AAECC (2017) 28:155–176
DOI 10.1007/s00200-016-0298-3

ORIGINAL PAPER

Several classes of Boolean functions with few Walsh transform values

Guangkui Xu[1,2] · **Xiwang Cao**[1,3] · **Shanding Xu**[1]

Received: 13 February 2016 / Revised: 16 June 2016 / Accepted: 25 July 2016 /
Published online: 20 August 2016
© Springer-Verlag Berlin Heidelberg 2016

Abstract In this paper, several classes of Boolean functions with few Walsh transform values, including bent, semi-bent and five-valued functions, are obtained by adding the product of two or three linear functions to some known bent functions. Numerical results show that the proposed class contains cubic bent functions that are affinely inequivalent to all known quadratic ones.

Keywords Boolean function · Bent function · Semi-bent function · Five-valued function · Walsh transform

Mathematics Subject Classification 94A60 · 94C10 · 06E30

1 Introduction

For a positive integer n, let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements, $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n}\backslash\{0\}$. A Boolean function is a mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. The Walsh transform is a powerful

✉ Guangkui Xu
xuguangkuiy@163.com

✉ Xiwang Cao
xwcao@nuaa.edu.cn

Shanding Xu
sdxzx11@163.com

[1] School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China

[2] Department of Applied Mathematics, Huainan Normal University, Huainan 232038, China

[3] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

tool to investigate cryptographic properties of Boolean functions which have wide applications in cryptography and coding theory. An interesting problem is to find Boolean functions with few Walsh transform values and determine their distributions. Bent functions, introduced by Rothaus [27], are Boolean functions with two Walsh transform values and achieve the maximum Hamming distance to all affine Boolean functions. Such functions have been extensively studied because of their important applications in coding theory [2,20], cryptography [6], sequence designs [26] and graph theory [12,29]. Complete classification of bent functions seems elusive even in the binary case. However, a number of recent interesting results on bent functions have been found through primary constructions and secondary constructions (see [3,4,7,10,15,17,19,21,23,25,33], and references therein).

As a particular case of the so-called plateaued Boolean functions [34], semi-bent functions are an important kind of Boolean functions with three Walsh transform values. The term of semi-bent function introduced by Chee et al. [11]. Semi-bent functions investigated under the name of three-valued almost optimal Boolean functions in [2], i.e., they have the highest possible nonlinearity in three-valued functions. They are also nice combinatorial objects and have wide applications in cryptography and coding theory. A lot of research work has been devoted to finding new families of semi-bent functions (see [8,10,13,17,22,28,30] and the references therein). However, there is only a few known constructions of semi-bent functions. In general, it is difficult to characterize all functions with few Walsh transform values.

For any positive integers n, and k dividing n, the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$, denoted by Tr_k^n, is the mapping defined as:

$$\mathrm{Tr}_k^n(x) = x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{n-k}}.$$

For $k = 1$, $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is called the absolute trace function. Recently, Mesnager [24] has proved a strong version of [5, Theorem 3], and provided several primary and secondary constructions of bent functions. In particular, by means of the second order derivative of the dual of known bent functions, she [24] presented two new infinite families of bent functions with the forms

$$f(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1}) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx) \tag{1}$$

and

$$f(x) = \mathrm{Tr}_1^m(x^{2^m+1}) + \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^{r-1}-1} x^{(2^m-1)\frac{i}{2^r}+1}\right) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx) \tag{2}$$

over $\mathbb{F}_{2^n}$, where $n = 2m$, $\lambda \in \mathbb{F}_{2^m}^*$ and $u, v \in \mathbb{F}_{2^n}^*$, and showed that the function defined by (1) is bent when $\mathrm{Tr}_1^n\left(\lambda^{-1}u^{2^m}v\right) = 0$ and the function defined by (2) is bent when $u, v \in \mathbb{F}_{2^m}^*$.

The aim of this paper is to present several classes of functions with few Walsh transform values. Inspired by the work of [24], we present several classes of bent functions by adding the product of three or two linear functions to some known bent functions. Computer experiments show that we can obtain some cubic bent functions from some quadratic bent functions, since the algebraic degree of the obtained bent functions is three, they can not affinely equivalent to any quadratic bent function. Meanwhile, several classes of semi-bent and five-valued functions are also obtained. The proofs of our main results are based on the study of the Walsh transform.

The paper is organized as follows. In Sect. 2, we give some notation and recall the necessary background. In Sect 3, we present some Boolean functions with few Walsh transform values from Kasami function and Gold function. A family of bent functions via Niho exponents is presented in Sect. 4 and two families of functions with few Walsh transform values via Maiorana–McFarland's class are provided in Sect. 5.

2 Preliminaries

By viewing each $x = x_1\xi_1 + x_2\xi_2 + \cdots + x_n\xi_n \in \mathbb{F}_{2^n}$ as a vector $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ where $\{\xi_1, \ldots, \xi_n\}$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, we identify $\mathbb{F}_2^n$ (the n-dimensional vector space over $\mathbb{F}_2$) with $\mathbb{F}_{2^n}$, and then every function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is equivalent to a Boolean function. For $x, y \in \mathbb{F}_{2^n}$, the inner product is defined as $x \cdot y = \mathrm{Tr}_1^n(xy)$. It is well known that every nonzero Boolean function defined on $\mathbb{F}_{2^n}$ can be written in the form of $f(x) = \sum_{j\in\Gamma_n} \mathrm{Tr}_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1})$, where Γ_n is a set of integers obtained by choosing one element in each cyclotomic coset of 2 modulo $2^n - 1$, $o(j)$ is the size of the cyclotomic coset containing j, $a_j \in \mathbb{F}_{2^{o(j)}}$ and $\epsilon = wt(f)(\mathrm{mod}\ 2)$, where $wt(f)$ is the cardinality of its support $supp := \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$. The algebraic degree of f is equal to the maximum 2-weight of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$.

The *Walsh transform* of a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the function $\widehat{\chi}_f : \mathbb{F}_{2^n} \to \mathbb{Z}$ defined by

$$\widehat{\chi}_f(a) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ax)}, \quad a \in \mathbb{F}_{2^n}.$$

The values $\widehat{\chi}_f(a)$, $a \in \mathbb{F}_{2^n}$ are called the *Walsh coefficients* of f. The *Walsh spectrum* of a Boolean function f is the multiset $\{\widehat{\chi}_f(a), a \in \mathbb{F}_{2^n}\}$. A Boolean function f is said to be *balanced* if $\widehat{\chi}_f(0) = 0$.

Definition 1 [27] A Boolean function f is said to be *bent* if $|\widehat{\chi}_f(a)| = 2^{n/2}$ for all $a \in \mathbb{F}_{2^n}$.

In view of Parseval's equation this definition implies that bent functions exist only for an even number of variables. For a bent function with n variables, its *dual* is the Boolean function $\tilde{f}$ defined by $\widehat{\chi}_f(a) = 2^{n/2}(-1)^{\tilde{f}(a)}$. It is easy to verify that the dual of f is again bent. Thus, Boolean bent functions occur in pair. However, determining the dual of a given bent function is not an easy thing. A bent function is said to be *self-dual* (resp. *anti-self-dual*) if $\tilde{f} = f$ (resp. $\tilde{f} = f+1$). For more study on self-dual and anti-self-dual bent functions can be founded in [5,9,16,24].

Two functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_2$ are called *affinely equivalent* if $f(x) = ag(l(x) + b) + c$ for some linearized permutation $l(x) \in \mathbb{F}_{2^n}[x]$, $a, c \in \mathbb{F}_2$ and $b \in \mathbb{F}_{2^n}$. Note that algebraic degree, the set of absolute values of Walsh coefficients and bentness of a Boolean function are affine invariants.

Definition 2 [11] A Boolean function f is said to be *semi-bent* if

$$\widehat{\chi}_f(a) \in \begin{cases} \{0, \pm 2^{\frac{n+1}{2}}\}, & \text{if } n \text{ is odd} \\ \{0, \pm 2^{\frac{n}{2}+1}\}, & \text{if } n \text{ is even} \end{cases}$$

for all $a \in \mathbb{F}_{2^n}$.

Our constructions can be derived from some known bent functions. The following result will be used in the sequel.

Lemma 1 *Let n be a positive integer and $u, v, r \in \mathbb{F}_{2^n}^*$. Let $g(x)$ be a Boolean function over $\mathbb{F}_{2^n}$. Define the Boolean function $f(x)$ by*

$$f(x) = g(x) + Tr_1^n(ux)Tr_1^n(vx)Tr_1^n(rx).$$

Then, for every $a \in \mathbb{F}_{2^n}$,

$$\begin{aligned}\widehat{\chi}_f(a) =& \frac{1}{4}\left[3\widehat{\chi}_g(a) + \widehat{\chi}_g(a+v) + \widehat{\chi}_g(a+u) - \widehat{\chi}_g(a+u+v)\right. \\ &\left. + \widehat{\chi}_g(a+r) - \widehat{\chi}_g(a+r+v) - \widehat{\chi}_g(a+r+u) + \widehat{\chi}_g(a+r+u+v)\right].\end{aligned}$$

In particular, if $r = v$, then

$$\widehat{\chi}_f(a) = \frac{1}{2}\left[\widehat{\chi}_g(a) + \widehat{\chi}_g(a+u) + \widehat{\chi}_g(a+v) - \widehat{\chi}_g(a+u+v)\right].$$

