Boolean Functions with Six-Valued Walsh Spectra and Their Application *

Wengang Jin[1] Xiaoni Du[1†] Yanzhong Sun[1] Cuiling Fan[2]

[1]College of Mathematics and Statistics
Northwest Normal University, Lanzhou 730070, China
[2]School of Mathematics
Southwest Jiaotong University, Chengdu 614202, China

Abstract Boolean functions play an important role in coding theory and symmetric cryptography. In this paper, three classes of Boolean functions with six-valued Walsh spectra are presented and their Walsh spectrum distributions are determined. They are derived from three classes of bent functions by complementing the values of the functions at three different points, where the bent functions are the Maiorana-McFarland types, Dillon $\mathcal{PS}_{ap}$ types and the monomial form $Tr_1^n(\lambda x^{r(2^m-1)})$, respectively. As an application, some classes of binary linear codes are constructed by using the functions we presented and point out these codes can be used in secret sharing schemes with interesting access structure.
Keywords: Boolean function, bent function, six-valued Walsh spectra, Walsh spectrum

1 Introduction

Boolean functions have wide applications in both symmetric cryptography and error correcting code. Over the past decades, various criteria related to cryptographically desirable Boolean functions have been proposed and studied extensively, such as balancedness, high nonlinearity, correlation immunity, satisfiability of the propagation criterion and so on.

The Walsh transform of Boolean functions is a very efficient tool to study and analyze Boolean functions since many cryptographic properties of Boolean

*This work is supported by National Natural Science Foundation of China (61462077, 61772022).

†Corresponding author. Email: ymldxn@126.com.

functions can be characterized by their Walsh transform values, see [3, 5, 20, 21, 22, 23] also for more details. For example, bent functions and plateaued functions [2] can be described by their Walsh spectrum. More specifically, the first possesses exactly two distinct Walsh transform values with maximal nonlinearity and the latter functions are ones with exactly three distinct Walsh transform values, one is zero and the other two have the same absolute values. The set of all Walsh transform values of a Boolean function is called the Walsh spectrum, and if the cardinality of the spectrum is t then we call it has t values of Walsh spectra.

Recall that bent functions were introduced by Rothaus [21] in 1976 but they exist only in an even number of variables and are not balanced. To get balanced functions with good nonlinearity in odd or even number of variables, Chee *et al.* [5] and Zhang [25] generalized the bent functions to Semi-bent and Plateaued functions, respectively. After that, in 2000 Pei *et al.* [20] discussed Boolean functions with at most eight Walsh transform values. Later in 2011 Tu *et al.* [23] characterized all Boolean functions with exactly two distinct Walsh transform values in terms of their spectrum, and they pointed out that the Boolean functions with exactly two distinct Walsh transform values were close to bent functions and affine functions. For Boolean functions with three-valued or five-valued Walsh spectra or more distinct Walsh transform values, there were many bent-like constructions [26]. Recently, in [22], some classes of Boolean functions with four-valued Walsh spectra are presented by complementing the values of bent functions at two points, one of which is zero and the other is nonzero, and their Walsh spectrum distributions are determined finally.

Inspired by the previous works, in this paper, we present three classes of Boolean functions with six-valued Walsh spectra, which are derived from bent functions by complementing their values at the zero and another two nonzero points, and determine their Walsh spectrum distributions with a similar method. The first two classes are derived from the bent functions of the Maiorana-McFarland and Dillon $\mathcal{PS}_{ap}$ classes, and the third class comes from the monomial functions $Tr_1^n(\lambda x^{r(2^m-1)})$, where integers $n = 2m$ and r is a positive integer such that $gcd(r,\ 2^m+1) = 1$ and λ is an element in finite field $\mathbb{F}_{2^m}$.

The rest of the paper is organized as follows. In Section 2, we introduce some notation and preliminary results on Boolean functions. In Section 3, we propose the Boolean functions with six-valued Walsh spectra. In Section 4, we derive some classes of linear codes from the Walsh spectrum of the functions we constructed and examine the application of the codes. Section 5 concludes the paper.

