence, $1 + w^{t_1} + w^{-t_1} \not\equiv 1 + w^{t_2} + w^{-t_2} \pmod{\mathfrak{R}}$.

From the definition of Kloosterman sums, we have

$$\begin{aligned} K_m(a) &= 1 + \sum_{x \in \mathbb{F}_q^*} w^{\mathrm{Tr}_1^m(ax + x^{-1})} \\ &= 1 + \sum_{y \in \mathbb{F}_q} w^{\mathrm{Tr}_1^m(y)} \#\{x \in \mathbb{F}_q^* : ax + x^{-1} = y\}. \end{aligned}$$

From Lemma 1,

$$\begin{aligned} K_m(a) &= 1 + \sum_{y \in \mathbb{F}_q} w^{\mathrm{Tr}_1^m(y)} \#\{x \in \mathbb{F}_q^* : ax + x^{-1} = y\} \\ &\equiv 1 + \sum_{y \in \mathbb{F}_q, y^2 - 4a = 0} w^{\mathrm{Tr}_1^m(y)} \pmod{\mathfrak{R}}. \end{aligned}$$

If a is a nonsquare, then $K_m(a) \equiv 1 \pmod{\mathfrak{R}}$.

If a is a square and $\mathrm{Tr}_1^m(\sqrt{a}) = 0$, then $K_m(a) \equiv 1 \pmod{\mathfrak{R}}$.

If a is a square, and $\mathrm{Tr}_1^m(2\sqrt{a}) = t$, then $K_m(a) \equiv 1 + w^t + w^{-t} \pmod{\mathfrak{R}}$.

Hence, this proposition follows. □

Remark 1 From Proposition 2, $K_m(a) \pmod{\mathfrak{R}} \in \{1 + w^t + w^{-t} \pmod{\mathfrak{R}} : 0 \le t \le \frac{p-1}{2}\}$.

Proposition 2 can be used to discuss the nonexistence of some regular p-ary bent functions. The following theorem demonstrates that some regular p-ary bent functions in Theorem 10 in [13] do not exist.

Theorem 1 *Let p be a prime bigger than 7, and 2 be a primitive root modulo p. Let $a \in \mathbb{F}_{q^2}$, and r, s be two integers satisfying $\gcd(s-r, q+1) = 1$. Then the function $f(x) = \sum_{i=0}^{q-1} \mathrm{Tr}_1^n(ax^{(ri+s)(q-1)})$ is not bent.*

Proof From Theorem 10 in [13], $f(x)$ is regular bent if and only if $\mathrm{Tr}_1^n(a) = f(0)$ and $K_m(a^{q+1}) = 2 - w^{f(0)} - w^{-f(0)}$. Denote $f(0) = i$. From Proposition 2, we just need to prove that

$$2 - w^i - w^{-i} \not\equiv 1 + w^t + w^{-t} \pmod{\mathfrak{R}},$$

where $\mathfrak{R}$ is a prime ideal lying above 2 in $Q(w)$ and $0 \le t \le \frac{p-1}{2}$. Hence, we just prove that

$$w^t + w^{p-1-t} + w^i + w^{p-1-i} + 1 \not\equiv 0 \pmod{\mathfrak{R}}.$$

Suppose that $w^t + w^{p-1-t} + w^i + w^{p-1-i} + 1 \equiv 0 \pmod{\mathfrak{R}}$. Then $w^t + w^{p-1-t} + w^i + w^{p-1-i} + 1 \pmod{\mathfrak{R}}$ is an annihilating polynomial with no more than 5 terms of no more than $p-1$ degree over $\mathbb{F}_2$. Since 2 is a primitive root modulo p, there is only an annihilating polynomial $w^{p-1} + w^{p-2} + \cdots + w + 1 \pmod{\mathfrak{R}}$ of no more than $p-1$ degree over $\mathbb{F}_2$. Since $p \ge 7$, $w^{p-1} + w^{p-2} + \cdots + w + 1 \pmod{\mathfrak{R}}$ has more than 5 terms, which makes a contradiction. Hence, $w^t + w^{p-1-t} + w^i + w^{p-1-i} + 1 \not\equiv 0 \pmod{\mathfrak{R}}$, and this theorem follows. □