Proof For $i, j \in \{0, 1\}$ and $u, v \in \mathbb{F}_{2^n}^*$, define

$$T_{(i,j)} = \{x \in \mathbb{F}_{2^n} | \mathrm{Tr}_1^n(ux) = i, \mathrm{Tr}_1^n(vx) = j\}$$

and denote

$$S_{(i,j)}(a) = \sum_{x \in T_{(i,j)}} (-1)^{g(x)+\mathrm{Tr}_1^n(ax)}$$

and

$$Q_{(i,j)}(a+r) = \sum_{x \in T_{(i,j)}} (-1)^{g(x)+\mathrm{Tr}_1^n((a+r)x)}.$$

For each $a \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned}\widehat{\chi}_f(a) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ax)} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{g(x)+\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)\mathrm{Tr}_1^n(rx)+\mathrm{Tr}_1^n(ax)}\\ &= \sum_{x\in T_{(0,0)}} (-1)^{g(x)+\mathrm{Tr}_1^n(ax)} + \sum_{x\in T_{(0,1)}} (-1)^{g(x)+\mathrm{Tr}_1^n(ax)}\\ &\quad + \sum_{x\in T_{(1,0)}} (-1)^{g(x)+\mathrm{Tr}_1^n(ax)} + \sum_{x\in T_{(1,1)}} (-1)^{g(x)+\mathrm{Tr}_1^n((a+r)x)}\\ &= S_{(0,0)}(a) + S_{(0,1)}(a) + S_{(1,0)}(a) + Q_{(1,1)}(a+r)\\ &= \widehat{\chi}_g(a) - S_{(1,1)}(a) + Q_{(1,1)}(a+r). \end{aligned} \tag{3}$$

In the following, we will compute the sums $S_{(1,1)}(a)$ and $Q_{(1,1)}(a+r)$. Let $T_{(i,j)}$ be defined as above. Clearly,

$$\widehat{\chi}_g(a) = S_{(0,0)}(a) + S_{(0,1)}(a) + S_{(1,0)}(a) + S_{(1,1)}(a). \tag{4}$$

Furthermore, we have

$$\begin{aligned}\widehat{\chi}_g(a+v) &= \sum_{x\in T_{(0,0)}} (-1)^{g(x)+\mathrm{Tr}_1^n(ax)} - \sum_{x\in T_{(0,1)}} (-1)^{g(x)+\mathrm{Tr}_1^n(ax)}\\ &\quad + \sum_{x\in T_{(1,0)}} (-1)^{g(x)+\mathrm{Tr}_1^n(ax)} - \sum_{x\in T_{(1,1)}} (-1)^{g(x)+\mathrm{Tr}_1^n(ax)}\\ &= S_{(0,0)}(a) - S_{(0,1)}(a) + S_{(1,0)}(a) - S_{(1,1)}(a). \end{aligned} \tag{5}$$

Similarly,

$$\widehat{\chi}_g(a+u) = S_{(0,0)}(a) + S_{(0,1)}(a) - S_{(1,0)}(a) - S_{(1,1)}(a) \tag{6}$$

and

$$\widehat{\chi}_g(a+u+v) = S_{(0,0)}(a) - S_{(0,1)}(a) - S_{(1,0)}(a) + S_{(1,1)}(a). \tag{7}$$

From (4)–(7), we have

$$\begin{pmatrix} 1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} S_{(0,0)}(a)\\ S_{(0,1)}(a)\\ S_{(1,0)}(a)\\ S_{(1,1)}(a) \end{pmatrix} = \begin{pmatrix} \widehat{\chi}_g(a)\\ \widehat{\chi}_g(a+v)\\ \widehat{\chi}_g(a+u)\\ \widehat{\chi}_g(a+u+v) \end{pmatrix}. \tag{8}$$

Note that the coefficient matrix of (8) is a Hadamard matrix of order 4. Then we have

$$S_{(1,1)}(a) = \frac{1}{4}\left[\widehat{\chi}_g(a) - \widehat{\chi}_g(a+v) - \widehat{\chi}_g(a+u) + \widehat{\chi}_g(a+u+v)\right]. \tag{9}$$

Substituting a by $a+r$ in (9), we can get

$$Q_{(1,1)}(a+r) = \frac{1}{4}\left[\widehat{\chi}_g(a+r) - \widehat{\chi}_g(a+r+v)\right.$$
$$\left. -\widehat{\chi}_g(a+r+u) + \widehat{\chi}_g(a+r+u+v)\right]. \tag{10}$$

The desired conclusion follows from (3), (9) and (10).

In particular, if $r = v$, it is easy to show that

$$\widehat{\chi}_f(a) = \frac{1}{2}\left[\widehat{\chi}_g(a) + \widehat{\chi}_g(a+u) + \widehat{\chi}_g(a+v) - \widehat{\chi}_g(a+v+u)\right].$$

The proof is completed. □

It must be pointed out that $f(x) = g(x) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)\mathrm{Tr}_1^n(rx) = g(x) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)\ \mathrm{Tr}_1^n(ux+vx) = g(x)$ when $u+v+r=0$. In the following, we always assume that $u+v+r \neq 0$.

3 Several infinite families of bent, semi-bent and five-valued functions from monomial bent functions

3.1 An infinite family of bent, semi-bent and five-valued functions from Kasami function

Let $n = 2m$ (m is at least 2) be a positive even integer. The Kasami function $g(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1})$ is bent where $\lambda \in \mathbb{F}_{2^m}^*$ and its dual $\tilde{g}$ is given by $\tilde{g}(x) = \mathrm{Tr}_1^m(\lambda^{-1}x^{2^m+1}) + 1$ [24]. In other words, for each $a \in \mathbb{F}_{2^n}$, the Walsh coefficient $\widehat{\chi}_g(a)$ is

$$\widehat{\chi}_g(a) = -2^m(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}. \tag{11}$$

In the following result, we will present some bent and five-valued functions by making use of the Kasami function.

Theorem 1 *Let $n = 2m$ be a positive even integer and let u, v, r be three distinct pairwise elements in $\mathbb{F}_{2^n}^*$ such that $u+v+r \neq 0$. Define the Boolean function f on $\mathbb{F}_{2^n}$ as*

$$f(x) = Tr_1^m(\lambda x^{2^m+1}) + Tr_1^n(ux)Tr_1^n(vx)Tr_1^n(rx),$$

where $\lambda \in \mathbb{F}_{2^m}^*$. If $Tr_1^n(\lambda^{-1}u^{2^m}v) = Tr_1^n(\lambda^{-1}r^{2^m}u) = Tr_1^n(\lambda^{-1}r^{2^m}v) = 0$, then f is bent. Otherwise, f is five-valued and the Walsh spectrum of f is $\{0, \pm 2^m, \pm 2^{m+1}\}$.

Proof Let $g(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1})$. For each $a \in \mathbb{F}_{2^n}$, by Lemma 1, we have

$$\begin{aligned}\widehat{\chi}_f(a) = &\frac{1}{4}\big[3\widehat{\chi}_g(a) + \widehat{\chi}_g(a+v) + \widehat{\chi}_g(a+u) - \widehat{\chi}_g(a+u+v) \\ &+\widehat{\chi}_g(a+r) - \widehat{\chi}_g(a+r+v) - \widehat{\chi}_g(a+r+u) + \widehat{\chi}_g(a+r+u+v)\big] \\ = &\triangle_1 + \triangle_2,\end{aligned}$$

where

$$\triangle_1 = \frac{1}{4}\big[3\widehat{\chi}_g(a) + \widehat{\chi}_g(a+v) + \widehat{\chi}_g(a+u) - \widehat{\chi}_g(a+u+v)\big]$$

and

$$\triangle_2 = \quad \frac{1}{4}\big[\widehat{\chi}_g(a+r) - \widehat{\chi}_g(a+r+v) - \widehat{\chi}_g(a+r+u) + \widehat{\chi}_g(a+r+u+v)\big].$$

Now we use (11) to compute the sums $\triangle_1$ and $\triangle_2$ respectively.

$$\begin{aligned}\triangle_1 = &\frac{1}{4}(-2^m)\Big[3(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})} + (-1)^{\mathrm{Tr}_1^m(\lambda^{-1}(a+v)^{2^m+1})} + (-1)^{\mathrm{Tr}_1^m(\lambda^{-1}(a+u)^{2^m+1})} \\ &- (-1)^{\mathrm{Tr}_1^m(\lambda^{-1}(a+u+v)^{2^m+1})}\Big] \\ = &-\frac{1}{4}2^m(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}\Big[3 + (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m}v+av^{2^m}+v^{2^m+1})\right)} \\ &+ (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m}u+au^{2^m}+u^{2^m+1})\right)} \\ &- (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m}v+av^{2^m}+v^{2^m+1}+a^{2^m}u+au^{2^m}+u^{2^m+1}+u^{2^m}v+uv^{2^m})\right)}\Big].\end{aligned}$$

Similarly, we have

$$\begin{aligned}\triangle_2 = &\frac{1}{4}(-2^m)(-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m+1}+a^{2^m}r+ar^{2^m}+r^{2^m+1})\right)} \\ &\times\Big[1 - (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m}v+av^{2^m}+v^{2^m+1}+r^{2^m}v+rv^{2^m})\right)} \\ &- (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m}u+au^{2^m}+u^{2^m+1}+r^{2^m}u+ru^{2^m})\right)} \\ &+ (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m}v+av^{2^m}+v^{2^m+1}+a^{2^m}u+au^{2^m}+u^{2^m+1})\right)} \\ &\times (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(r^{2^m}v+rv^{2^m}+r^{2^m}u+ru^{2^m}+u^{2^m}v+uv^{2^m})\right)}\Big].\end{aligned}$$

To simplify $\triangle_1$ and $\triangle_2$, we write $t_1 = \mathrm{Tr}_1^m(\lambda^{-1}(r^{2^m}v + rv^{2^m})) = \mathrm{Tr}_1^n(\lambda^{-1}r^{2^m}v)$, $t_2 = \mathrm{Tr}_1^m(\lambda^{-1}(r^{2^m}u + ru^{2^m})) = \mathrm{Tr}_1^n(\lambda^{-1}r^{2^m}u)$ and $t_3 = \mathrm{Tr}_1^m(\lambda^{-1}(u^{2^m}v + uv^{2^m})) = \mathrm{Tr}_1^n(\lambda^{-1}u^{2^m}v)$ due to the transitivity property of the trace function (for every k dividing