2 Preliminaries

Throughout this paper, $\mathbb{F}_2^n$ denotes the n-dimensional vector space over $\mathbb{F}_2$ and B_n be the set of all n-variable Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.

Any Boolean function f admits a representation as a squarefree polynomial in n variables, called algebraic normal form (ANF)

$$f(x_1,\ldots,x_n)=\sum_{u\in\mathbb{F}_2^n} a_u\prod_{i=1}^{n}x_i^{u_i},\ u=(u_1,u_2,\ldots,u_n),\ a_u,u_i\in\mathbb{F}_2$$

where the sum is taken over $\mathbb{F}_2$, and the term $\prod_{i=1}^{n}x_i^{u_i}$ is called monomial. The algebraic degree $\deg(f)$ of the Boolean function f equals the maximum degree of those monomials whose coefficients are nonzero in its ANF and is referred to as affine if it has algebraic degree at most 1.

The Walsh transform of $f\in B_n$ is the integer valued function over $\mathbb{F}_2^n$ defined by

$$W_f(a)=\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x},\ a\in\mathbb{F}_2^n$$

where $a\cdot x$ is the usual inner product of vectors. Moreover, the value $W_f(a)$ is called Walsh coefficient of f at $a\in\mathbb{F}_2^n$ and the set of Walsh coefficients is called the Walsh spectrum of f. In particular, if we denote the Hamming weight of f by $wt(f)$, which define the cardinality of the set $\{x\in\mathbb{F}_2^n\mid f(x)\neq 0\}$, then we have $W_f(0)=2^n-2wt(f)$ and $wt(f)=2^{n-1}-\frac{1}{2}W_f(0)$.

For even n, if $f\in B_n$ with Wash spectrum distribution as

$$W_f(a)=\begin{cases}-2^{n/2}, & 2^{n-1}-2^{n/2-1}\text{ times},\\ 2^{n/2}, & 2^{n-1}+2^{n/2-1}\text{ times},\end{cases}$$

then f is called a bent function. Bent functions always occur in pairs. In fact, given a bent function $f\in B_n$, we define the dual function $\widetilde{f}$ of f by

$$W_f(a)=2^{n/2}(-1)^{\widetilde{f}(a)}.$$

In other words, we consider the signs of the Walsh-coefficients of f. Due to the involution law the Fourier transform is self-inverse, the dual of a bent function is still a bent function and the dual of $\widetilde{f}$ is equals to f.

We can naturally identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$. As the notion of a Walsh transform refers to a scalar product, it is convenient to choose the isomorphism such that the canonical scalar product in $\mathbb{F}_2^n$ coincides with the canonical scalar product in $\mathbb{F}_{2^n}$, which is the trace of the product: $x\cdot y=Tr_1^n(xy)$,

where $x, y \in \mathbb{F}_{2^n}$ and Tr_1^n denote the absolute trace function from $\mathbb{F}_{2^n}$ onto $\mathbb{F}_2$ given by

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

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

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

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

Another possible unique representation of a Boolean function f defined on $\mathbb{F}_2^n$ is by means of trace function. In fact, any n-variable Boolean function can be represented as follows

$$f(x) = \sum_{j \in \Gamma_n} Tr_1^{n_j}(a_j x^j) + a_0 + a_{2^n-1} x^{2^n-1},$$

where Γ_n is the set of integers obtained by choosing one element in each cyclotomic class $C_j = \{j \cdot 2^t \pmod{2^n-1} \mid t \in \mathbb{N}\}$, n_j is the size of C_j and $a_j \in \mathbb{F}_{2^{n_j}}$, as well as $a_0,\ a_{2^n-1} \in \mathbb{F}_2$. In particular, we call $f(x)$ of the form $Tr_1^{n_j}(a_j x^j)$ a monomial function.

3 Boolean Functions with Six-Valued Walsh Spectra Derived from bent Functions

In this section, we construct a function h starting from a given bent function f modifying its image at three points and establish the relation of the Walsh spectrum values between them. Then, as an application of the result, we study the Walsh transform of three classes of functions explicitly.