Remark 2 The prime required in the above theorem is just an Artin prime for 2. Let $S(2)$ be the set of primes p such that 2 is a primitive root modulo p. Then $S(2)$ has a positive asymptotic density inside the set of primes. Let P_i and AP_i be the numbers of primes and primes in $S(2)$ between 3 and 10^i. Artin conjecture claims that $S(2)$ has the density $C_{artin} \approx 0.3739558136\ldots$. Table 1 lists some values for $\frac{AP_i}{P_i}$. And all the primes in $S(2)$ less than 100 are 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83.

4 Regular bent functions with five terms

In this section, we consider functions of the form

$$\begin{aligned} f(x) = \mathrm{Tr}_1^n(a_1 x^{r_1(q-1)}) + \mathrm{Tr}_1^n\left(c_1 x^{r_1(q-1)+\frac{q^2-1}{2}}\right) + \mathrm{Tr}_1^n\left(a_2 x^{r_2(q-1)}\right) \\ + \mathrm{Tr}_1^n\left(c_2 x^{r_2(q-1)+\frac{q^2-1}{2}}\right) + bx^{\frac{q^2-1}{2}}, \end{aligned} \tag{1}$$

where $a_1, c_1, a_2, c_2 \in \mathbb{F}_{q^2}$, and $b \in F_p$. If $b = 0$, and $a_1, c_1, a_2, c_2 \in \mathbb{F}_{q^2}^*$, $f(x)$ has four terms.

Table 1 The density of Artin primes for 2

$\frac{AP_3}{P_3}$ (%)	$\frac{AP_4}{P_4}$ (%)	$\frac{AP_5}{P_5}$ (%)	$\frac{AP_6}{P_6}$ (%)	$\frac{AP_7}{P_7}$ (%)	$\frac{AP_8}{P_8}$ (%)
40.1198	38.2736	37.5665	37.3785	37.3908	37.3991

In convenience, we denote the function over U induced by $f(x)$

$$\widetilde{f}(u) = \mathrm{Tr}_1^n(a_1 u^{r_1}) + \mathrm{Tr}_1^n\left(c_1 u^{r_1+\frac{q+1}{2}}\right) + \mathrm{Tr}_1^n(a_2 u^{r_2}) + \mathrm{Tr}_1^n\left(c_2 u^{r_2+\frac{q+1}{2}}\right) + b u^{\frac{q+1}{2}}.$$

Define an exponential sum

$$S_f = \sum_{u\in U} w^{\widetilde{f}(u)}. \tag{2}$$

Then the following lemma determines regular bent function $f(x)$.

Lemma 2 *Let $f(x)$ be a p-ary function defined in (1) and S_f be the exponential sum in (2). Then $f(x)$ is bent if and only if $S_f = 1$. Further, if $f(x)$ is bent, then $f(x)$ is regular bent.*

Proof Suppose $f(x)$ is bent. For $\lambda \in \mathbb{F}_{q^2}^*$,

$$\begin{aligned} W_f(\lambda) &= \sum_{x\in\mathbb{F}_{q^2}} w^{f(x)-\mathrm{Tr}_1^n(\lambda x)} \\ &= 1 + \sum_{i=0}^{q} w^{f(\xi^i)} \sum_{y\in\mathbb{F}_q^*} w^{-\mathrm{Tr}_1^n(\lambda\xi^i y)} \\ &= 1 + \sum_{i=0}^{q} w^{f(\xi^i)} \sum_{y\in\mathbb{F}_q^*} w^{-\mathrm{Tr}_1^m((\lambda\xi^i+\lambda^q(\xi^i)^q)y)} \\ &= 1 - \sum_{i=0}^{q} w^{f(\xi^i)} + \sum_{i=0}^{q} w^{f(\xi^i)} \sum_{y\in\mathbb{F}_q} w^{-\mathrm{Tr}_1^m((\lambda\xi^i+\lambda^q(\xi^i)^q)y)} \\ &= 1 - \sum_{i=0}^{q} w^{f(\xi^i)} + q \sum_{0\le i\le q,\lambda\xi^i+\lambda^q(\xi^i)^q=0} w^{f(\xi^i)} \\ &= 1 - \sum_{u\in U} w^{\widetilde{f}(u)} + q w^{f(\xi^{i_\lambda})}, \end{aligned}$$

