Boolean Functions with a Few Walsh Transform Values

Wengang Jin, Xiaoni Du(✉), Jinxia Hu, and Yanzhong Sun

College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, Gansu, People's Republic of China

Abstract. Boolean functions have been extensively studied in coding theory, cryptography, sequence design and graph theory. By adding two products of three linear functions to some known bent functions, in this paper, we construct a class of bent functions and obtain their dual functions. In the meantime, a class of semi-bent functions and some classes of five-valued Walsh spectra are given.

Keywords: Boolean functions · Bent functions · Semi-bent functions · Walsh transform · Five-valued Walsh spectra

1 Introduction

Boolean functions are widely used in cryptography, error correction codes [2] and signal sequence design [7]. Their applications in cryptographic systems have been studied for more than three decades. Some important properties of these functions, including balance, nonlinearity and algebraic immunity, are obtained. Walsh transform is a powerful tool to study the properties of Boolean functions in the application of cryptography and coding theory. The Walsh transform of a Boolean function, a discrete Fourier transform, can be used to express the cryptographic properties of a Boolean function.

Bent functions proposed by [14] are Boolean functions with two different Walsh transform values and implements the maximum Hamming distance function to all the affine Boolean functions. Bent functions exist only with even number of variables. Bent functions have been extensively studied because of their interesting algebraic and combinatorial properties and it have received a lot of attention in the literature on communications, because of their multiple applications in cryptography [1], the fields of coding theory [8] and sequence design [13].

No bent function is balanced. As generalizations of bent functions, [5] introduced the concept of semi-bent functions and obtained the balancedness and good nonlinearity in both even and odd number of variables. Moreover, [17,18] proved that bent functions and semi-bent functions are particular cases of the so-called plateaued functions. Like bent functions, semi-bent functions are also widely studied in cryptography. Because they have low Walsh transform values which can provide protection against fast correlation attacks [12] and linear

© Springer Nature Switzerland AG 2021
X. Sun et al. (Eds.): ICAIS 2021, CCIS 1423, pp. 642–655, 2021.
https://doi.org/10.1007/978-3-030-78618-2_53

cryptanalysis [9], they can possess desirable properties such as low autocorrelation, propagation criteria, resiliency, and high algebraic degree. Several new families of semi-bent functions were proposed by [3,4,6,10,15].

In 2014, [11] provided several new effective constructions of bent functions, and then gave several new infinite families of bent functions by adding a product of two linear functions to some known bent functions and their duals. After that, by adding a product of three linear functions to some known bent functions, [16] presented several classes of bent functions. Inspired by those results, in this paper, we firstly add a product of three linear functions to some known bent functions, and then add another product of three linear functions to which one (the added two products are related each other), so we obtain a class of bent functions and their duals. On the other hand, we promote a class of semi-bent functions and some classes of Boolean functions with five-valued Walsh spectra. Finally, a spectrum distribution of some class of Boolean functions with five-valued Walsh spectra is presented.

The paper is organized as follows. In Sect. 2, we introduce some notations and preliminaries. In Sect. 3, we present some bent functions, semi-bent functions and some functions with five-valued Walsh spectra. In Sect. 4, a spectrum distribution of the Boolean functions obtained in Sect. 3 is given. Section 5 concludes the paper.

2 Preliminaries

For a positive integer n, let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements, $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$. Tr_1^n denotes the absolute trace function from $\mathbb{F}_{2^n}$ onto $\mathbb{F}_2$

$$Tr_1^n(x) = x + x^2 + \cdots + x^{2^{n-1}}, \text{ for all } x \in \mathbb{F}_{2^n}.$$

Thus the Walsh transform of a Boolean function f on $\mathbb{F}_{2^n}$ is defined by

$$\hat{f}(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(ax)}, \text{ for all } a \in \mathbb{F}_{2^n}.$$

Let N_i be the number of $\alpha \in \mathbb{F}_{2^n}$ such that $\hat{f}(\alpha) = v_i$, i.e., $N_i = |\{\alpha \in \mathbb{F}_{2^n} : \hat{f}(\alpha) = v_i\}|$, where $1 \leqq i \leqq t$ and t is a positive integer. By the properties of Walsh transform, we have the following system of equations:

$$\begin{cases} \sum_{i=1}^{t} N_i = 2^n, \\ \sum_{i=1}^{t} N_i v_i = 2^n(-1)^{f(0)}, \\ \sum_{i=1}^{t} N_i v_i^2 = 2^{2n}, \end{cases} \tag{1}$$

A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be bent if $\hat{f}(\omega) = \pm 2^{\frac{n}{2}}$ for all $\omega \in \mathbb{F}_{2^n}$. Bent functions occur in pair. In fact, given a bent function f

over $\mathbb{F}_{2^n}$, we define its dual function, denoted by $\tilde{f}$, when considering the signs of the values of the Walsh transform $\hat{f}(x)(x \in \mathbb{F}_{2^n})$ of f. More precisely, $\tilde{f}$ is defined by

$$\hat{f}(x) = 2^{\frac{n}{2}}(-1)^{\tilde{f}(x)}. \tag{2}$$

A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be semi-bent if $\hat{f}(\omega) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ and if $\hat{f}(\omega) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ for all $\omega \in \mathbb{F}_{2^n}$ corresponding to n even and n odd, respectively. It is well known that the algebraic degree of a bent or semi-bent function defined on $\mathbb{F}_{2^n}$ is at most $\frac{n}{2}$ [2].

Let $n = 2m$ be a positive even integer and h be the monomial Niho quadratic function

$$h(x) = Tr_1^m(\lambda x^{2^m+1}), \tag{3}$$

with $\lambda \in \mathbb{F}_{2^m}^*$. It is well known that h is bent, and its dual function $\tilde{h}$ is given (see [11]) by

$$\tilde{h}(x) = Tr_1^m(\lambda^{-1}x^{2^m+1}) + 1. \tag{4}$$

Below we always let $n = 2m$ be an even and $\lambda \in \mathbb{F}_{2^m}^*$.