$n, \mathrm{Tr}_1^n(x) = \mathrm{Tr}_1^k(\mathrm{Tr}_k^n(x))$). Meanwhile, denote $c_1 = \mathrm{Tr}_1^m(\lambda^{-1}(a^{2^m}v + av^{2^m} + v^{2^m+1}))$, $c_2 = \mathrm{Tr}_1^m(\lambda^{-1}(a^{2^m}u + au^{2^m} + u^{2^m+1}))$ and $c_3 = \mathrm{Tr}_1^m(\lambda^{-1}(a^{2^m}r + ar^{2^m} + r^{2^m+1}))$. Then the sums $\triangle_1$ and $\triangle_2$ can be written as

$$\triangle_1 = \frac{1}{4}(-2^m)(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})} \times \left[3 + (-1)^{c_1} + (-1)^{c_2} - (-1)^{c_1+c_2+t_3}\right] \quad (12)$$

and

$$\begin{aligned}\triangle_2 = &\frac{1}{4}(-2^m)(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})+c_3} \\ &\times \left[1 - (-1)^{c_1+t_1} - (-1)^{c_2+t_2} + (-1)^{c_1+c_2+t_1+t_2+t_3}\right]. \end{aligned} \quad (13)$$

Firstly, we prove that f is bent when $t_1 = t_2 = t_3 = 0$. If $t_1 = t_2 = t_3 = 0$, then

$$\triangle_1 = \frac{1}{4}(-2^m)(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}\left[3 + (-1)^{c_1} + (-1)^{c_2} - (-1)^{c_1+c_2}\right]$$

and

$$\triangle_2 = \frac{1}{4}(-2^m)(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})+c_3} \times \left[1 - (-1)^{c_1} - (-1)^{c_2} + (-1)^{c_1+c_2}\right].$$

When $c_3 = 0$, we can get

$$\widehat{\chi}_f(a) = \triangle_1 + \triangle_2 = -2^m(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}.$$

When $c_3 = 1$, we can get

$$\begin{aligned}\widehat{\chi}_f(a) = \triangle_1 + \triangle_2 &= \frac{1}{2}(-2^m)(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}\left[1 + (-1)^{c_1} + (-1)^{c_2} - (-1)^{c_1+c_2}\right] \\ &= \begin{cases} 2^m(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}, & \text{if } c_1 = c_2 = 1 \\ -2^m(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}, & \text{otherwise.} \end{cases}\end{aligned}$$

Hence, f is bent if $\mathrm{Tr}_1^n(\lambda^{-1}u^{2^m}v) = \mathrm{Tr}_1^n(\lambda^{-1}r^{2^m}u) = \mathrm{Tr}_1^n(\lambda^{-1}r^{2^m}v) = 0$.

Secondly, we show that f is five-valued if at least one t_i ($i \in \{1, 2, 3\}$) is equal to 1. We only give the proof of the case of $t_1 = t_2 = 0$ and $t_3 = 1$ since the others can be proven in a similar manner. In this case, (12) and (13) become

$$\triangle_1 = \frac{1}{4}(-2^m)(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}\left[3 + (-1)^{c_1} + (-1)^{c_2} + (-1)^{c_1+c_2}\right]$$

and

$$\triangle_2 = \frac{1}{4}(-2^m)(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})+c_3}\left[1 - (-1)^{c_1} - (-1)^{c_2} - (-1)^{c_1+c_2}\right].$$

When $c_3 = 0$, then we have

$$\widehat{\chi}_f(a) = \triangle_1 + \triangle_2 = -2^m(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}. \tag{14}$$

When $c_3 = 1$, then we have

$$\begin{aligned}\widehat{\chi}_f(a) = \triangle_1 + \triangle_2 &= \frac{1}{2}(-2^m)(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}\left[1+(-1)^{c_1}+(-1)^{c_2}+(-1)^{c_1+c_2}\right] \\ &= \begin{cases} -2^{m+1}(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}, & \text{if}\, c_1 = c_2 = 0 \\ 0, & \text{otherwise.} \end{cases}\end{aligned} \tag{15}$$

It then follows from (14) and (15) that f is five-valued and its Walsh spectrum is $\{0, \pm 2^m, \pm 2^{m+1}\}$.

This completes the proof. □

It is easily checked that $\mathrm{Tr}_1^n(\lambda^{-1}u^{2^m}v) = \mathrm{Tr}_1^n(\lambda^{-1}r^{2^m}u) = \mathrm{Tr}_1^n(\lambda^{-1}r^{2^m}v) = 0$ when $u, v, r \in \mathbb{F}_{2^m}^*$. From Theorem 1, we get the following corollary.

Corollary 1 *Let $n = 2m$ be a positive even integer and $\lambda \in \mathbb{F}_{2^m}^*$. If $u, v, r \in \mathbb{F}_{2^m}^*$ are three pairwise distinct elements such that $u + v + r \neq 0$, then the Boolean function f*

$$f(x) = Tr_1^m(\lambda x^{2^m+1}) + Tr_1^n(ux)Tr_1^n(vx)Tr_1^n(rx)$$

is bent.

Remark 1 If $r = v$, the bent functions f presented in Theorem 1 become ones in [24, Theorem 9], i.e., if $\mathrm{Tr}_1^n(\lambda^{-1}u^{2^m}v) = 0$, then the Boolean function $f(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1}) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$ is bent.

Now let us consider the algebraic degree of f in Theorem 1. Let $i, j, k \in \{0, 1, \cdots, n-1\}$ are pairwise distinct integers. Denote the set of all permutations on i, j, k by $\mathcal{P}$. It is clear that the possible cubic term in the expression of f has the form $(\sum_{(i,j,k)\in\mathcal{P}} u^{2^i}v^{2^j}r^{2^k})x^{2^i+2^j+2^k}$. If there exist three pairwise distinct integers $i, j, k \in \{0, 1, \ldots, n-1\}$ such that $(\sum_{(i,j,k)\in\mathcal{P}} u^{2^i}v^{2^j}r^{2^k}) \neq 0$, then the algebraic degree of f is 3.

Next we will show that if $\mathrm{Tr}_1^n(\lambda^{-1}u^{2^m}v) = \mathrm{Tr}_1^n(\lambda^{-1}r^{2^m}u) = \mathrm{Tr}_1^n(\lambda^{-1}r^{2^m}v) = 0$, the algebraic degree of f in Theorem 1 is not equal to 3 when $m = 2$. Otherwise, this will contradict the fact that the algebraic degree of a bent function f is at most $n/2$. Let $\mathcal{P}_1$ be the set of all permutations on $\{0, 1, 3\}$, $\mathcal{P}_2$ be the set of all permutations on $\{0, 1, 2\}$, $\mathcal{P}_3$ be the set of all permutations on $\{1, 2, 3\}$ and $\mathcal{P}_4$ be the set of all permutations on $\{0, 2, 3\}$. The condition $\mathrm{Tr}_1^4(\lambda^{-1}r^{2^2}v) = \mathrm{Tr}_1^4(\lambda^{-1}r^{2^2}u) = \mathrm{Tr}_1^4(\lambda^{-1}u^{2^2}v) = 0$ can be written as

$$\begin{cases} r^{2^2}v + r^{2^3}v^2 + rv^{2^2} + r^2v^{2^3} = 0 \\ r^{2^2}u + r^{2^3}u^2 + ru^{2^2} + r^2u^{2^3} = 0 \\ u^{2^2}v + u^{2^3}v^2 + uv^{2^2} + u^2v^{2^3} = 0. \end{cases} \tag{16}$$

Multiplying u, v and r to the first, the second and the third equation of (16) respectively yields

$$\begin{cases} r^{2^2}vu + r^{2^3}v^2u + rv^{2^2}u + r^2v^{2^3}u = 0 \\ r^{2^2}vu + r^{2^3}vu^2 + rvu^{2^2} + r^2vu^{2^3} = 0 \\ ru^{2^2}v + ru^{2^3}v^2 + ruv^{2^2} + ru^2v^{2^3} = 0. \end{cases} \tag{17}$$

Adding three equations of (17) gives $\sum_{(i,j,k)\in\mathcal{P}_1} u^{2^i}v^{2^j}r^{2^k} = 0$. Similarly, multiplying u^2, v^2 and r^2 to the first, the second and the third equation of (16) respectively yields $\sum_{(i,j,k)\in\mathcal{P}_2} u^{2^i}v^{2^j}r^{2^k} = 0$. Multiplying u^{2^2}, v^{2^2} and r^{2^2} to the first, the second and the third equation of (16) respectively yields $\sum_{(i,j,k)\in\mathcal{P}_3} u^{2^i}v^{2^j}r^{2^k} = 0$ and multiplying u^{2^3}, v^{2^3} and r^{2^3} to the first, the second and the third equation of (16) respectively yields $\sum_{(i,j,k)\in\mathcal{P}_4} u^{2^i}v^{2^j}r^{2^k} = 0$. Therefore, there are no cubic terms in the expression of f when $m = 2$, which implies that the algebraic degree of f in Theorem 1 is equal to 2.

Remark 2 When $m = 2$, the algebraic degree of the bent function f in Theorem 1 is equal to 2. When $m \geq 3$, the bent functions f in Theorem 1 may be cubic according to our numerical results. Recall that algebraic degree is an affine invariant. We conclude that there exist bent functions in Theorem 1 which are affinely inequivalent to all known quadratic bent functions.