where i_λ is the unique number such that $0 \le i_\lambda \le q, \lambda\xi^{i_\lambda} + \lambda^q(\xi^{i_\lambda})^q = 0$. From the definition of S_f,

$$W_f(\lambda) = 1 - S_f + q w^{f(\xi^{i_\lambda})}. \tag{3}$$

Since $f(x)$ is bent, from Property 8 in [11], there exists $0 \le j \le p-1$ satisfying $W_f(\lambda) = \pm q w^j$. From (3), we have $S_f - 1 - q w^{f(\xi^{i_\lambda})} \pm q w^j = 0$. Suppose that $S_f - 1 - q w^{f(\xi^{i_\lambda})} - q w^j = 0$. Then we have

$$\sum_{k=0}^{p-1} N_k w^k - 1 - q w^{f(\xi^{i_\lambda})} - q w^j = 0 \tag{4}$$

where $N_i = \#\{u \in U : \widetilde{f}(u) = i\}$. Obviously, $N_0 + N_1 + \cdots + N_{p-1} = q + 1$. Since $f(x)$ is bent, then $1 \le N_i \le q$. Since the minimal polynomial of w is $w^{p-1} + w^{p-2} + \cdots +$

$w+1=0$, (4) does not hold. Hence, $S_f - 1 - qw^{f(\xi^{i_\lambda})} + qw^j = 0$, i.e., $j = f(\xi^{i_\lambda})$. We have $S_f = 1$.

On the other hand,

$$\begin{aligned} W_f(0) &= \sum_{x\in\mathbb{F}_{q^2}} w^{f(x)} \\ &= 1 + \sum_{i=0}^{q} \sum_{y\in\mathbb{F}_q^*} w^{f(y\xi^i)} \\ &= 1 + \sum_{i=0}^{q} \sum_{y\in\mathbb{F}_q^*} w^{f(\xi^i)} \\ &= 1 + (q-1)\sum_{i=0}^{q} w^{f(\xi^i)} \\ &= 1 + (q-1)\sum_{u\in U} w^{\widetilde{f}(u)}. \end{aligned}$$

From the definition of $\widetilde{f}(u)$ and S_f, we have

$$W_f(0) = 1 + (q-1)S_f. \tag{5}$$

If $S_f = 1$, from (3) and (5), $f(x)$ is bent.

If $f(x)$ is bent, from (3) and (5), $f(x)$ is regular bent.

Hence, this lemma follows. □

The following lemma gives a simpler expression for S_f.

Lemma 3 *Let $f(x)$ be a p-ary function defined in* (1) *and S_f be the exponential sum in* (2). *Then*

$$S_f = w^b \sum_{u\in U_0} w^{\mathrm{Tr}_1^n((a_1+c_1)u^{r_1})+\mathrm{Tr}_1^n((a_2+c_2)u^{r_2})} + w^{-b}\sum_{u\in U_1} w^{\mathrm{Tr}_1^n((a_1-c_1)u^{r_1})+\mathrm{Tr}_1^n((a_2-c_2)u^{r_2})}.$$