3 Infinite Families of Bent, Semi-bent and Five-Valued Functions from Monomial Bent Functions

In this section, we give a class of bent functions, its dual function, a class of semi-bent functions and some classes of five-valued Walsh spectra.

We begin with the result presented by [11] that plays an important role. Let f_1, f_2 and f_3 be three pairwise distinct Boolean functions. Then define $g : \mathbb{F}_{2^n} \to \mathbb{F}_2$:

$$g(x) = f_1(x)f_2(x) + f_1(x)f_3(x) + f_2(x)f_3(x). \tag{5}$$

Lemma 1. *[11] Let f_1, f_2 and f_3 be three pairwise distinct bent functions over $\mathbb{F}_{2^n}$ such that $\psi = f_1 + f_2 + f_3$ is bent. Let g be a Boolean function defined by Eq. (5). Then g is bent if and only if $\tilde{f}_1 + \tilde{f}_2 + \tilde{f}_3 + \tilde{\psi} = 0$. Furthermore, if g is a bent function, then $\tilde{g}$ is given by*

$$\tilde{g}(x) = \tilde{f}_1(x)\tilde{f}_2(x) + \tilde{f}_2(x)\tilde{f}_3(x) + \tilde{f}_3(x)\tilde{f}_1(x), \text{ for all } x \in \mathbb{F}_{2^n}.$$

[11] provides several new effective constructions of bent functions based on Eq. (5). Let $f_i, 1 \leqq i \leqq 3$ be three bent functions given by

$$f_i(x) = Tr_1^m(\lambda x^{2^m+1}) + Tr_1^n(a_i x), a_i \in \mathbb{F}_{2^n}^*,$$

where a_1, a_2 and a_3 are pairwise distinct elements of $\mathbb{F}_{2^n}^*$. After a simple calculation, Mesnager obtained that the Boolean function $g(x) = f_1(x)f_2(x) + f_1(x)f_3(x) + f_2(x)f_3(x) = Tr_1^m(\lambda x^{2^m+1}) + Tr_1^n(ax)Tr_1^n(bx) + Tr_1^n(a_1 x)$, where $a = a_1 + a_3, b = a_1 + a_2$. In the next lemma, Mesnager pointed out that $g(x)$ is a bent function under some conditions.

Lemma 2. *[11] Let $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$ such that $a \neq b$ and $Tr_1^n(\lambda^{-1}b^{2^m}a) = 0$. Then the Boolean function g defined on $\mathbb{F}_{2^n}$ as $g(x) = Tr_1^m(\lambda x^{2^m+1}) + Tr_1^n(ax)Tr_1^n(bx)$, it is a bent function of algebraic degree 2 and its dual function $\tilde{g}$ is given by*

$$\tilde{g}(x) = 1 + Tr_1^m(\lambda^{-1}x^{2^m+1}) + \Big(Tr_1^m(\lambda^{-1}a^{2^m+1}) + Tr_1^n(\lambda^{-1}a^{2^m}x)\Big) \cdot \Big(Tr_1^m(\lambda^{-1}b^{2^m+1}) + Tr_1^n(\lambda^{-1}b^{2^m}x)\Big).$$

Then one constructs a new class of Boolean functions and invests their properties by the two lemmas above. Let

$$f_i(x) = Tr_1^m(\lambda x^{2^m+1}) + Tr_1^n(ax)Tr_1^n(a_i x),$$

where a, a_1, a_2, a_3 are pairwise distinct elements of $\mathbb{F}_{2^n}^*$. Hence by Eq. (5), one can obtain

$$\begin{aligned} f(x) &= f_1(x)f_2(x) + f_2(x)f_3(x) + f_1(x)f_3(x) \\ &= Tr_1^m(\lambda x^{2^m+1}) + Tr_1^n(ax)Tr_1^n(a_1x)Tr_1^n((a_2+a_3)x) \\ &\quad + Tr_1^n(ax)Tr_1^n(a_2x)Tr_1^n(a_3x). \end{aligned} \tag{6}$$

Motivated by [16, Lemma 1], we get the following result.

Lemma 3. *Let $h(x)$ be a Boolean function on $\mathbb{F}_{2^n}$, and a, a_1, a_2, a_3 are pairwise distinct elements of $\mathbb{F}_{2^n}^*$. If $f(x)$ is defined as follows*

$$f(x) = h(x) + Tr_1^n(ax)Tr_1^n(a_1x)Tr_1^n((a_2+a_3)x) + Tr_1^n(ax)Tr_1^n(a_2x)Tr_1^n(a_3x),$$

then for any $b \in \mathbb{F}_{2^n}$,

$$\hat{f}(b) = \frac{1}{4}\Big(2\hat{h}(b) + \sum_{i=1}^{3}\hat{h}(b+a_i) - \hat{h}(b+\sum_{i=1}^{3}a_i) + 2\hat{h}(a+b) - \sum_{i=1}^{3}\hat{h}(a+b+a_i) + \hat{h}(a+b+\sum_{i=1}^{3}a_i)\Big).$$

Proof. For any $(\varepsilon_1, \varepsilon_2, \varepsilon_3) \in \mathbb{F}_2^3$, we define the set

$$T(\varepsilon_1, \varepsilon_2, \varepsilon_3) = \{x \in \mathbb{F}_{2^n} | Tr_1^n(a_1x) = \varepsilon_1, Tr_1^n(a_2x) = \varepsilon_2, Tr_1^n(a_3x) = \varepsilon_3\}$$

and integer

$$S_{(\varepsilon_1,\varepsilon_2,\varepsilon_3)}(b) = \sum_{x \in T(\varepsilon_1,\varepsilon_2,\varepsilon_3)} (-1)^{h(x)+Tr_1^n(bx)}.$$