Example 1 Let $m = 3$, $\mathbb{F}_{2^6}$ be generated by the primitive polynomial $x^6 + x^4 + x^3 + x + 1$ and ξ be a primitive element of $\mathbb{F}_{2^6}$. Take $\lambda = 1$, $u = \xi$, $v = \xi^9$ and $r = \xi^{27}$. Let $\mathcal{P}$ be the set of all permutations on 0, 1, 2. By help of a computer, we can get $\mathrm{Tr}_1^6(u^8v) = \mathrm{Tr}_1^6(r^8u) = \mathrm{Tr}_1^6(r^8v) = 0, u+v+r \neq 0, \sum_{(i,j,k)\in\mathcal{P}} u^{2^i}v^{2^j}v^{2^k} = \xi^{45} \neq 0$ and the function $f(x) = \mathrm{Tr}_1^3(x^9)+\mathrm{Tr}_1^6(\xi x)\mathrm{Tr}_1^6(\xi^9 x)\mathrm{Tr}_1^6(\xi^{27}x)$ is a cubic bent function, which coincides with the results in Theorem 1.

Example 2 Let $m = 4$, $\mathbb{F}_{2^8}$ be generated by the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$ and ξ be a primitive element of $\mathbb{F}_{2^8}$. Take $\lambda = \xi^{17}$, $u = \xi^{10}$, $v = \xi^9$, $r = \xi^3$. Then the function f in Theorem 1 is $f(x) = \mathrm{Tr}_1^4(\xi^{17}x^{17}) + \mathrm{Tr}_1^8(\xi^{10}x)\mathrm{Tr}_1^8(\xi^9x)\mathrm{Tr}_1^8(\xi^3x)$. By help of a computer, we can get $\mathrm{Tr}_1^8(\lambda^{-1}u^{16}v) = 1$, $\mathrm{Tr}_1^8(\lambda^{-1}r^{16}u) = \mathrm{Tr}_1^8(\lambda^{-1}r^{16}v) = 0$ and f is five-valued, which is consistent with the results given in Theorem 1.

As noted in Remark 1, if $\mathrm{Tr}_1^n(\lambda^{-1}u^{2^m}v) = 0$, then the Boolean function $f(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1}) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$ is bent. In the following result, we will prove that if $\mathrm{Tr}_1^n(\lambda^{-1}u^{2^m}v) = 1$, the Boolean function $f(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1}) + \mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$ is semi-bent by using Lemma 1.

Theorem 2 *Let $n = 2m$ be a positive even integer and $u, v \in \mathbb{F}_{2^n}^*$. Define a Boolean function f on $\mathbb{F}_{2^n}$ by*

$$f(x) = Tr_1^m(\lambda x^{2^m+1}) + Tr_1^n(ux)Tr_1^n(vx),$$

where $\lambda \in \mathbb{F}_{2^m}^*$. *If* $Tr_1^n(\lambda^{-1}u^{2^m}v) = 1$, *then* f *is semi-bent. Moreover, when* $Tr_1^n(\lambda^{-1}u^{2^m}v) = 1$, *if* $Tr_1^m(\lambda^{-1}u^{2^m+1}) = 1$ *or* $Tr_1^m(\lambda^{-1}v^{2^m+1}) = 1$, *then* f *is a balanced semi-bent function.*

Proof Let $g(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1})$. By Lemma 1 and (11), for each $a \in \mathbb{F}_{2^n}^*$, we have

$$\begin{aligned}
\widehat{\chi}_f(a) &= \frac{1}{2}\left[\widehat{\chi}_g(a) + \widehat{\chi}_g(a+v) + \widehat{\chi}_g(a+u) - \widehat{\chi}_g(a+u+v)\right] \\
&= \frac{1}{2}\widehat{\chi}_g(a)\Big[1 + (-1)^{\mathrm{Tr}_1^m(\lambda^{-1}(a^{2^m}v+av^{2^m}+v^{2^m+1}))} \\
&\quad + (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m}u+au^{2^m}+u^{2^m+1})\right)} \\
&\quad - (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m}v+av^{2^m}+v^{2^m+1}+a^{2^m}u+au^{2^m}+u^{2^m+1}+u^{2^m}v+uv^{2^m})\right)}\Big] \\
&= \frac{1}{2}\widehat{\chi}_g(a)\Big[1 + (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m}v+av^{2^m}+v^{2^m+1})\right)} \\
&\quad + (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m}u+au^{2^m}+u^{2^m+1})\right)} \\
&\quad + (-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}(a^{2^m}v+av^{2^m}+v^{2^m+1}+a^{2^m}u+au^{2^m}+u^{2^m+1})\right)}\Big]
\end{aligned} \tag{18}$$

where the last identity holds because $\mathrm{Tr}_1^n(\lambda^{-1}u^{2^m}v) = \mathrm{Tr}_1^m(u^{2^m}v + uv^{2^m}) = 1$.

Denote $c_1 = \mathrm{Tr}_1^m(\lambda^{-1}(a^{2^m}v + av^{2^m} + v^{2^m+1}))$ and $c_2 = \mathrm{Tr}_1^m((\lambda^{-1}(a^{2^m}u + au^{2^m} + u^{2^m+1}))$. Then (18) can be written as

$$\begin{aligned}
\widehat{\chi}_f(a) &= \frac{1}{2}(-2^m)(-1)^{\mathrm{Tr}_1^m\lambda^{-1}a^{2^m+1})}[1 + (-1)^{c_1} + (-1)^{c_2} + (-1)^{c_1+c_2}] \\
&= \begin{cases} (-2^{m+1})(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})}, & \text{if } c_1 = c_2 = 0 \\ 0, & \text{otherwise.} \end{cases}
\end{aligned}$$

It then follows from Definition 2 that f is semi-bent. Furthermore, from (18), if $\mathrm{Tr}_1^n(\lambda^{-1}u^{2^m}v) = \mathrm{Tr}_1^m(\lambda^{-1}(u^{2^m}v + uv^{2^m})) = 1$ then the Walsh transform coefficient of the function f evaluated at 0 is equal to

$$\begin{aligned}
\widehat{\chi}_f(0) = \frac{1}{2}(-2^m)\Big[&1 + (-1)^{\mathrm{Tr}_1^m(\lambda^{-1}v^{2^m+1})} \\
&+ (-1)^{\mathrm{Tr}_1^m(\lambda^{-1}u^{2^m+1})} + (-1)^{\mathrm{Tr}_1^m(\lambda^{-1}(v^{2^m+1}+u^{2^m+1}))}\Big].
\end{aligned}$$

It is easy to check that $\widehat{\chi}_f(0) = 0$ if $\mathrm{Tr}_1^m(\lambda^{-1}v^{2^m+1}) = 1$ or $\mathrm{Tr}_1^m(\lambda^{-1}u^{2^m+1}) = 1$. Therefore, $f(x)$ is a balanced semi-bent function. □

3.2 An infinite family of bent, semi-bent and five-valued functions from Gold-like monomial function

In [9], Carlet et.al proved that the Gold-like monomial function $g(x) = \mathrm{Tr}_1^{4k}(\lambda x^{2^k+1})$ over $\mathbb{F}_{2^{4k}}$ where k is at least 2 and $\lambda \in \mathbb{F}_{2^{4k}}^*$, is self-dual or anti-self-dual bent if and only if $\lambda^2 + \lambda^{2^{3k+1}} = 1$ and $\lambda^{2^k+1} + \lambda^{2^{3k}+2^k} = 0$. Recently, Mesnager showed that $g(x) = \mathrm{Tr}_1^{4k}(\lambda x^{2^k+1})$ over $\mathbb{F}_{2^{4k}}$ is self-dual bent when $\lambda + \lambda^{2^{3k}} = 1$ in [24, Lemma 23], i.e., for each $a \in \mathbb{F}_{2^{4k}}^*$, the Walsh coefficient $\widehat{\chi}_f(a)$ is

$$\widehat{\chi}_g(a) = 2^{2k}(-1)^{\mathrm{Tr}_1^{4k}(\lambda a^{2^k+1})}$$

when $\lambda + \lambda^{2^{3k}} = 1$.

Theorem 3 *Let k be a positive integer such that $k > 1$ and let u, v, r be three pairwise distinct elements in $\in \mathbb{F}_{2^{4k}}^*$ such that $u+v+r \neq 0$. Let $\lambda \in \mathbb{F}_{2^{4k}}^*$ such that $\lambda+\lambda^{2^{3k}} = 1$. If $Tr_1^{4k}(\lambda(u^{2^k}v + uv^{2^k})) = Tr_1^{4k}(\lambda(r^{2^k}u + ru^{2^k})) = Tr_1^{4k}(\lambda(r^{2^k}v + rv^{2^k})) = 0$, then the Boolean function*

$$f(x) = Tr_1^{4k}(\lambda x^{2^k+1}) + Tr_1^{4k}(ux)Tr_1^{4k}(vx)Tr_1^{4k}(rx)$$

over $\mathbb{F}_{2^{4k}}$ is a bent function. Otherwise, $f(x)$ is a five-valued function.