Proof We have

$$\begin{aligned} S_f &= \sum_{u\in U} w^{\widetilde{f}(u)} \\ &= \sum_{u\in U_0} w^{\widetilde{f}(u)} + \sum_{u\in U_1} w^{\widetilde{f}(u)} \\ &= \sum_{u\in U_0} w^{\mathrm{Tr}_1^n((a_1+c_1)u^{r_1})+\mathrm{Tr}_1^n((a_2+c_2)u^{r_2})+b} + \sum_{u\in U_1} w^{\mathrm{Tr}_1^n((a_1-c_1)u^{r_1})+\mathrm{Tr}_1^n((a_2-c_2)u^{r_2})-b} \\ &= w^b \sum_{u\in U_0} w^{\mathrm{Tr}_1^n((a_1+c_1)u^{r_1})+\mathrm{Tr}_1^n((a_2+c_2)u^{r_2})} + w^{-b}\sum_{u\in U_1} w^{\mathrm{Tr}_1^n((a_1-c_1)u^{r_1})+\mathrm{Tr}_1^n((a_2-c_2)u^{r_2})}, \end{aligned}$$

which completes the proof. □

For general $f(x)$, S_f is difficult to compute. We consider a subclass of functions in (1) defined by

$$f(x) = \mathrm{Tr}_1^n\left(a_1 x^{r_1(q-1)}\right) + \mathrm{Tr}_1^n\left(a_1 x^{r_1(q-1)+\frac{q^2-1}{2}}\right) + \mathrm{Tr}_1^n(a_2 x^{r_2(q-1)})$$
$$-\mathrm{Tr}_1^n\left(a_2 x^{r_2(q-1)+\frac{q^2-1}{2}}\right) + bx^{\frac{q^2-1}{2}}, \quad (6)$$

where $a_1, a_2 \in \mathbb{F}_{q^2}$ and $b \in F_p$.

Lemma 4 *Let $f(x)$ be a p-ary function defined in (6) and S_f be the exponential sum in (2). Then $S_f = w^b \sum_{u\in U_0} w^{\mathrm{Tr}_1^n(2a_1u^{r_1})} + w^{-b}\sum_{u\in U_1} w^{\mathrm{Tr}_1^n(2a_2u^{r_2})}$.*

Proof From Lemma 3, this lemma can be obviously obtained. □

Theorem 2 *Let $f(x)$ be a p-ary function defined in (6). Let $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$ and r_2 be odd. Then $f(x)$ is regular bent if and only if*

$$w^b K_m\left(4a_1^{q+1}\right) + w^{-b}K_m\left(4a_2^{q+1}\right) = \begin{cases} M(A-B)+C-2, & 2a_1, 2a_2 \in \mathcal{C}_0^+; \\ MA+C-2, & 2a_1 \in \mathcal{C}_0^+, 2a_2 \notin \mathcal{C}_0^+; \\ -MB+C-2, & 2a_1 \notin \mathcal{C}_0^+, 2a_2 \in \mathcal{C}_0^+; \\ C-2, & 2a_1, 2a_2 \notin \mathcal{C}_0^+. \end{cases}$$

where $M = 4I\sqrt{-1}$, $A = w^b \sin\frac{2\pi Q(2a_1)}{p}$, $B = w^{-b}\sin\frac{2\pi Q(2a_2)}{p}$, and $C = 2\cos\frac{2\pi b}{p}$.

Proof Since $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$ and r_2 is odd, the map $u \longmapsto u^{r_1}$ is a permutation from U_0 to U_0 and $u \longmapsto u^{r_2}$ is a permutation from U_1 to U_1. From Lemma 4, $S_f = w^b\sum_{u\in U_0} w^{\mathrm{Tr}_1^n(2a_1u)} + w^{-b}\sum_{u\in U_1} w^{\mathrm{Tr}_1^n(2a_2u)}$. From Proposition 1 and Lemma 2, this theorem follows. □