Then for any $b \in \mathbb{F}_{2^n}$ and $(\varepsilon_1, \varepsilon_2, \varepsilon_3) \in \mathbb{F}_2^3$, we have

$$\begin{aligned}\hat{f}(b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(bx)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{h(x)+Tr_1^n(ax)Tr_1^n(a_1x)Tr_1^n((a_2+a_3)x)} \\ &\quad \cdot \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(ax)Tr_1^n(a_2x)Tr_1^n(a_3x)+Tr_1^n(bx)} \\ &= \sum_{wt(\varepsilon_1,\varepsilon_2,\varepsilon_3)\leqq 1} S_{(\varepsilon_1,\varepsilon_2,\varepsilon_3)}(b) + \sum_{2\leqq wt(\varepsilon_1,\varepsilon_2,\varepsilon_3)} S_{(\varepsilon_1,\varepsilon_2,\varepsilon_3)}(a+b) \\ &= \hat{h}(b) - \sum_{2\leqq wt(\varepsilon_1,\varepsilon_2,\varepsilon_3)} \Big(S_{(\varepsilon_1,\varepsilon_2,\varepsilon_3)}(b) - S_{(\varepsilon_1,\varepsilon_2,\varepsilon_3)}(a+b)\Big), \end{aligned} \tag{7}$$

One can immediately have $wt(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ is the Hamming weight of the vector $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$.

From the definitions of $S_{(\varepsilon_1,\varepsilon_2,\varepsilon_3)}(b)$ we have

$$\begin{aligned} 8S_{(\varepsilon_1,\varepsilon_2,\varepsilon_3)}(b) &= 8 \sum_{x\in\mathbb{F}_{2^n}} (-1)^{h(x)+Tr_1^n(bx)} \prod_{i=1}^{3} \frac{1+(-1)^{\varepsilon_i+Tr_1^n(a_ix)}}{2} \\ &= \hat{h}(b) + \sum_{\substack{d_i\in\mathbb{F}_2 \\ 1\leqq i\leqq 3}} (-1)^{\sum_{i=1}^{3} d_i\varepsilon_i} \hat{h}(b+\sum_{i=1}^{3} d_ia_i), \end{aligned} \tag{8}$$

for $2 \leqq wt(\varepsilon_1, \varepsilon_2, \varepsilon_3)$, substitute $a + b$ for b in the above equation, we get

$$8S_{(\varepsilon_1,\varepsilon_2,\varepsilon_3)}(a+b) = \hat{h}(a+b) + \sum_{\substack{d_i\in\mathbb{F}_2 \\ 1\leqq i\leqq 3}} (-1)^{\sum_{i=1}^{3} d_i\varepsilon_i} \hat{h}(a+b+\sum_{i=1}^{3} d_ia_i). \tag{9}$$

Applying Eqs. (8) and (9) to Eq. (7), and after a simple calculation, we get

$$\begin{aligned} 4\hat{f}(b) = 2\hat{h}(b) &+ \sum_{i=1}^{3} \hat{h}(b+a_i) - \hat{h}(b+\sum_{i=1}^{3} a_i) + 2\hat{h}(a+b) \\ &- \sum_{i=1}^{3} \hat{h}(a+b+a_i)) + \hat{h}(a+b+\sum_{i=1}^{3} a_i). \end{aligned}$$

This completes the proof. □

In the following, we assume that $A = Tr_1^m(\lambda^{-1}b^{2^m+1})$. Replace $h(x)$ with $Tr_1^m(\lambda x^{2^m+1})$ in Lemma 3, which happens to be Eq. (6), then after a tedious calculation by using Eqs. (2)–(4), we obtain

$$\hat{f}(b) = \frac{1}{4}(-2^m)(-1)^A\Big(2 + \sum_{i=1}^{3}(-1)^{c_i} - (-1)^{\sum_{i=1}^{3}(c_i+t_i)} + 2(-1)^{c_4} - \sum_{i=1}^{3}(-1)^{c_i+c_4+t_{i+3}} + (-1)^{\sum_{i=1}^{4} c_i + \sum_{i=1}^{6} t_i}\Big), \tag{10}$$

where

$c_i = Tr_1^m(\lambda^{-1}(b^{2^m}a_i + ba_i^{2^m} + a_i^{2^m+1}))$, $c_4 = Tr_1^m(\lambda^{-1}(b^{2^m}a + ba^{2^m} + a^{2^m+1}))$,
$t_1 = Tr_1^n(\lambda^{-1}a_1^{2^m}a_2)$, $t_2 = Tr_1^n(\lambda^{-1}a_2^{2^m}a_3)$,
$t_3 = Tr_1^n(\lambda^{-1}a_3^{2^m}a_1)$, $t_{i+3} = Tr_1^n(\lambda^{-1}a^{2^m}a_i)$,

for $1 \leqq i \leqq 3$.

Remark 1. In fact, since a, a_1, a_2, a_3 are pairwise distinct elements of $\mathbb{F}_{2^n}^*$, if a, a_1, a_2, a_3 are linear dependent over $\mathbb{F}_2$, we have the following two cases holds:

(1) If $a + a_i + a_j = 0, i \neq j$, then the three cases are corresponding to the result with [11].
(2) If $\sum_{i=1}^{3} a_i = 0$ or $a + \sum_{i=1}^{3} a_i = 0$, then the two cases are the same with the result of [16].

Below we always put $t_0 = \sum_{i=1}^{3} t_i$ modulo 2.

Now we discuss the properties of the function defined in Eq. (6).