Below, we always let $\varepsilon \in \{0,1\}$ and $n = 2m \geq 6$ with m being a positive integer. Let $f(x)$ be a bent function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. For any two distinct elements $\omega, \nu \in \mathbb{F}_2^n \backslash \{0\}$, we define the Boolean function

$$h(x) = \begin{cases} f(x), & \text{if } x \in \mathbb{F}_2^n \backslash \{0, \omega, \nu\}, \\ f(x)+1, & \text{if } x \in \{0, \omega, \nu\}. \end{cases} \tag{1}$$

The following lemma describes the Walsh spectrum properties of the function $h(x)$ given in Eq.(1).

Lemma 1. *The Wlash spectrum value of $h(x)$ at $\mathrm{u} \in \mathbb{F}_2^n$ is given by*

$$W_h(\mathrm{u}) = W_f(\mathrm{u}) - 2((-1)^{f(0)} + (-1)^{f(\omega)+\mathrm{u}\cdot\omega} + (-1)^{f(\nu)+\mathrm{u}\cdot\nu}).$$

Proof. From the definition of the Walsh spectrum and $h(x)$, it is easy to get that

$$\begin{aligned} W_h(\mathrm{u}) &= \sum_{x\in\mathbb{F}_2^n}(-1)^{h(x)+\mathrm{u}\cdot x} \\ &= \sum_{x\in\mathbb{F}_2^n\setminus\{0,\omega,\nu\}}(-1)^{f(x)+\mathrm{u}\cdot x}+\sum_{x\in\{0,\omega,\nu\}}(-1)^{f(x)+1+\mathrm{u}\cdot x} \\ &= \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+\mathrm{u}\cdot x}-2\sum_{x\in\{0,\omega,\nu\}}(-1)^{f(x)+\mathrm{u}\cdot x} \\ &= W_f(\mathrm{u})-2((-1)^{f(0)}+(-1)^{f(\omega)+\mathrm{u}\cdot\omega}+(-1)^{f(\nu)+\mathrm{u}\cdot\nu}). \end{aligned}$$

Thus, we finish the proof of the lemma. □

For any $\mathrm{u}\in\mathbb{F}_2^n$, we denote by $\widetilde{f}(\mathrm{u})=\varepsilon$, then it follows from the definition of the dual function $\widetilde{f}$ of f and Lemma 1 that the Walsh spectrum of the function $h(x)$ in Eq.(1) satisfies

$$W_h(\mathrm{u})=\begin{cases}(-1)^{\varepsilon}2^m-6, & \text{if } \mathrm{u}\cdot\omega=f(\omega),\ \mathrm{u}\cdot\nu=f(\nu),\\ (-1)^{\varepsilon}2^m-2, & \text{if } \mathrm{u}\cdot\omega-f(\omega)\neq\mathrm{u}\cdot\nu-f(\nu),\\ (-1)^{\varepsilon}2^m+2, & \text{if } \mathrm{u}\cdot\omega=f(\omega)+1,\ \mathrm{u}\cdot\nu=f(\nu)+1,\end{cases} \tag{2}$$

if $f(0)=0$, and otherwise

$$W_h(\mathrm{u})=\begin{cases}(-1)^{\varepsilon}2^m+6, & \text{if } \mathrm{u}\cdot\omega=f(\omega)+1,\ \mathrm{u}\cdot\nu=f(\nu)+1,\\ (-1)^{\varepsilon}2^m+2, & \text{if } \mathrm{u}\cdot\omega-f(\omega)\neq\mathrm{u}\cdot\nu-f(\nu),\\ (-1)^{\varepsilon}2^m-2, & \text{if } \mathrm{u}\cdot\omega=f(\omega),\ \mathrm{u}\cdot\nu=f(\nu).\end{cases}$$

Below we can always assume that the bent function $f(x)$ satisfies $f(0)=0$, since we may consider the function $f(x)+1$ if $f(0)=1$.