Corollary 1 *Let $f(x)$ be a p-ary function defined in (6). Let $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$, r_2 be odd and $b = 0$. Then $f(x)$ is regular bent if and only if*

$$K_m\left(4a_1^{q+1}\right)+K_m\left(4a_2^{q+1}\right) = \begin{cases} 4I\sqrt{-1}\left[\sin\frac{2\pi Q(2a_1)}{p} - \sin\frac{2\pi Q(2a_2)}{p}\right], & 2a_1, 2a_2 \in \mathcal{C}_0^+; \\ 4I\sqrt{-1}\sin\frac{2\pi Q(2a_1)}{p}, & 2a_1 \in \mathcal{C}_0^+, 2a_2 \notin \mathcal{C}_0^+; \\ -4I\sqrt{-1}\sin\frac{2\pi Q(2a_2)}{p}, & 2a_1 \notin \mathcal{C}_0^+, 2a_2 \in \mathcal{C}_0^+; \\ 0, & 2a_1, 2a_2 \notin \mathcal{C}_0^+. \end{cases}$$

In particular, if $q \equiv 1 \pmod 4$, then $f(x)$ is regular bent if and only if $K_m(4a_1^{q+1}) + K_m(4a_2^{q+1}) = 0$.

Proof From Theorem 2 , the first part of this corollary can be obviously obtained. Note that $K_m\left(4a_1^{q+1}\right)$ and $K_m\left(4a_2^{q+1}\right)$ are real. Since $q \equiv 1 \pmod 4$, I is real. Hence, the rest part of this corollary also holds. □

Example: Let $p = 7, m = 2, n = 2m, q = p^m \equiv 1 \pmod 4$, and $w = e^{\frac{2\pi\sqrt{-1}}{p}}$. Let $\mathbb{F}_{q^2} = \mathbb{F}_p(\xi)$, where the minimal polynomial of ξ is $w^4 + 5w^2 + 4w + 3 = 0$. Then ξ is a primitive element of $\mathbb{F}_{q^2}$. Take r_1, r_2 satisfying $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$ and r_2 is odd. Let $b = 0$, $a_1 = \xi^{289}$, and $a_2 = \xi^{841}$. Then $K_m\left(4a_1^{q+1}\right) = -6w^5 - 4w^4 - 4w^3 - 6w^2 - 1$ and $K_m\left(4a_2^{q+1}\right) = 6w^5 + 4w^4 + 4w^3 + 6w^2 + 1$. And $K_m\left(4a_1^{q+1}\right) + K_m(4a_2^{q+1}) = 0$. From Corollary 1, the function defined in (6) is a regular bent function with four terms.

Corollary 2 *Let $f(x)$ be a p-ary function defined in (6). Let $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$, r_2 be odd, $b \neq 0$ and $2a_1, 2a_2 \notin \mathcal{C}_0^+$. Then $f(x)$ is regular bent if and only if $K_m\left(4a_1^{q+1}\right) = K_m\left(4a_2^{q+1}\right) = 1 - \sec\frac{2\pi b}{p}$.*

Proof From Theorem 2, if $2a_1, 2a_2 \notin \mathcal{C}_0^+$, $f(x)$ is regular bent if and only if $w^b K_m\left(4a_1^{q+1}\right) + w^{-b} K_m\left(4a_2^{q+1}\right) = 2\cos\frac{2\pi b}{p} - 2$. Take the complex conjugate of both sides. And we have $w^{-b} K_m\left(4a_1^{q+1}\right) + w^b K_m\left(4a_2^{q+1}\right) = 2\cos\frac{2\pi b}{p} - 2$. Since $b \neq 0$, we have $K_m\left(4a_1^{q+1}\right) = K_m\left(4a_2^{q+1}\right) = 1 - \sec\frac{2\pi b}{p}$. Hence, this corollary follows. □

Remark 3 From Corollary 2 and Theorem 3.9 in [18], if $p = 11$, $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$ and r_2 is odd, then for any $2a_1, 2a_2 \notin \mathcal{C}_0^+$ and $b \neq 0$, the function $f(x)$ defined in (6) is not bent.