Theorem 1. *With the notation as above. Let a, a_1, a_2, a_3 are linear independent over $\mathbb{F}_2$. If $(t_4, t_5, t_6) = (0, 0, 0)$, then $f(x)$ in Eq. (6) is a bent function if and only if $t_0 = 0$. Furthermore, the dual function $\tilde{f}(x)$ of the bent function $f(x)$ in Eq. (6) is given by*

$$\begin{aligned}\tilde{f}(x) &= \tilde{f}_1(x)\tilde{f}_2(x) + \tilde{f}_2(x)\tilde{f}_3(x) + \tilde{f}_1(x)\tilde{f}_3(x)\\ &= 1 + Tr_1^m(\lambda^{-1}x^{2^m+1}) + \Big(Tr_1^n(\lambda^{-1}a^{2^m}x) + Tr_1^m(\lambda^{-1}a^{2^m+1})\Big)\\ &\quad\Big(\sum_{1\leqq i<j\leqq 3}\Big(Tr_1^n(\lambda^{-1}a_i^{2^m}x) + Tr_1^m(\lambda^{-1}a_i^{2^m+1})\Big)\\ &\quad\cdot\Big(Tr_1^n(\lambda^{-1}a_j^{2^m}x) + Tr_1^m(\lambda^{-1}a_j^{2^m+1})\Big)\Big).\end{aligned}$$

Proof. Let $\varphi(x) = \sum_{i=1}^{3} f_i(x) = Tr_1^m(\lambda x^{2^m+1}) + Tr_1^n(ax)Tr_1^n(\sum_{i=1}^{3} a_i x)$. Since $t_4 = t_5 = t_6 = 0$, i.e., $Tr_1^n(\lambda^{-1}a^{2^m}a_i) = 0$ for $1 \leqq i \leqq 3$, by Lemma 2 we find that f_1, f_2, f_3, φ are all bent functions and their dual functions $\tilde{f}_1, \tilde{f}_2, \tilde{f}_3, \tilde{\varphi}$ are given by

$$\begin{aligned}\tilde{f}_i(x) &= 1 + Tr_1^m(\lambda^{-1}x^{2^m+1}) + Tr_1^m(\lambda^{-1}a^{2^m+1})\\ &\quad + Tr_1^n(\lambda^{-1}a^{2^m}x)\Big(Tr_1^m(\lambda^{-1}a_i^{2^m+1}) + Tr_1^n(\lambda^{-1}a_i^{2^m}x)\Big),\end{aligned}$$

and

$$\tilde{\varphi}(x) = 1 + Tr_1^m(\lambda^{-1}x^{2^m+1}) + Tr_1^m(\lambda^{-1}a^{2^m+1}) + Tr_1^n(\lambda^{-1}a^{2^m}x)$$
$$\Big(Tr_1^m(\lambda^{-1}(\sum_{i=1}^{3}a_i)^{2^m+1}) + Tr_1^n(\lambda^{-1}(\sum_{i=1}^{3}a_i)^{2^m}x)\Big).$$

Assume that $0 = \sum_{i=1}^{3}\tilde{f}_i(x) + \tilde{\varphi}(x)$, which is equivalent to

$$\Big(Tr_1^n(\lambda^{-1}a^{2^m+1}) + Tr_1^n(\lambda^{-1}a^{2^m}x)\Big)\Big(\sum_{i=1}^{3}Tr_1^m(\lambda^{-1}a_i^{2^m+1}\Big)$$
$$+ Tr_1^m(\lambda^{-1}(\sum_{i=1}^{3}a_i)^{2^m+1})\Big) = 0,$$

for all $x \in \mathbb{F}_{2^m}$, hence the equation holds if and only if $Tr_1^n(\lambda^{-1}(a_1^{2^m}a_2 + a_1^{2^m}a_3 + a_2^{2^m}a_3)) = 0$. Thus the result follows from Lemma 1.

The dual function $\tilde{f}$ of the bent function $f(x)$ then follows from Lemmas 1–2. □

Remark 2. The condition $t_0 = 0$ in Theorem 1 implies that $(t_1, t_2, t_3) \in \{(1,1,0),(0,1,1),(1,0,1),(0,0,0)\}$. Thus, if $(t_1, t_2, t_3) = (0,0,0)$, then Theorem 1 can be easily obtained by [19, Corollary 4.2]. Even though the function constructed in Eq. (6) is contained in the function in [19, Corollary 4.2], where the other three cases are not discussed.

Theorem 2. *Let a, a_1, a_2, a_3 are linear independent over $\mathbb{F}_2$. If $(t_0, t_4, t_5, t_6) = (0,1,1,1)$, then $f(x)$ in Eq. (6) is a semi-bent function.*

Proof. If $(t_0, t_4, t_5, t_6) = (0,1,1,1)$, then Eq. (10) can be written as

$$\hat{f}(b) = \frac{1}{4}(-2^m)(-1)^A\Big(2 + 2(-1)^{c_4} + \sum_{i=1}^{3}(-1)^{c_i} - (-1)^{\sum_{i=1}^{3}c_i}$$
$$- \sum_{i=1}^{3}(-1)^{c_i+c_4+1} + (-1)^{\sum_{i=1}^{4}c_i+1}\Big).$$

So if $c_4 = 0$, we have

$$\hat{f}(b) = \frac{1}{2}(-2^m)(-1)^A(2 + \sum_{i=1}^{3}(-1)^{c_i} + (-1)^{\sum_{i=1}^{3}c_i+1})$$
$$= \begin{cases} -2^{m+1}(-1)^A, & wt(c_1,c_2,c_3) \leqq 1, \\ 0, & 2 \leqq wt(c_1,c_2,c_3), \end{cases}$$

and if $c_4 = 1$, we have

$$\hat{f}(b) = \frac{1}{4}(-2^m)(-1)^A(0) = 0.$$

According to the definition of semi-bent function, we find that $f(x)$ is a semi-bent function. □

Theorem 3. *With the notation defined as above, we have*

(1) If $(t_0, t_4, t_5, t_6) = (1, 1, 1, 1)$, *then* $f(x)$ *in Eq. (6) is five-valued and the Walsh spectrum of* f *is* $\{0, \pm 2^m, \pm 3 \cdot 2^m\}$.
(2) If $(t_0, t_4, t_5, t_6) \in \mathbb{F}_2^4 \backslash \{(0,0,0,0), (0,1,1,1), (1,1,1,1)\}$, *then* $f(x)$ *is five-valued and the Walsh spectrum of* f *is* $\{0, \pm 2^m, \pm 2^{m+1}\}$.