Proof Let $g(x) = \mathrm{Tr}_1^{4k}(\lambda x^{2^k+1})$. We write $\mathrm{Tr}_1^{4k}(\lambda(r^{2^k}v + rv^{2^k})) = t_1$, $\mathrm{Tr}_1^{4k}(\lambda(r^{2^k}u + ru^{2^k})) = t_2$, $\mathrm{Tr}_1^{4k}(\lambda(u^{2^k}v + uv^{2^k})) = t_3$. Denote $c_1 = \mathrm{Tr}_1^{4k}(\lambda(a^{2^k}v + av^{2^k} + v^{2^k+1}))$, $c_2 = \mathrm{Tr}_1^{4k}(\lambda(a^{2^k}u + au^{2^k} + u^{2^k+1}))$ and $c_3 = \mathrm{Tr}_1^{4k}(\lambda(a^{2^k}r + ar^{2^k} + r^{2^k+1}))$. By analyses similar to those in Theorem 1, we have

$$\widehat{\chi}_f(a) = \triangle_1 + \triangle_2,$$

where

$$\triangle_1 = \frac{1}{4}2^{2k}(-1)^{\mathrm{Tr}_1^{4k}(\lambda a^{2^k+1})}\left[3 + (-1)^{c_1} + (-1)^{c_2} - (-1)^{c_1+c_2+t_3}\right] \tag{19}$$

and

$$\triangle_2 = \frac{1}{4}2^{2k}(-1)^{\mathrm{Tr}_1^{4k}(\lambda a^{2^k+1})+c_3}\left[1 - (-1)^{c_1+t_1} - (-1)^{c_2+t_2} + (-1)^{c_1+c_2+t_1+t_2+t_3}\right]. \tag{20}$$

Similar to Theorem 1, we can prove that $f(x)$ is bent if $t_1 = t_2 = t_3 = 0$.

Next we will prove that f is five-valued in the case of $t_1 = t_2 = 0$ and $t_3 = 1$ since the others can be proven in a similar manner. In this case, (19) and (20) become

$$\triangle_1 = \frac{1}{4}2^{2k}(-1)^{\mathrm{Tr}_1^{4k}(\lambda a^{2^k+1})}\left[3 + (-1)^{c_1} + (-1)^{c_2} + (-1)^{c_1+c_2}\right]$$

and

$$\triangle_2 = \frac{1}{4}2^{2k}(-1)^{\mathrm{Tr}_1^{4k}(\lambda a^{2^k+1})+c_3}\big[1-(-1)^{c_1}-(-1)^{c_2}-(-1)^{c_1+c_2}\big].$$

When $c_3 = 0$, then we have

$$\widehat{\chi}_f(a) = \triangle_1 + \triangle_2 = 2^{2k}(-1)^{\mathrm{Tr}_1^{4k}(\lambda a^{2^k+1})}. \tag{21}$$

When $c_3 = 1$, then we have

$$\begin{aligned}\widehat{\chi}_f(a) &= \triangle_1 + \triangle_2 = \frac{1}{2}2^{2k}(-1)^{\mathrm{Tr}_1^{4k}(\lambda a^{2^k+1})}\big[1+(-1)^{c_1}+(-1)^{c_2}+(-1)^{c_1+c_2}\big]\\ &= \begin{cases} 2^{2k+1}(-1)^{\mathrm{Tr}_1^{4k}(\lambda a^{2^k+1})}, & \text{if } c_1 = c_2 = 0\\ 0, & \text{otherwise.}\end{cases}\end{aligned} \tag{22}$$

Thus, f is a five-valued function if $t_1 = t_2 = 0$ and $t_3 = 1$. □

By analyses similar to those in Theorem 2, we get the following result.

Theorem 4 *Let k be a positive integer such that $k > 1$ and let $u, v \in \mathbb{F}_{2^{4k}}^*$. Assume that $\lambda \in \mathbb{F}_{2^{4k}}^*$ such that $\lambda + \lambda^{2^{3k}} = 1$. Define a Boolean function as*

$$f(x) = Tr_1^{4k}(\lambda x^{2^k+1}) + Tr_1^{4k}(ux)Tr_1^{4k}(vx)$$

over $\mathbb{F}_{2^{4k}}$. Then the following hold:

1) *If $Tr_1^{4k}(\lambda(u^{2^k}v + uv^{2^k})) = 0$, then f is bent.*
2) *If $Tr_1^{4k}(\lambda(u^{2^k}v + uv^{2^k})) = 1$, then f is semi-bent. Moreover, if $Tr_1^{4k}(\lambda u^{2^k+1}) = 1$ or $Tr_1^{4k}(\lambda v^{2^k+1}) = 1$, then f is a balanced semi-bent function.*

Example 3 Let $k = 2$, $\mathbb{F}_{2^8}$ be generated by the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$ and ξ be a primitive element of $\mathbb{F}_{2^8}$.

1) Let $\mathcal{P}$ be the set of all permutations on 0, 1, 2. If one takes $\lambda = \xi^{34}$, $u = \xi^{212}$, $v = \xi^{10}$ and $r = \xi^{16}$, then by a Magma program, one can get $\lambda + \lambda^{2^6} = 1$, $\mathrm{Tr}_1^8(\lambda(u^4v + uv^4)) = \mathrm{Tr}_1^8(\lambda(r^4u + ru^4)) = \mathrm{Tr}_1^8(\lambda(r^4v + rv^4)) = 0$ and $\sum_{(i,j,k)\in\mathcal{P}} u^{2^i}v^{2^j}v^{2^k} = \xi^8 \neq 0$. Computer experiment shows that $f(x) = \mathrm{Tr}_1^8(\xi^{34}x^5) + \mathrm{Tr}_1^8(\xi^{212}x)\mathrm{Tr}_1^{4k}(\xi^{10}x)\mathrm{Tr}_1^{4k}(\xi^{16}x)$ given by in Theorem 3 is a cubic bent function, which is consistent with the results given in Theorem 3.
2) If one takes $\lambda = \xi^{34}$, $u = \xi^{212}$, $v = \xi^{10}$ and $r = \xi^{12}$, then by a Magma program, one can get $\mathrm{Tr}_1^8(\lambda(r^4v + rv^4)) = \mathrm{Tr}_1^8(\lambda(r^4u + ru^4)) = 1$ and $\mathrm{Tr}_1^8(\lambda(u^4v + uv^4)) = 0$. Computer experiment shows that $f(x) = \mathrm{Tr}_1^8(\xi^{34}x^5) + \mathrm{Tr}_1^8(\xi^{212}x)\mathrm{Tr}_1^{4k}(\xi^{10}x)\mathrm{Tr}_1^{4k}(\xi^{12}x)$ given by in Theorem 3 is a five-valued function. This is compatible with the results given in Theorem 3.

4 An infinite family of bent functions from the Niho exponents

The bent function

$$g(x) = \mathrm{Tr}_1^m(x^{2^m+1}) + \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^{k-1}-1} x^{(2^m-1)\frac{i}{2^k}+1}\right)$$

via 2^k Niho exponents was found by Leander and Kholosha [18], where $\gcd(k, m) = 1$. Take any $\alpha \in \mathbb{F}_{2^n}$ with $\alpha + \alpha^{2^m} = 1$. It was shown in [1] that $\tilde{g}$ is

$$\tilde{g}(a) = \mathrm{Tr}_1^m\big((\alpha(1 + a + a^{2^m}) + \alpha^{2^{n-k}} + a^{2^m})(1 + a + a^{2^m})^{1/(2^k-1)}\big). \tag{23}$$

Now using Lemma 1 and (23), we can present the following class of bent functions via 2^k Niho exponents.

Theorem 5 *Let $n = 2m$, k be a positive with $\gcd(k, m) = 1$ and $u, v, r \in \mathbb{F}_{2^m}^*$ such that $u + v + r \neq 0$. Then the Boolean function*

$$f(x) = Tr_1^m(x^{2^m+1}) + Tr_1^n\left(\sum_{i=1}^{2^{k-1}-1} x^{(2^m-1)\frac{i}{2^k}+1}\right) + Tr_1^n(ux)Tr_1^n(vx)Tr_1^n(rx)$$

is a bent function.

Proof Let $g(x) = \mathrm{Tr}_1^m(x^{2^m+1}) + \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^{k-1}-1} x^{(2^m-1)\frac{i}{2^k}+1}\right)$. For each $a \in \mathbb{F}_{2^n}$, by Lemma 1, we have

$$\begin{aligned}\widehat{\chi}_f(a) &= \frac{1}{4}\big[3\widehat{\chi}_g(a) + \widehat{\chi}_g(a+v) + \widehat{\chi}_g(a+u) - \widehat{\chi}_g(a+u+v)\\ &\quad + \widehat{\chi}_g(a+r) - \widehat{\chi}_g(a+r+v) - \widehat{\chi}_g(a+r+u) + \widehat{\chi}_g(a+r+u+v)\big]\\ &= \triangle_1 + \triangle_2,\end{aligned}$$

where

$$\triangle_1 = \frac{1}{4}\big[3\widehat{\chi}_g(a) + \widehat{\chi}_g(a+v) + \widehat{\chi}_g(a+u) - \widehat{\chi}_g(a+u+v)\big]$$

and

$$\triangle_2 = \frac{1}{4}\big[\widehat{\chi}_g(a+r) - \widehat{\chi}_g(a+r+v) - \widehat{\chi}_g(a+r+u) + \widehat{\chi}_g(a+r+u+v)\big].$$

Set $A = 1 + a + a^{2^m}$. It follows from (23) that

$$\widehat{\chi}_g(a) = 2^m(-1)^{\mathrm{Tr}_1^m\left((\alpha A + \alpha^{2^{n-k}} + a^{2^m})A^{1/(2^k-1)}\right)},$$

where $\alpha \in \mathbb{F}_{2^n}$ such that $\alpha + \alpha^{2^m} = 1$. Now we compute $\triangle_1$ and $\triangle_2$ respectively. Note that $u, v, r \in \mathbb{F}_{2^m}^*$. Then we have

$$\begin{aligned}
\triangle_1 &= \frac{1}{4}\left[3 + \widehat{\chi}_g(a+v) + \widehat{\chi}_g(a+u) - \widehat{\chi}_g(a+u+v)\right]\\
&= \frac{1}{4}\widehat{\chi}_g(a)\Bigg[3 + (-1)^{\mathrm{Tr}_1^m\left(vA^{1/(2^k-1)}\right)} + (-1)^{\mathrm{Tr}_1^m\left(uA^{1/(2^k-1)}\right)}\\
&\quad - (-1)^{\mathrm{Tr}_1^m\left(vA^{1/(2^k-1)}\right)+\mathrm{Tr}_1^m\left(uA^{1/(2^k-1)}\right)}\Bigg]\\
&= \frac{1}{4}2^m(-1)^{\mathrm{Tr}_1^m\left((\alpha A+\alpha^{2^{n-k}}+a^{2^m})A^{1/(2^k-1)}\right)}\Big[3 + (-1)^{\mathrm{Tr}_1^m\left(vA^{1/(2^k-1)}\right)}\\
&\quad + (-1)^{\mathrm{Tr}_1^m\left(uA^{1/(2^k-1)}\right)}\\
&\quad - (-1)^{\mathrm{Tr}_1^m\left(vA^{1/(2^k-1)}\right)+\mathrm{Tr}_1^m\left(uA^{1/(2^k-1)}\right)}\Big]. \qquad (24)
\end{aligned}$$