Example. Let $p = 5, m = 4, n = 2m, q = p^m \equiv 1 \pmod 4$, and $w = e^{\frac{2\pi\sqrt{-1}}{p}}$. Let $\mathbb{F}_{q^2} = \mathbb{F}_p(\xi)$, where the minimal polynomial of ξ is $\xi^8 + \xi^4 + 3\xi^2 + 4\xi + 2 = 0$. Then ξ is a primitive element of $\mathbb{F}_{q^2}$. Take r_1, r_2 satisfying $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$ and r_2 is odd. Take $b = 1$, $a_1 = \xi^{64401}$, and $a_2 = \xi^{374925}$. Then $2a_1, 2a_2 \notin \mathcal{C}_0^+$ and $K_m(4a_1^{q+1}) = K_m\left(4a_2^{q+1}\right) = 1 - \sec\frac{2\pi}{p} = -\sqrt{5}$. From Corollary 2, the function defined in (6) is a regular bent function with five terms.

Corollary 3 *Let $f(x)$ be a p-ary function defined in (6). Let $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$, r_2 be odd, $b = 0$, and $a_1 = a_2 = a$. Then $f(x)$ is regular bent if and only if $K_m\left(4a^{q+1}\right) = 0$.*

Proof From Corollary 1, this corollary can be obviously obtained. □

Remark 4 Kononen et al. [10] proved that if $p \geq 5$, for any $a \in \mathbb{F}_q$, $K_m(a) \neq 0$. Hence, if $p \geq 5$, a p-ary function in Corollary 3 is not bent.

Example. Let $p = 3, m = 4, n = 2m, q = p^m \equiv 1 \pmod 4$, and $w = e^{\frac{2\pi\sqrt{-1}}{p}}$. Let $\mathbb{F}_{q^2} = \mathbb{F}_p(\xi)$, where the minimal polynomial of ξ is $\xi^8 + 2\xi^5 + \xi^4 + 2\xi^2 + 2\xi + 2 = 0$. Then

ξ is a primitive element of $\mathbb{F}_{q^2}$. Take r_1, r_2 satisfying $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$ and r_2 is odd. Take $b = 0$, $a_1 = a_2 = a = \xi^{434}$. Then $K_m(4a^{q+1}) = 0$. From Corollary 3, the function defined in (6) is a regular bent function with four terms.

Corollary 4 *Let $f(x)$ be a p-ary function defined in (6). Let $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$, r_2 be odd, $a_1 = a_2 = a$ and $b \neq 0$. Then $f(x)$ is regular bent if and only if*

$$K_m(4a^{q+1}) = \begin{cases} -4I \sin\frac{2\pi b}{p} \sin\frac{2\pi Q(2a)}{p} \sec\frac{2\pi b}{p} + 1 - \sec\frac{2\pi b}{p}, & 2a \in C_0^+; \\ 1 - \sec\frac{2\pi b}{p}, & 2a \notin C_0^+. \end{cases}$$

In particular, if $q \equiv 3 \pmod 4$, $f(x)$ is regular bent if and only if $K_m\left(4a^{q+1}\right) = 1 - \sec\frac{2\pi b}{p}$.

Proof Note that if $q \equiv 3 \pmod 4$, then I is not real. From Theorem 2, this corollary can be obviously obtained. □

Theorem 3 *Let $f(x)$ be a p-ary function defined in (6). Let $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$ and r_2 be even. Then $f(x)$ is bent if and only if*

$$w^b K_m\left(4a_1^{q+1}\right) + w^{-b} K_m(4a_2^{q+1}) = \begin{cases} M(A+B) + C - 2, & 2a_1, 2a_2 \in C_0^+; \\ MA + C - 2, & 2a_1 \in C_0^+, 2a_2 \notin C_0^+; \\ MB + C - 2, & 2a_1 \notin C_0^+, 2a_2 \in C_0^+; \\ C - 2, & 2a_1, 2a_2 \notin C_0^+. \end{cases}$$

where $M = 4I\sqrt{-1}$, $A = w^b \sin\frac{2\pi Q(2a_1)}{p}$, $B = w^{-b} \sin\frac{2\pi Q(2a_2)}{p}$, and $C = 2\cos\frac{2\pi b}{p}$.