In order to determine the Walsh spectrum distribution of $h(x)$, we need to introduce the following notation

$$\begin{aligned} S_{\varepsilon 0}&=\{\mathrm{u}\in\mathbb{F}_2^n\mid \widetilde{f}(\mathrm{u})=\varepsilon,\ \omega\cdot\mathrm{u}=0,\ \nu\cdot\mathrm{u}=0\},\\ S_{\varepsilon 1}&=\{\mathrm{u}\in\mathbb{F}_2^n\mid \widetilde{f}(\mathrm{u})=\varepsilon,\ \omega\cdot\mathrm{u}=0,\ \nu\cdot\mathrm{u}=1\},\\ S_{\varepsilon 2}&=\{\mathrm{u}\in\mathbb{F}_2^n\mid \widetilde{f}(\mathrm{u})=\varepsilon,\ \omega\cdot\mathrm{u}=1,\ \nu\cdot\mathrm{u}=0\},\\ S_{\varepsilon 3}&=\{\mathrm{u}\in\mathbb{F}_2^n\mid \widetilde{f}(\mathrm{u})=\varepsilon,\ \omega\cdot\mathrm{u}=1,\ \nu\cdot\mathrm{u}=1\}. \end{aligned}$$

Denote the cardinalities of a set S by $|S|$. Clearly, we have

$$|S_{0j}|=2^{n-2}-|S_{1j}|,\ 0\le j\le 3, \tag{3}$$

and

$$|S_{10}|+|S_{11}|+|S_{12}|+|S_{13}|=wt(\widetilde{f})=2^{n-1}-2^{m-1} \tag{4}$$

from the bentness of $\widetilde{f}$.

Thus, from the definition of $|S_{\varepsilon j}|$, we have the following equivalent form of Eq.(2).

If $f(\omega) = f(\nu)$, then

$$W_h(\mathrm{u}) = \begin{cases} (-1)^{\varepsilon} 2^m - 6, & A_0 \text{ times}, \\ (-1)^{\varepsilon} 2^m - 2, & |S_{\varepsilon 1}| + |S_{\varepsilon 2}| \text{ times}, \\ (-1)^{\varepsilon} 2^m + 2, & A_1 \text{ times}, \end{cases} \tag{5}$$

where $A_0 = \begin{cases} |S_{\varepsilon 0}|, & \text{if } f(\nu) = 0, \\ |S_{\varepsilon 3}|, & \text{if } f(\nu) = 1, \end{cases}$ and $A_1 = \begin{cases} |S_{\varepsilon 3}|, & \text{if } f(\nu) = 0, \\ |S_{\varepsilon 0}|, & \text{if } f(\nu) = 1. \end{cases}$

If $f(\omega) \neq f(\nu)$, then

$$W_h(\mathrm{u}) = \begin{cases} (-1)^{\varepsilon} 2^m - 6, & B_0 \text{ times}, \\ (-1)^{\varepsilon} 2^m - 2, & |S_{\varepsilon 0}| + |S_{\varepsilon 3}| \text{ times}, \\ (-1)^{\varepsilon} 2^m + 2, & B_1 \text{ times}, \end{cases} \tag{6}$$

where $B_0 = \begin{cases} |S_{\varepsilon 2}|, & \text{if } f(\nu) = 0, \\ |S_{\varepsilon 1}|, & \text{if } f(\nu) = 1, \end{cases}$ and $B_1 = \begin{cases} |S_{\varepsilon 1}|, & \text{if } f(\nu) = 0, \\ |S_{\varepsilon 2}|, & \text{if } f(\nu) = 1. \end{cases}$

In the rest of this section, we will construct three classes of Boolean functions from known bent functions and apply Lemma 1, and Eq.(2) or Eqs.(5) and (6) to determine the spectrum distribution of the new functions.

3.1 The Maiorana-McFarland Class

In this subsection, denote by $\mathbb{F}_2^n = \{(x,y) \mid x,y \in \mathbb{F}_2^m\}$. With the conclusion above, we will obtain the Walsh spectrum of the Boolean functions derived from the Maiorana-McFarland function class, which is defined by

$$f(x,y) = x \cdot \pi(y) + g(y),$$

where π is any permutation on $\mathbb{F}_2^m$ and g is a Boolean function on $\mathbb{F}_2^m$. It has been proved that such function is bent and the dual of $f(x,y)$ is $\widetilde{f}(x,y) = y \cdot \pi^{-1}(x) + g(\pi^{-1}(x))$, where π^{-1} is the inverse permutation of π.