Similarly, we have

$$\begin{aligned}
\triangle_2 &= \frac{1}{4}2^m(-1)^{\mathrm{Tr}_1^m\left((\alpha A+\alpha^{2^{n-k}}+a^{2^m}+r)A^{1/(2^k-1)}\right)}\Big[1 - (-1)^{\mathrm{Tr}_1^m\left(vA^{1/(2^k-1)}\right)}\\
&\quad - (-1)^{\mathrm{Tr}_1^m\left(uA^{1/(2^k-1)}\right)}\\
&\quad + (-1)^{\mathrm{Tr}_1^m\left(vA^{1/(2^k-1)}\right)+\mathrm{Tr}_1^m\left(uA^{1/(2^k-1)}\right)}\Big]. \qquad (25)
\end{aligned}$$

Let $c_1 = \mathrm{Tr}_1^m\left(vA^{1/(2^k-1)}\right)$ and $c_2 = \mathrm{Tr}_1^m\left(uA^{1/(2^k-1)}\right)$. When $\mathrm{Tr}_1^m\left(rA^{1/(2^k-1)}\right) = 0$, by (24) and (25) we have

$$\widehat{\chi}_f(a) = \triangle_1 + \triangle_2 = 2^m(-1)^{\mathrm{Tr}_1^m\left((\alpha A+\alpha^{2^{n-k}}+a^{2^m})A^{1/(2^k-1)}\right)}.$$

When $\mathrm{Tr}_1^m\left(rA^{1/(2^k-1)}\right) = 1$, by (24) and (25) again, we have

$$\begin{aligned}
\widehat{\chi}_f(a) = \triangle_1 + \triangle_2 &= \frac{1}{2}2^m(-1)^{\mathrm{Tr}_1^m\left((\alpha A+\alpha^{2^{n-k}}+a^{2^m})A^{1/(2^k-1)}\right)}\\
&\quad \times \left[1 + (-1)^{c_1} + (-1)^{c_2} - (-1)^{c_1+c_2}\right]\\
&= \begin{cases} -2^m(-1)^{\mathrm{Tr}_1^m\left((\alpha A+\alpha^{2^{n-k}}+a^{2^m})A^{1/(2^k-1)}\right)}, & \text{if } c_1 = 1, c_2 = 1\\ 2^m(-1)^{\mathrm{Tr}_1^m\left((\alpha A+\alpha^{2^{n-k}}+a^{2^m})A^{1/(2^k-1)}\right)}, & \text{otherwise.} \end{cases}
\end{aligned}$$

Therefore, $f(x)$ is a bent function. □

Remark 3 This result generalizes the case in [24, Theorem 11] for $r = v$. It may be noted that we can not construct more bent functions for the case $u, v, r \notin \mathbb{F}_{2^m}^*$ according to our numerical results.

Example 4 Let $m = 4$, $k = 3$ and $\mathbb{F}_{2^8}$ be generated by the primitive polynomial $x^8+x^4+x^3+x^2+1$ and ξ be a primitive element of $\mathbb{F}_{2^8}$. If we take $u = \xi^{34}$, $v = \xi^{17}$, $r = \xi^{51}$, then by a Magma program, we can see that $f(x) = \mathrm{Tr}_1^4(x^{17}) + \mathrm{Tr}_1^8(x^{226}) + \mathrm{Tr}_1^8(x^{196}) + \mathrm{Tr}_1^8(x^{166}) + \mathrm{Tr}_1^8(\xi^{34}x)\mathrm{Tr}_1^8(\xi^{17}x)\mathrm{Tr}_1^8(\xi^{51}x)$ given by in Theorem 5 is a bent function, which is consistent with the results given in Theorem 5.

5 Several infinite families of bent, semi-bent and five-valued functions from the class of Maiorana–McFarland

In this section, we identify $\mathbb{F}_{2^n}$ (where $n = 2m$) with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ and consider Boolean functions with bivariate representation $f(x, y) = \mathrm{Tr}_1^m(P(x, y))$, where $P(x, y)$ is a polynomial in two variables over $\mathbb{F}_{2^m}$. For $a = (a_1, a_2)$, $b = (b_1, b_2) \in \mathbb{F}_{2^n}$, the scalar product in $\mathbb{F}_{2^n}$ can be defined as

$$\langle (a_1, a_2), (b_1, b_2) \rangle = \mathrm{Tr}_1^m(a_1 b_1 + a_2 b_2).$$

The well-known Maiorana–McFarland class of bent functions can be defined as follows.

$$g(x, y) = \mathrm{Tr}_1^m(x\pi(y)) + h(y), (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$$

where $\pi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is a permutation and h is a Boolean function over $\mathbb{F}_{2^m}$, and its dual is given by

$$\tilde{g}(x, y) = \mathrm{Tr}_1^m(y\pi^{-1}(x)) + h(\pi^{-1}(x))$$

where π^{-1} denotes the inverse mapping of the permutation π [6]. This together with the definition of the dual function implies that for each $a = (a_1, a_2) \in \mathbb{F}_{2^n}$

$$\widehat{\chi}_g(a_1, a_2) = 2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+h(\pi^{-1}(a_1))}. \tag{26}$$

In what follows, by choosing suitable permutations π, we will construct some bent, semi-bent and five-valued functions from the class of Maiorana–McFarland. It is well known that the compositional inverse of a linearized permutation polynomial is also a linearized polynomial. The following two theorems will employ the linearized permutation polynomial over $\mathbb{F}_{2^m}$ to give Boolean functions with few Walsh transform values.

Theorem 6 *Let $n = 2m$ and $u = (u_1, u_2), v = (v_1, v_2), r = (r_1, r_2)$ are three pairwise distinct nonzero elements in $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ such that $u + v + r \neq 0$. Assume that π is a linearized permutation polynomial over $\mathbb{F}_{2^m}$. Let $f(x, y)$ be the Boolean function given by*

$$f(x, y) = Tr_1^m(x\pi(y)) + Tr_1^m(y) + Tr_1^m(u_1x + u_2y)Tr_1^m(v_1x + v_2y)Tr_1^m(r_1x + r_2y).$$

If $Tr_1^m(r_2\pi^{-1}(v_1)+v_2\pi^{-1}(r_1))=0$*,* $Tr_1^m(r_2\pi^{-1}(u_1)+u_2\pi^{-1}(r_1))=0$ *and* $Tr_1^m(u_2\pi^{-1}(v_1)+v_2\pi^{-1}(u_1))=0$*, then* $f(x,y)$ *is bent. Otherwise,* $f(x,y)$ *is five-valued and the Walsh spectrum of* $f(x,y)$ *is* $\{0,\pm 2^m,\pm 2^{m+1}\}$.

Proof Let $g(x,y)=\mathrm{Tr}_1^m(x\pi(y))+\mathrm{Tr}_1^m(y)$. From (26), for each $(a_1,a_2)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$, we get

$$\widehat{\chi}_g(a_1,a_2)=2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))}. \tag{27}$$

Applying Lemma 1 again, for each $(a_1,a_2)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$, we have

$$\widehat{\chi}_f(a_1,a_2)=\triangle_1+\triangle_2,$$

where

$$\begin{aligned}\triangle_1=\frac{1}{4}\big[&3\widehat{\chi}_g(a_1,a_2)+\widehat{\chi}_g(a_1+v_1,a_2+v_2)+\widehat{\chi}_g(a_1+u_1,a_2+u_2)\\&-\widehat{\chi}_g(a_1+v_1+u_1,a_2+v_2+u_2)\big]\end{aligned}$$

and

$$\begin{aligned}\triangle_2=\frac{1}{4}\big[&\widehat{\chi}_g(a_1+r_1,a_2+r_2)-\widehat{\chi}_g(a_1+r_1+v_1,a_2+r_2+v_2)\\&-\widehat{\chi}_g(a_1+r_1+u_1,a_2+r_2+u_2)\\&+\widehat{\chi}_g(a_1+r_1+v_1+u_1,a_2+r_2+v_2+u_2)\big].\end{aligned}$$

Note that π^{-1} is a linearized polynomial. Let $c_1=\mathrm{Tr}_1^m\big(a_2\pi^{-1}(v_1)+v_2\pi^{-1}(a_1)+(v_2+1)\pi^{-1}(v_1)\big)$, $c_2=\mathrm{Tr}_1^m(a_2\pi^{-1}(u_1)+u_2\pi^{-1}(a_1)+(u_2+1)\pi^{-1}(u_1))$ and $c_3=\mathrm{Tr}_1^m(a_2\pi^{-1}(r_1)+r_2\pi^{-1}(a_1)+(r_2+1)\pi^{-1}(r_1))$. Denote $t_1=\mathrm{Tr}_1^m(r_2\pi^{-1}(v_1)+v_2\pi^{-1}(r_1))$, $t_2=\mathrm{Tr}_1^m(r_2\pi^{-1}(u_1)+u_2\pi^{-1}(r_1))$ and $t_3=\mathrm{Tr}_1^m(u_2\pi^{-1}(v_1)+v_2\pi^{-1}(u_1))$. A similar analysis as the proof of Theorem 1 shows that

$$\triangle_1=\frac{1}{4}2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))}\big[3+(-1)^{c_1}+(-1)^{c_2}-(-1)^{c_1+c_2+t_3}\big] \tag{28}$$

and

$$\begin{aligned}\triangle_2=\ &\frac{1}{4}2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))+c_3}\big[1-(-1)^{c_1+t_1}-(-1)^{c_2+t_2}\\&+(-1)^{c_1+c_2+t_1+t_2+t_3}\big].\end{aligned} \tag{29}$$

It is easy to see that when $t_1=t_2=t_3=0$ and $c_3=0$

$$\widehat{\chi}_f(a_1,a_2)=2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))}$$

and when $t_1 = t_2 = t_3 = 0$ and $c_3 = 1$

$$\widehat{\chi}_f(a_1, a_2) = \begin{cases} -2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))}, & \text{if } c_1 = c_2 = 1 \\ 2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))}, & \text{otherwise.} \end{cases}$$

Hence, $f(x, y)$ is bent if $t_1 = t_2 = t_3 = 0$.