Proof. We only give the proof for the case of (1) since the other case can be proved in the same manner.

(1) If $(t_0, t_4, t_5, t_6) = (1, 1, 1, 1)$, then Eq. (10) can be reduced as

$$\hat{f}(b) = \frac{1}{4}(-2^m)(-1)^A \Big(2 + 2(-1)^{c_4} + \sum_{i=1}^{3}(-1)^{c_i} - (-1)^{\sum_{i=1}^{3} c_i + 1} - \sum_{i=1}^{3}(-1)^{c_i + c_4 + 1} + (-1)^{\sum_{i=1}^{4} c_i}\Big).$$

Thus if $c_4 = 0$, we have

$$\hat{f}(b) = \begin{cases} 3 \cdot 2^m (-1)^{A+1}, & wt(c_1, c_2, c_3) = 0, \\ 2^m (-1)^A, & wt(c_1, c_2, c_3) = 3, \\ 2^m (-1)^{A+1}, & \text{otherwise.} \end{cases}$$

And if $c_4 = 1$, we have

$$\hat{f}(b) = \frac{1}{4}(-2^m)(-1)^A(0) = 0.$$

The remaining cases of proof are similar to that of $(t_0, t_4, t_5, t_6) = (1, 1, 1, 1)$, so we omit it here. □

Let $m = 6$ and ξ be a primitive element in $\mathbb{F}_{2^6}$ such that $\xi^6 + \xi^4 + \xi^3 + \xi + 1 = 0$.

Example 1. Let $\lambda = a = 1, a_1 = \xi, a_2 = \xi^5, a_3 = \xi^7$. Then we have $(t_0, t_4, t_5, t_6) = (0, 0, 0, 0)$ and it was verified by a Magma program that

$$f(x) = Tr_1^3(x^9) + Tr_1^6(x)Tr_1^6(\xi x)Tr_1^6((\xi^5 + \xi^7)x) + Tr_1^6(x)Tr_1^6(\xi^5 x)Tr_1^6(\xi^7 x)$$

is a bent function. This is consistent with our result in Theorem 1.

Example 2. Let $\lambda = a = 1, a_1 = \xi^3, a_2 = \xi^6, a_3 = \xi^{12}$. Then we have $(t_0, t_4, t_5, t_6) = (0, 1, 1, 1)$ and it was verified by a Magma program that

$$f(x) = Tr_1^3(x^9) + Tr_1^6(x)Tr_1^6(\xi^3 x)Tr_1^6((\xi^6 + \xi^{12})x) + Tr_1^6(x)Tr_1^6(\xi^6 x)Tr_1^6(\xi^{12} x)$$

is a semi-bent function. This is consistent with our result in Theorem 2.

Example 3. (1) If $\lambda = 1, a = \xi, a_1 = \xi^3, a_2 = \xi^9, a_3 = \xi^{13}$, then we have $(t_0, t_4, t_5, t_6) = (1, 1, 1, 1)$ and it was verified by a Magma program that

$$f(x) = Tr_1^3(x^9) + Tr_1^6(\xi x)Tr_1^6(\xi^3 x)Tr_1^6((\xi^5 + \xi^{13})x) + Tr_1^6(\xi x)Tr_1^6(\xi^5 x)Tr_1^6(\xi^{13} x)$$

has $\{0, \pm 2^3, \pm 3 \cdot 2^3\}$ five-valued Walsh spectra.

(2) If $\lambda = a = 1, a_1 = \xi, a_2 = \xi^2, a_3 = \xi^4$, then we have $(t_0, t_4, t_5, t_6) = (1, 0, 0, 0)$ and it was verified by a Magma program that

$$f(x) = Tr_1^3(x^9) + Tr_1^6(x)Tr_1^6(\xi x)Tr_1^6((\xi^2 + \xi^4)x) + Tr_1^6(x)Tr_1^6(\xi^2 x)Tr_1^6(\xi^4 x)$$

has $\{0, \pm 2^3, \pm 2^4\}$ five-valued Walsh spectra.

4 The Walsh Spectrum of the Functions Given in Section 3

In this section, we give a spectrum distribution of the Boolean functions proposed in Sect. 3 with five-valued Walsh spectra.

Theorem 4. *Let a, a_1, a_2, a_3 are linear independent over $\mathbb{F}_2$. Then for $f(x)$ given by Eq. (6), the following statements hold:*

(1) If $(t_0, t_4, t_5, t_6) = (1, 1, 1, 1)$, then the spectrum distribution of $f(x)$ is

$$\hat{f}(b) = \begin{cases} (-1)^A 3 \cdot 2^m, & 2^{n-5} + (-1)^A 2^{m-4}(1 + \sum_{i=1}^{3}(-1)^{t_i}) \text{ times}, \\ (-1)^A 2^m, & 7 \cdot 2^{n-5} + (-1)^A 2^{m-4}(5 - 3\sum_{i=1}^{3}(-1)^{t_i}) \text{ times}, \\ 0, & 2^{n-1} \text{ times}. \end{cases}$$

(2) If $(t_0, t_4, t_5, t_6) = (1, 0, 0, 0)$, then the spectrum distribution of $f(x)$ is

$$\hat{f}(b) = \begin{cases} (-1)^A 2^{m+1}, & 2^{n-4} \text{ times}, \\ (-1)^A 2^m, & 2^{n-2} + (-1)^A 2^{m-1} \text{ times}, \\ 0, & 3 \cdot 2^{n-3} \text{ times}. \end{cases}$$