Proof Since $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$ and r_2 is even, then the map $u \longmapsto u^{r_1}$ is a permutation from U_0 to U_0 and $u \longmapsto u^{r_2}$ is a bijection between U_1 and U_0. From Lemma 4, $S_f = w^b \sum_{u \in U_0} w^{\mathrm{Tr}_1^n(2a_1 u)} + w^{-b} \sum_{u \in U_0} w^{\mathrm{Tr}_1^n(2a_2 u)}$. From Proposition 1 and Lemma 2, this theorem follows. □

Example. Let $p = 3$, $m = 6$ and $n = 2m$. Let $\mathbb{F}_{q^2} = \mathbb{F}_p(\xi)$, where the minimal polynomial of ξ is $\xi^{12} + \xi^6 + \xi^5 + \xi^4 + \xi^2 + 2 = 0$. Then ξ is a primitive element of $\mathbb{F}_{q^2}$. Take r_1, r_2 satisfying $\gcd\left(r_1, \frac{q+1}{2}\right) = \gcd\left(r_2, \frac{q+1}{2}\right) = 1$ and r_2 is even. Take $b = 1$, $a_1 = \xi^{88976}$ and $a_2 = \xi^{325189}$. Then $2a_1, 2a_2 \notin C_0^+$ and $K_m\left(4a_1^{q+1}\right) = K_m\left(4a_2^{q+1}\right) = 1 - \sec\left(\frac{2\pi}{p}\right) = 3$. From Theorem 3, the function defined in (6) is a regular bent function with five terms.

Theorem 4 *Let $f(x)$ be a p-ary function defined in (1). If $\gcd\left(r_1, r_2, \frac{q+1}{2}\right) > 1$, then $f(x)$ is not bent.*

Proof Let $d = \gcd\left(r_1, r_2, \frac{q+1}{2}\right)$. From Lemma 3,

$$S_f = dw^b \sum_{v \in \mathcal{H}_0} w^{\mathrm{Tr}_1^n((a_1+c_1)u^{r_1/d}) + \mathrm{Tr}_1^n((a_2+c_2)u^{r_2/d})} + dw^{-b} \sum_{v \in \mathcal{H}_1} w^{\mathrm{Tr}_1^n((a_1-c_1)u^{r_1/d}) + \mathrm{Tr}_1^n((a_2-c_2)u^{r_2/d})},$$

where $\mathcal{H}_0 = U_0^d$ and $\mathcal{H}_1 = U_1^d$. Hence, $S_f \equiv 0 \pmod{d}$. Since $d > 1$, then $S_f \neq 1$. From Lemma 2, $f(x)$ is not bent. □

Corollary 5 *Let* $q \equiv 3 \pmod 4$. *Let* $f(x) = \mathrm{Tr}_1^n(ax^{r(p^m-1)}) + bx^{\frac{q^2-1}{2}}$, *where* $a \in \mathbb{F}_q$, $b \in \mathbb{F}_p$, *r is even, and* $\gcd(\frac{r}{2}, q+1) = 1$. *Then* $f(x)$ *is not bent.*

Proof In Theorem 4, take $a_1 = a$, $c_1 = 0$, $a_2 = c_2 = 0$, $r_1 = r$, and $r_2 = 0$. Then $2 | \gcd\left(r, 0, \frac{q+1}{2}\right)$. From Theorem 4, $f(x)$ is not bent. □

Remark 5 Corollary 5 is a generalization of Theorem 3 in [21]. [21] just discussed the case $q \equiv 7 \pmod 8$ and did not solve the case $q \equiv 3 \pmod 8$.