Next we will prove that $f(x, y)$ is five-valued in the case of $t_1 = t_2 = 1$ and $t_3 = 0$ and others can be proved by a similar manner. In this case, (28) and (29) become

$$\triangle_1 = \frac{1}{4}2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))}\left[3 + (-1)^{c_1} + (-1)^{c_2} - (-1)^{c_1+c_2}\right]$$

and

$$\triangle_2 = \frac{1}{4}2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))+c_3}\left[1 + (-1)^{c_1} + (-1)^{c_2} + (-1)^{c_1+c_2}\right].$$

When $c_3 = 0$, we have

$$\begin{aligned}\widehat{\chi}_f(a_1, a_2) &= \triangle_1 + \triangle_2 = \frac{1}{2}2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))}[2+(-1)^{c_1}+(-1)^{c_2}] \\ &= \begin{cases} 2^{m+1}(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))}, & \text{if } c_1 = c_2 = 0 \\ 0, & \text{if } c_1 = c_2 = 1 \\ 2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))}, & \text{otherwise.} \end{cases} \end{aligned} \tag{30}$$

When $c_3 = 1$, we have

$$\begin{aligned}\widehat{\chi}_f(a_1, a_2) &= \triangle_1 + \triangle_2 = \frac{1}{2}2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))}[1 - (-1)^{c_1+c_2}] \\ &= \begin{cases} 0, & \text{if } c_1 = c_2 = 1 \\ & \text{or } c_1 = c_2 = 0 \\ 2^m(-1)^{\mathrm{Tr}_1^m(a_2\pi^{-1}(a_1))+\mathrm{Tr}_1^m(\pi^{-1}(a_1))}, & \text{otherwise.} \end{cases} \end{aligned} \tag{31}$$

Combining (30) and (31), we conclude that $f(x, y)$ is five-valued and the Walsh spectrum of $f(x, y)$ is $\{0, \pm 2^m, \pm 2^{m+1}\}$. □

It should be noted that two of $u, v, r \in \mathbb{F}_{2^n}^*$ can be equal. Without loss of generality, we assume that $r = v$, then the following result can be obtained.

Theorem 7 *Let $n = 2m$ and $u = (u_1, u_2)$, $v = (v_1, v_2)$ are two distinct nonzero elements in $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Assume that π is a linearized permutation polynomial of $\mathbb{F}_{2^m}$. Let $f(x, y)$ be the Boolean function given by*

$$f(x, y) = Tr_1^m(x\pi(y)) + Tr_1^m(y) + Tr_1^m(u_1x + u_2y)Tr_1^m(v_1x + v_2y).$$

If $Tr_1^m(u_2\pi^{-1}(v_1) + v_2\pi^{-1}(u_1)) = 0$, then f is bent. Otherwise, f is semi-bent.

Proof The proof is similar to Theorem 2 and we omit it here. □

Remark 4 To obtain our constructions in Theorems 6 and 7, we need to determine the compositional inverse of a given linearized permutation polynomial over $\mathbb{F}_{2^m}$. Information on the compositional inverses of certain linearized permutation polynomials could be found in [14,31,32]. Clearly, the simplest suitable linearized permutation polynomial π over $\mathbb{F}_{2^m}$ in Theorems 6 and 7 is x^{2^k} where $0 \le k \le n-1$.

Theorem 8 *Let $n = 2m$ and s be a divisor of m with $\frac{m}{s}$ is odd. Assume that $u = (u_1, u_2)$, $v = (v_1, v_2)$ are two distinct nonzero elements in $\mathbb{F}_{2^s} \times \mathbb{F}_{2^s}$ such that $u_1 v_2 + v_1 u_2 = 0$. Let $f(x, y)$ be the Boolean function given by*

$$f(x, y) = Tr_1^m(xy^d) + Tr_1^m(u_1 x + u_2 y) Tr_1^m(v_1 x + v_2 y)$$

where $d(2^s + 1) \equiv 1 \pmod{2^m - 1}$. If $Tr_1^m(u_1^2 v_2 + u_2 v_1^2) = 0$, then $f(x, y)$ is bent. Otherwise, $f(x, y)$ is semi-bent.

Proof Let $\pi(y) = y^d$ and $g(x, y) = \mathrm{Tr}_1^m(x\pi(y))$. Since $d(2^s+1) \equiv 1 \pmod{2^m - 1}$, then $\pi^{-1}(y) = y^{2^s+1}$. This together with (26) implies that for each $a = (a_1, a_2) \in \mathbb{F}_{2^n}$

$$\widehat{\chi}_g(a_1, a_2) = 2^m(-1)^{\mathrm{Tr}_1^m(a_2 a_1^{2^s+1})}. \tag{32}$$

According to Lemma 1, for each $(a_1, a_2) \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned}\widehat{\chi}_f(a_1, a_2) = \frac{1}{2}\big[&\widehat{\chi}_g(a_1, a_2) + \widehat{\chi}_g(a_1 + v_1, a_2 + v_2)\\ &+ \widehat{\chi}_g(a_1 + u_1, a_2 + u_2) - \widehat{\chi}_g(a_1 + v_1 + u_1, a_2 + v_2 + u_2)\big].\end{aligned}$$

Now we compute $\widehat{\chi}_g(a_1+v_1, a_2+v_2)$, $\widehat{\chi}_g(a_1+u_1, a_2+u_2)$ and $\widehat{\chi}_g(a_1+v_1+u_1, a_2+v_2+u_2)$ respectively. By (32), we have

$$\begin{aligned}&\widehat{\chi}_g(a_1 + v_1, a_2 + v_2)\\ &\quad = 2^m(-1)^{\mathrm{Tr}_1^m\left((a_2+v_2)(a_1+v_1)^{2^s+1}\right)}\\ &\quad = 2^m(-1)^{\mathrm{Tr}_1^m(a_2 a_1^{2^s+1}) + \mathrm{Tr}_1^m(a_2 a_1^{2^s} v_1 + a_2 a_1 v_1^{2^s} + a_2 v_1^{2^s+1}) + \mathrm{Tr}_1^m\left(a_1^{2^s+1} v_2 + a_1^{2^s} v_1 v_2 + a_1 v_1^{2^s} v_2 + v_1^{2^s+1} v_2\right)}\\ &\quad = \widehat{\chi}_g(a_1, a_2)(-1)^{\mathrm{Tr}_1^m\left(a_2 a_1^{2^s} v_1 + a_2 a_1 v_1 + a_2 v_1^2\right) + \mathrm{Tr}_1^m\left(a_1^{2^s+1} v_2 + a_1^{2^s} v_1 v_2 + a_1 v_1 v_2 + v_1^2 v_2\right)}\end{aligned} \tag{33}$$

where the last identity holds since $v = (v_1, v_2)$ is a nonzero element in $\mathbb{F}_{2^s} \times \mathbb{F}_{2^s}$.

Similarly, we can show that

$$\begin{aligned}&\widehat{\chi}_g(a_1 + u_1, a_2 + u_2)\\ &\quad = \widehat{\chi}_g(a_1, a_2)(-1)^{\mathrm{Tr}_1^m\left(a_2 a_1^{2^s} u_1 + a_2 a_1 u_1 + a_2 u_1^2\right) + \mathrm{Tr}_1^m\left(a_1^{2^s+1} u_2 + a_1^{2^s} u_1 u_2 + a_1 u_1 u_2 + u_1^2 u_2\right)}\end{aligned} \tag{34}$$

and

$$\begin{aligned}&\widehat{\chi}_g(a_1+v_1+u_1, a_2+v_2+u_2)\\&\quad=\widehat{\chi}_g(a_1,a_2)(-1)^{\mathrm{Tr}_1^m\left(a_2a_1^{2^s}v_1+a_2a_1v_1+a_2v_1^2\right)+\mathrm{Tr}_1^m\left(a_1^{2^s+1}v_2+a_1^{2^s}v_1v_2+a_1v_1v_2+v_1^2v_2\right)}\\&\qquad\times(-1)^{\mathrm{Tr}_1^m\left(a_2a_1^{2^s}u_1+a_2a_1u_1+a_2u_1^2\right)+\mathrm{Tr}_1^m(a_1^{2^s+1}u_2+a_1^{2^s}u_1u_2+a_1u_1u_2+u_1^2u_2)}\\&\qquad\times(-1)^{\mathrm{Tr}_1^m\left((a_1^{2^s}+a_1)(u_1v_2+v_1u_2)+u_1^2v_2+v_1^2u_2\right)}.\end{aligned}\tag{35}$$

Let $c_1=\mathrm{Tr}_1^m(a_2a_1^{2^s}v_1+a_2a_1v_1+a_2v_1^2+a_1^{2^s+1}v_2+a_1^{2^s}v_1v_2+a_1v_1v_2+v_1^2v_2)$ and $c_2=\mathrm{Tr}_1^m(a_2a_1^{2^s}u_1+a_2a_1u_1+a_2u_1^2+a_1^{2^s+1}u_2+a_1^{2^s}u_1u_2+a_1u_1u_2+u_1^2u_2)$.