(3) For other cases, the spectrum distribution of $f(x)$ is

$$\hat{f}(b) = \begin{cases} (-1)^{A+1} 2^{m+1}, & 2^{n-4} + (-1)^{A+1} 2^{m-3}(1 - (-1)^{\delta}) \text{ times}, \\ (-1)^A 2^m, & 2^{n-2} + (-1)^A 2^{m-2}(1 + (-1)^{\delta}) \text{ times}, \\ 0, & 3 \cdot 2^{n-3} \text{ times}, \end{cases}$$

with

$$\delta = \begin{cases} t_1, & \text{if } (t_0, t_4, t_5, t_6) = (0, 0, 0, 1), \\ t_2, & \text{if } (t_0, t_4, t_5, t_6) = (0, 1, 0, 0), \\ t_3, & \text{if } (t_0, t_4, t_5, t_6) = (0, 0, 1, 0), \\ t_1 + 1, & \text{if } (t_0, t_4, t_5, t_6) \in \{(0, 1, 1, 0), (1, 0, 0, 1), (1, 1, 1, 0)\}, \\ t_2 + 1, & \text{if } (t_0, t_4, t_5, t_6) \in \{(0, 0, 1, 1), (1, 1, 0, 0), (1, 0, 1, 1)\}, \\ t_3 + 1, & \text{if } (t_0, t_4, t_5, t_6) \in \{(0, 1, 0, 1), (1, 0, 1, 0), (1, 1, 0, 1)\}. \end{cases}$$

Proof. We only prove $(t_0, t_4, t_5, t_6) = (0, 0, 0, 1)$, i.e., $\delta = t_1$ in (3), since the other cases can be proved in the same method. If $(t_0, t_4, t_5, t_6) = (0, 0, 0, 1)$, then from Eq. (10) we have

$$\hat{f}(b) = \frac{1}{4}(-2^m)(-1)^A(2 + 2(-1)^{c_4} + \sum_{i=1}^{3}(-1)^{c_i} + (-1)^{\sum_{i=1}^{3} c_i+1} + \sum_{i=1}^{2}(-1)^{c_i+c_4+1} + (-1)^{c_3+c_4} + (-1)^{\sum_{i=1}^{4} c_i+1}).$$

So if $c_4 = 0$, we have

$$\hat{f}(b) = \begin{cases} 2^m(-1)^{A+1}, & (c_1, c_2, c_3) \in \{(0,0,0), (0,0,1), (1,1,0), (1,1,1)\}, \\ 2^{m+1}(-1)^{A+1}, & (c_1, c_2, c_3) \in \{(1,0,0), (0,1,0)\}, \\ 0, & (c_1, c_2, c_3) \in \{(1,0,1), (0,1,1)\}, \end{cases} \tag{11}$$

and if $c_4 = 1$, we have

$$\hat{f}(b) = \begin{cases} 2^m(-1)^{A+1}, & (c_1, c_2) = (0,0), \\ 2^m(-1)^A, & (c_1, c_2) = (1,1), \\ 0, & (c_1, c_2) \in \{(0,1), (1,0)\}. \end{cases} \tag{12}$$

Now we figure out the number of $b \in \mathbb{F}_{2^n}$ such that $\hat{f}(b) = 2^{m+1}$, i.e., $c_4 = 0, A = 1$. Let N_1 denote the number of $b \in \mathbb{F}_{2^n}$ such that $(c_1, c_2, c_3, c_4, A) \in \{(1,0,0,0,1), (0,1,0,0,1)\}$. Then we have

$$\begin{aligned} N_1 &= \sum_{b \in \mathbb{F}_{2^n}} \Big(\frac{1+(-1)^{c_4}}{2} \cdot \frac{1+(-1)^{c_1+1}}{2} \cdot \frac{1+(-1)^{c_2}}{2} \cdot \frac{1+(-1)^{c_3}}{2} \cdot \frac{1+(-1)^{A+1}}{2} \\ &\quad + \frac{1+(-1)^{c_4}}{2} \cdot \frac{1+(-1)^{c_1}}{2} \cdot \frac{1+(-1)^{c_2+1}}{2} \cdot \frac{1+(-1)^{c_3}}{2} \cdot \frac{1+(-1)^{A+1}}{2} \Big) \\ &= \frac{1}{2^5} \sum_{\substack{d_i \in \mathbb{F}_2 \\ 1 \leqq i \leqq 4}} \sum_{b \in \mathbb{F}_{2^n}} \Big((-1)^{\sum_{i=1}^{4} d_i c_i + d_1} + (-1)^{\sum_{i=1}^{4} d_i c_i + d_2} \\ &\quad + (-1)^{\sum_{i=1}^{4} d_i c_i + d_1 + A + 1} + (-1)^{\sum_{i=1}^{4} d_i c_i + d_2 + A + 1} \Big). \end{aligned}$$

To calculate N_1, we first consider $N_{11} = \sum_{\substack{d_i \in \mathbb{F}_2 \\ 1 \leqq i}} \sum_{b \in \mathbb{F}_{2^n}} (-1)^{\sum_{i=1}^{4} d_i c_i + d_1}$ and $N_{12} = \sum_{\substack{d_i \in \mathbb{F}_2 \\ 1 \leqq i}} \sum_{b \in \mathbb{F}_{2^n}} (-1)^{\sum_{i=1}^{4} d_i c_i + d_2}$, from the definitions of $c_i, 1 \leqq i \leqq 3$, we have

$$
\begin{aligned}
N_{11} &= \sum_{\substack{d_i\in\mathbb{F}_2\\ 1\leqq i\leqq 4}} \sum_{b\in\mathbb{F}_{2^n}} (-1)^{\sum_{i=1}^{3} Tr_1^m(d_i\lambda^{-1}(b^{2^m}a_i+ba_i^{2^m}+a_i^{2^m+1}))} \\
&\quad \cdot(-1)^{Tr_1^m(d_4\lambda^{-1}(b^{2^m}a+ba^{2^m}+a^{2^m+1}))+d_1} \\
&= \sum_{\substack{d_i\in\mathbb{F}_2\\ 1\leqq i\leqq 4}} (-1)^{Tr_1^m(\lambda^{-1}(\sum_{i=1}^{3} d_ia_i^{2^m+1}+d_4a^{2^m+1}))+d_1} \\
&\quad \cdot \sum_{b\in\mathbb{F}_{2^n}} (-1)^{Tr_1^m(\lambda^{-1}(b^{2^m}(\sum_{i=1}^{3} d_ia_i+d_4a)+b(\sum_{i=1}^{3} d_ia_i+d_4a)^{2^m}))}
\end{aligned}
$$