5 Conclusion

This paper first presents a congruence property for Kloosterman sums and with it prove the nonexistence of some regular p-ary bent functions. Further, we study p-ary functions of the form $f(x) = \mathrm{Tr}_1^n\left(a_1x^{r_1(q-1)}\right) + \mathrm{Tr}_1^n\left(a_1x^{r_1(q-1)+\frac{q^2-1}{2}}\right) + \mathrm{Tr}_1^n\left(a_2x^{r_2(q-1)}\right) - \mathrm{Tr}_1^n\left(a_2x^{r_2(q-1)+\frac{q^2-1}{2}}\right) + bx^{\frac{q^2-1}{2}}$ and characterize the bentness of these functions with Kloosterman sums. Finally, we solve an open problem in [9] and prove the nonexistence of some regular bent functions. A natural problem is to study general regular p-ary bent functions of the form $f(x) = \mathrm{Tr}_1^n\left(a_1x^{r_1(q-1)}\right) + \mathrm{Tr}_1^n\left(c_1x^{r_1(q-1)+\frac{q^2-1}{2}}\right) + \mathrm{Tr}_1^n\left(a_2x^{r_2(q-1)}\right) + \mathrm{Tr}_1^n\left(c_2x^{r_2(q-1)+\frac{q^2-1}{2}}\right) + bx^{\frac{q^2-1}{2}}$, which is our further work.

Acknowledgments We would like to thank the anonymous reviewers and Prof. Claude Carlet for their helpful comments and suggestions. This work is supported by the National Natural Science Foundation of China (Grant No. 11871058, 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.: A new class of monomial bent functions. Finite Fields Appl. **14**(1), 221–241 (2008)

2. Charpin, P., Kyureghyan, G.: Cubic monomial bent functions: A subclass of $\mathcal{M}$. SIAM J. Discr. Math. **22**(2), 650–665 (2008)
3. Charpin, P., Pasalic, E., Tavernier, C.: On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inf. Theory **51**(12), 4286–4298 (2005)
4. Dillon, J.F.: Elementary Hadamard difference sets. Ph.D. disserta-tion. Univ Maryland, Collage Park (1974)
5. Dobbertin, H., Leander, G., Canteaut, A., Carlet, C., Felke, P., Ga-borit, P.: Construction of bent functions via Niho power functions. J. Comb. Theory, Ser. A **113**(5), 779–798 (2006)
6. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(2), 2018–2032 (2006)
7. Helleseth, T., Kholosha, A.: On generalized bent functions. In: Proc. IEEE Inf. Theory Appl. Workshop, pp. 1–6 (2010)
8. Helleseth, T., Kholosha, A.: Sequences, bent functions and Jacob-sthal sums. Lecture Notes Comput. Sci. **6338**, 416–429 (2010)
9. 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)
10. Kononen, K.P., Rinta-aho, M.J., Väänänen, K.O.: On integer values of Kloosterman sums. IEEE Trans. Inf. Theory **56**(8), 4011–4013 (2010)
11. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. J. Combin. Theory Ser. A **40**, 90–107 (1985)
12. Leander, G.: Monomial bent functions. IEEE Trans. Inf. Theory **2**(52), 738–743 (2006)
13. 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)
14. Lidl, R., Niederreiter, H.: Introduction to finite fields and applications. Cambridge University Press, Cambridge (1994)
15. 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)
16. Mesnager, S., Flori, J.: Hyper-bent functions via Dillon-like exponents. IEEE Trans. Inf. Theory **59**(5), 3215–3232 (2013)
17. Rothaus, O.S.: On bent functions. J. Combinatorial Theory Ser. A **20**, 300–305 (1976)
18. Tang, C., Qi, Y.: Special values of Kloosterman sums and binomial bent functions. Finite Fields Appl. **41**, 113–131 (2016)
19. Wang, B., Tang, C., Qi, Y., Yang, Y., Xu, M.: A new class of hyper-bent Boolean functions in binomial forms [Online]. Available: arXiv:pdf/1112.0062.pdf
20. Yu, N.Y., Gong, G.: Constructions of quadratic bent functions in polynomial forms. IEEE Trans. Inf. Theory **52**(7), 3291–3299 (2006)
21. 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)