Note that $u_1v_2+v_1u_2=0$. If $\mathrm{Tr}_1^m(u_1^2v_2+u_2v_1^2)=0$, combining (33), (34) and (35), we get

$$\begin{aligned}\widehat{\chi}_f(a_1,a_2)&=\frac{1}{2}2^m(-1)^{\mathrm{Tr}_1^m(a_2a_1^{2^s+1})}[1+(-1)^{c_1}+(-1)^{c_2}-(-1)^{c_1+c_2}]\\&=\begin{cases}-2^m(-1)^{\mathrm{Tr}_1^m(a_2a_1^{2^s+1})}, & \text{if } c_1=c_2=1\\ 2^m(-1)^{\mathrm{Tr}_1^m(a_2a_1^{2^s+1})}, & \text{otherwise.}\end{cases}\end{aligned}$$

If $\mathrm{Tr}_1^m(u_1^2v_2+u_2v_1^2)=1$, then

$$\begin{aligned}\widehat{\chi}_f(a_1,a_2)&=\frac{1}{2}2^m(-1)^{\mathrm{Tr}_1^m(a_2a_1^{2^s+1})}[1+(-1)^{c_1}+(-1)^{c_2}+(-1)^{c_1+c_2}]\\&=\begin{cases}2^{m+1}(-1)^{\mathrm{Tr}_1^m(a_2a_1^{2^s+1})}, & \text{if } c_1=c_2=0\\ 0, & \text{otherwise.}\end{cases}\end{aligned}$$

The desired conclusion follows from the definitions of bent and semi-bent function. □

Example 5 Let $m=9$, $s=3$ and $\mathbb{F}_{2^9}$ be generated by the primitive polynomial x^9+x^4+1 and ξ be a primitive element of $\mathbb{F}_{2^9}$.

1) Take $u=(u_1,u_2)=(\xi^{219},\xi^{73})$ and $v=(v_1,v_2)=(\xi^{146},1)$. Clearly, $u_1v_2+u_2v_1=0$ and $284\times(2^3+1)\equiv 1(\mathrm{mod}\ 512)$. By help of a computer, we can get $\mathrm{Tr}_1^9(u_1^2v_2+u_2v_1^2)=0$ and the function $f(x)=\mathrm{Tr}_1^9(xy^{284})+\mathrm{Tr}_1^9(\xi^{219}x+\xi^{73}y)\mathrm{Tr}_1^9(\xi^{146}x+y)$ is a bent function over $\mathbb{F}_{2^9}\times\mathbb{F}_{2^9}$, which is consistent with the results given in Theorem 8.
2) Take $u=(u_1,u_2)=(\xi^{146},\xi^{73})$ and $v=(v_1,v_2)=(\xi^{73},1)$. Clearly, $u_1v_2+u_2v_1=0$ and $284\times(2^3+1)\equiv 1(\mathrm{mod}\ 512)$. By help of a computer, we can get $\mathrm{Tr}_1^9(u_1^2v_2+u_2v_1^2)=1$ and the function $f(x)=\mathrm{Tr}_1^9(xy^{284})+\mathrm{Tr}_1^9(\xi^{146}x+\xi^{73}y)\mathrm{Tr}_1^9(\xi^{73}x+y)$ is semi-bent function over $\mathbb{F}_{2^9}\times\mathbb{F}_{2^9}$, which is consistent with the results given in Theorem 8.

6 Conclusion

Several classes of Boolean functions with few Walsh transform values, including bent, semi-bent and five-valued functions are provided. As a generalization of the result [24], we obtained not only bent functions but also semi-bent and five-valued functions from a different approach. Furthermore, some cubic bent functions can be given by using our approach.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grants 11371011, 11601177, 61403157, and 61572027), Anhui Provincial Natural Science Foundation (Grant No.1608085QA05), the Foundation for Distinguished Young Talents in Higher Education of Anhui Province of China (Grant No. gxyqZD2016258) and the Funding of Jiangsu Innovation Program for Graduate Education (Grant No. KYZZ15_0090).

References

1. Budaghyan, L., Carlet, C., Helleseth, T., Kholosha, A., Mesnager, S.: Further results on Niho bent functions. IEEE Trans. Inf. Theory **58**(11), 6979–6985 (2012)
2. Canteaut, A., Carlet, C., Charpin, P., Fontaine, C.: On cryptographic properties of the cosets of r (1, m). IEEE Trans. Inf. Theory **47**(4), 1494–1513 (2001)
3. Canteaut, A., Charpin, P., Kyureghyan, G.M.: A new class of monomial bent functions. Finite Fields Appl. **14**(1), 221–241 (2008)
4. Carlet, C.: Two new classes of bent functions. In: Helleseth, T. (ed.) Advances in Cryptology-EUROCRYPT '93. Lecture Notes in Computer Science, vol. 765, pp. 77–101. Springer, Heidelberg (1994)
5. Carlet, C.: On bent and highly nonlinear balanced/resilient functions and their algebraic immunities. In: Appl. Algebra Eng. Commun. Comput., pp. 1–28. Springer (2006)
6. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P. (eds.) Chapter of the Monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press, Cambridge (2010)
7. Carlet, C., Mesnager, S.: On Dillon's class $\mathcal{H}$ of bent functions, Niho bent functions and o-polynomials. J. Comb. Theory Ser. A **18**(8), 2392–2410 (2011)
8. Carlet, C., Mesnager, S.: On semibent Boolean functions. IEEE Trans. Inf. Theory **58**(5), 3287–3292 (2012)
9. Carlet, C., Danielsen, L.E., Parker, M.G., Solé, P.: Self-dual bent functions. Int. J. Inf. Coding Theory **1**(4), 384–399 (2010)
10. Charpin, P., Pasalic, E., Tavernier, C.: On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inf. Theory **51**(12), 4286–4298 (2005)
11. Chee, S., Lee, S., Kim, K.: Semi-bent functions. In: Advances in CryptologyASIACRYPT'94, pp. 105–118. Springer (1995)
12. Chee, Y.M., Tan, Y., Zhang, X.D.: Strongly regular graphs constructed from p-ary bent functions. J. Algebraic Comb. **34**(2), 251–266 (2011)
13. Chen, H., Cao, X.: Some semi-bent functions with polynomial trace form. J. Syst. Sci. Complex. **27**(4), 777–784 (2014)
14. Coulter, R.S., Henderson, M.: The compositional inverse of a class of permutation polynomials over a finite field. Bull. Aust. Math. Soc. **65**(3), 521–526 (2002)
15. Dillon, J.F.: Elementary Hadamard difference sets. Ph.D. thesis, University of Maryland, College Park (1974)
16. Hou, X.D.: Classification of self dual quadratic bent functions. Des. Codes Cryptogr. **63**(2), 183–198 (2012)
17. Khoo, K., Gong, G., Stinson, D.R.: A new characterization of semi-bent and bent functions on finite fields. Des. Codes Cryptogr. **38**(2), 279–295 (2006)
18. Leander, G., Kholosha, A.: Bent functions with 2r Niho exponents. IEEE Trans. Inf. Theory **52**(12), 5529–5532 (2006)

19. 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)
20. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes, vol. 16. Elsevier, Amsterdam (1977)
21. Mesnager, S.: Bent Functions: Fundamentals and Results. Springer, New York (to appear)
22. Mesnager, S.: Semibent functions from Dillon and Niho exponents, Kloosterman sums, and Dickson polynomials. IEEE Trans. Inf. Theory **57**(11), 7443–7458 (2011)
23. Mesnager, S.: A new class of bent and hyper-bent Boolean functions in polynomial forms. Des. Codes Cryptogr. **59**(1), 265–279 (2011)
24. Mesnager, S.: Several new infinite families of bent functions and their duals. IEEE Trans. Inf. Theory **60**(7), 4397–4407 (2014)
25. Mesnager, S., Flori, J.P.: Hyperbent functions via Dillon-like exponents. IEEE Trans. Inf. Theory **59**(5), 3215–3232 (2013)
26. Olsen, J., Scholtz, R.A., Welch, L.: Bent-function sequences. IEEE Trans. Inf. Theory **28**(6), 858–864 (1982)
27. Rothaus, O.S.: On bent functions. J. Comb. Theory Ser. A **20**(3), 300–305 (1976)
28. Sun, G., Wu, C.: Construction of semi-bent Boolean functions in even number of variables. Chin. J. Electron. **18**(2), 231–237 (2009)
29. Tan, Y., Pott, A., Feng, T.: Strongly regular graphs associated with ternary bent functions. J. Comb. Theory Ser. A **117**(6), 668–682 (2010)
30. Wolfmann, J.: Special bent and near-bent functions. Adv. Math. Commun. **8**(1), 21–33 (2014)
31. Wu, B.: The compositional inverse of a class of linearized permutation polynomials over $\mathbb{F}_{2^n}$, n odd. Finite Fields Appl. **29**, 34–48 (2014)
32. Wu, B., Liu, Z.: Linearized polynomials over finite fields revisited. Finite Fields Appl. **22**, 79–100 (2013)
33. Yu, N.Y., Gong, G.: Constructions of quadratic bent functions in polynomial forms. IEEE Trans. Inf. Theory **52**(7), 3291–3299 (2006)
34. Zheng, Y., Zhang, X.-M.: Plateaued functions. In: Information and Communication Security, pp. 284–300. Springer (1999)