Note that a_1, a_2, a_3 and a are linear independent, that is, we have $\sum_{i=1}^{3} d_ia_i+d_4a \neq 0$ if and only if $(d_1,\cdots,d_4)\neq(0,\cdots,0)$. If $(d_1,\cdots,d_4)\in\mathbb{F}_2^4\backslash\{(0,\cdots,0)\}$, then we have

$$
\sum_{b\in\mathbb{F}_{2^n}} (-1)^{Tr_1^m(\lambda^{-1}(b^{2^m}(\sum_{i=1}^{3} d_ia_i+d_4a)+b(\sum_{i=1}^{3} d_ia_i+d_4a)^{2^m}))} = 0
$$

since $\lambda\neq 0$. Therefore, we obtain

$$
N_{11} = \begin{cases} 2^n, (d_1,\cdots,d_4)=(0,\cdots,0), \\ 0, \quad \text{otherwise.} \end{cases}
$$

Then by a similar argument, we can also have $N_{12}=N_{11}$.

Now we considered $N_{13} = \sum_{\substack{d_i\in\mathbb{F}_2\\ 1\leqq i\leqq 4}} \sum_{j=1}^{2} \sum_{b\in\mathbb{F}_{2^n}} (-1)^{\sum_{i=1}^{4} d_ic_i+A+d_j+1}$, then we have

$$
\begin{aligned}
N_{13} &= \sum_{\substack{d_i\in\mathbb{F}_2\\ 1\leqq i\leqq 4}} \sum_{j=1}^{2} \sum_{b\in\mathbb{F}_{2^n}} (-1)^{\sum_{i=1}^{3} d_iTr_1^m(\lambda^{-1}(b^{2^m}a_i+ba_i^{2^m}+a_i^{2^m+1}))} \\
&\quad \cdot(-1)^{d_4Tr_1^m(\lambda^{-1}(b^{2^m}a+ba^{2^m}+a^{2^m+1}))} \cdot (-1)^{Tr_1^m(\lambda^{-1}b^{2^m+1})+d_j+1} \\
&= \sum_{\substack{d_i\in\mathbb{F}_2\\ 1\leqq i\leqq 4}} \sum_{j=1}^{2} (-1)^{\sum_{i=1}^{2} Tr_1^n(\lambda^{-1}d_id_{i+1}a_i^{2^m}a_{i+1})+Tr_1^n(\lambda^{-1}d_3d_1a_3^{2^m}a_1)} \\
&\quad \cdot(-1)^{\sum_{i=1}^{3} d_iTr_1^n(\lambda^{-1}d_id_4a_i^{2^m}a)+d_j+1} \cdot \sum_{b\in\mathbb{F}_{2^n}} (-1)^{Tr_1^m(\lambda^{-1}(b+\sum_{i=1}^{3} d_ia_i+d_4a)^{2^m+1})}.
\end{aligned}
$$

Note that $\sum_{b\in\mathbb{F}_{2^n}}(-1)^{Tr_1^m(\lambda^{-1}(b+\sum_{i=1}^{3}d_ia_i+d_4a)^{2^m+1})}=-2^m$ from the bentness of $Tr_1^m(\lambda^{-1}x^{2^m+1})$. Thus, one can obtain that N_{13} can expressed as

$$N_{13}=\sum_{\substack{d_i\in\mathbb{F}_2\\1\leqq i\leqq 4}}\sum_{j=1}^{2}2^m(-1)^{\sum_{i=1}^{2}d_id_{i+1}t_i+d_1d_3t_3+\sum_{i=1}^{3}d_4d_it_{i+3}+d_j}.$$

So we get

$$\begin{aligned}N_1&=\frac{1}{2^5}(N_{11}+N_{12}+N_{13})\\&=2^{n-4}+2^{m-4}\Big(3-(-1)^{t_4}+\sum_{i=5}^{6}(-1)^{t_i}-(-1)^{t_3}-(-1)^{t_1}+(-1)^{t_2}\\&\quad-(-1)^{t_3+t_4+t_6}-(-1)^{t_0}+(-1)^{t_2+t_5+t_6}-(-1)^{t_1+t_4+t_5}-(-1)^{\sum_{i=1}^{6}t_i}\Big)\\&=2^{n-4}+2^{m-3}(1-(-1)^{t_1}).\end{aligned}$$

Let N_2 denote the number of $b\in\mathbb{F}_{2^n}$ such that $\hat{f}(b)=0$. It then follows from Eqs. (11) and (12) that $\hat{f}(b)=0$ for any $(c_1,c_2,c_3,c_4)\in\{(1,0,1,0),(0,1,1,0),(0,1,0,1),(0,1,1,1),(1,0,0,1),(1,0,1,1)\}$. It is the same as the calculation of N_{11}, we have

$$\begin{aligned}N_2&=\frac{1}{2^4}\sum_{\substack{d_i\in\mathbb{F}_2\\1\leqq i\leqq 4}}\sum_{b\in\mathbb{F}_{2^n}}\Big((-1)^{\sum_{i=1}^{4}d_ic_i+d_1+d_3}+(-1)^{\sum_{i=1}^{4}d_ic_i+d_2+d_3}+(-1)^{\sum_{i=1}^{4}d_ic_i+d_2+d_4}\\&\quad+(-1)^{\sum_{i=1}^{4}d_ic_i+d_2+d_3+d_4}+(-1)^{\sum_{i=1}^{4}d_ic_i+d_1+d_4}+(-1)^{\sum_{i=1}^{4}d_ic_i+d_1+d_3+d_4}\Big)\\&=\frac{1}{2^4}(2^n+2^n+2^n+2^n+2^n+2^n)\\&=3\cdot 2^{n-3}.\end{aligned}$$

Let $n_1=|\{b\in\mathbb{F}_{2^n}:\hat{f}(b)=2^m\}|, n_2=|\{b\in\mathbb{F}_{2^n}:\hat{f}(b)=-2^m\}|$, and $n_3=|\{b\in\mathbb{F}_{2^n}:\hat{f}(b)=-2^{m+1}\}|$. Then from Eq. (1) we have

$$\begin{cases}2^n=n_1+n_2+n_3+2^{n-4}+2^{m-3}-2^{m-3}(-1)^{t_1}+3\cdot 2^{n-3},\\2^n=2^m\cdot n_1-2^m\cdot n_2-2^{m+1}\cdot n_3+2^{m+1}\cdot(2^{n-4}+2^{m-3}-2^{m-3}(-1)^{t_1}),\\2^{2n}=(2^m)^2\cdot(n_1+n_2)+(-2^{m+1})^2\cdot n_3+(2^{m+1})^2\\\cdot(2^{n-3}+2^{m-3}-2^{m-3}(-1)^{t_1}).\end{cases}$$

After a simple calculation, we have

$$\begin{cases}n_1=2^{n-4}+2^{m-3}+2^{m-3}(-1)^{t_1},\\n_2=2^{n-4}-2^{m-3}-2^{m-3}(-1)^{t_1},\\n_3=2^{n-4}-2^{m-3}+2^{m-3}(-1)^{t_1}.\end{cases}$$

□

5 Conclusion

In this paper, a class of bent functions and their dual functions are constructed according to [11]. In addition, we obtain a class of semi-bent functions and some classes of five-valued Walsh spectra. Then according to the Magma program, we can see that the conclusion is consistent with our result in this paper.

References

1. 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). https://doi.org/10.1109/18.923730
2. 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 (2010)
3. Carlet, C., Mesnager, S.: On semibent Boolean functions. IEEE Trans. Inf. Theory **58**(5), 3287–3292 (2012). https://doi.org/10.1109/TIT.2011.2181330
4. Charpin, P., Pasalic, E., Tavernier, C.: On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inf. Theory **51**(12), 4286–4298 (2005). https://doi.org/10.1109/TIT.2005.858929
5. Chee, S., Lee, S., Kim, K.: Semi-bent functions. In: Pieprzyk, J., Safavi-Naini, R. (eds.) ASIACRYPT 1994. LNCS, vol. 917, pp. 105–118. Springer, Heidelberg (1995). https://doi.org/10.1007/BFb0000428
6. 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). https://doi.org/10.1007/s10623-005-6345-x
7. Khoo, K.: Sequence design and construction of cryptographic Boolean functions. Ph. D. Thesis, University Waterloo (Canada) (2004)
8. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes. North-Holland, New York (1977)
9. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_33
10. Mesnager, S.: Semi-bent functions from Dillon and Niho exponents, Kloosterman sums, and Dickson polynomials. IEEE Trans. Inf. Theory **57**(11), 7443–7458 (2011). https://doi.org/10.1109/TIT.2011.2160039
11. Mesnager, S.: Several new infinite families of bent functions and their duals. IEEE Trans. Inf. Theory **60**(7), 4397–4407 (2014). https://doi.org/10.1109/TIT.2014.2320974
12. Meier, W., Staffelbach, O.: Fast correlation attacks on stream ciphers. In: Barstow, D., et al. (eds.) EUROCRYPT 1988. LNCS, vol. 330, pp. 301–314. Springer, Heidelberg (1988). https://doi.org/10.1007/3-540-45961-8_28
13. Olsen, J., Scholtz, R.A., Welch, L.: Bent-function sequences. IEEE Trans. Inf. Theory **28**(6), 858–864 (1982). https://doi.org/10.1109/TIT.1982.1056589
14. Rothaus, O.S.: On bent functions. J. Comb. Theory Ser. A **20**(3), 300–305 (1976). https://doi.org/10.1016/0097-3165(76)90024-8
15. Wolfmann, J.: Special bent and near-Bent functions. Adv. Math. Commun. **8**(1), 21–33 (2014). https://doi.org/10.3934/amc.2014.8.21

16. Xu, G., Cao, X., Xu, S.: Several classes of Boolean functions with few Walsh transform values. Appl. Algebra Eng. Commun. Comput. **28**(2), 155–176 (2016). https://doi.org/10.1007/s00200-016-0298-3
17. Zheng, Y., Zhang, X.-M.: Plateaued functions. In: Varadharajan, V., Mu, Y. (eds.) ICICS 1999. LNCS, vol. 1726, pp. 284–300. Springer, Heidelberg (1999). https://doi.org/10.1007/978-3-540-47942-0_24
18. Zheng, Y., Zhang, X.-M.: Relationships between bent functions and complementary plateaued functions. In: Song, J.S. (ed.) ICISC 1999. LNCS, vol. 1787, pp. 60–75. Springer, Heidelberg (2000). https://doi.org/10.1007/10719994_6
19. Zheng, L., Peng, J., Kan, H., Li, Y.: Several new infinite families of bent functions via second order derivatives. Cryptogr. Commun. **12**(6), 1143–1160 (2020). https://doi.org/10.1007/s12095-020-00436-0