Let a,b,c, and $d \in \mathbb{F}_2^m$ with $b \neq d$ and all of them are nonzeros. If we replace f by the Maiorana-McFarland function $f(x,y)$, replace u, ω and ν by (u,v), (a,b), and (c,d) in Eq.(1), respectively, then Eq.(1) becomes

$$h(x,y) = \begin{cases} f(x,y), & \text{if } (x,y) \in \mathbb{F}_2^m \times \mathbb{F}_2^m \backslash \{(0,0),(a,b),(c,d)\}, \\ f(x,y)+1, & \text{if } (x,y) \in \{(0,0),(a,b),(c,d)\}. \end{cases} \tag{7}$$

For the function $h(x,y)$ defined by Eq.(7), we have the following theorem.

Theorem 2. *Let $g(0)=0$ and $\pi(0)=0$. The spectrum distribution of the function $h(x,y)$ defined by Eq.(7) is given as*

$$W_h(u,v)=\begin{cases}(-1)^{\varepsilon}2^m-6, & 2^{n-3}+(-1)^{\varepsilon}2^{m-1} \text{ times},\\ (-1)^{\varepsilon}2^m-2, & 2^{n-2} \text{ times},\\ (-1)^{\varepsilon}2^m+2, & 2^{n-3} \text{ times},\end{cases}$$

if $g(b+d)=a\cdot\pi(b)+g(b)+a\cdot\pi(b+d)+c\cdot\pi(d)+g(d)+c\cdot\pi(b+d)$, and

$$W_h(u,v)=\begin{cases}(-1)^{\varepsilon}2^m-6, & 2^{n-3}+(-1)^{\varepsilon}2^{m-2} \text{ times},\\ (-1)^{\varepsilon}2^m-2, & 2^{n-2}+(-1)^{\varepsilon}2^{m-1} \text{ times},\\ (-1)^{\varepsilon}2^m+2, & 2^{n-3}-(-1)^{\varepsilon}2^{m-2} \text{ times},\end{cases}$$

otherwise, where $\varepsilon\in\{0,1\}$.

Proof. According to Lemma 1 and Eq.(2), to determine the spectrum distribution of the function $h(x,y)$, we need to examine the number of $(u,v)\in\mathbb{F}_2^m$ such that $(u,v)\cdot(a,b)-f(a,b)=(u,v)\cdot(c,d)-f(c,d)=0$ or 1, and $(u,v)\cdot(a,b)-f(a,b)\neq(u,v)\cdot(c,d)-f(c,d)$.

We first figure out the number of $(u,v)\in\mathbb{F}_2^m$ such that $W_h(u,v)=2^m-6$ and denote it by N. Note that $g(0)=\pi(0)=0$, thus, it suffices to calculate the number of solutions of the following equation system

$$\begin{cases}\pi^{-1}(u)\cdot v=g(\pi^{-1}(u)),\\ b\cdot v=a\cdot\pi(b)+g(b)+a\cdot u,\\ d\cdot v=c\cdot\pi(d)+g(d)+c\cdot u.\end{cases}\tag{8}$$

To solve the above equations system, we divide the discussion into four cases.

Case 1: If $\pi^{-1}(u)=0$, i.e. $u=0$, Eq.(8) can be reduced to

$$\begin{cases}b\cdot v=a\cdot\pi(b)+g(b),\\ d\cdot v=c\cdot\pi(d)+g(d).\end{cases}\tag{9}$$

Clearly, $N=2^{m-2}$.

Case 2: If $\pi^{-1}(u)\in\{b,d\}$, similar to the proof of Case 1, we get that $N=2^{m-2}$.

Case 3: If $\pi^{-1}(u)=b+d$, Eq.(8) becomes

$$\begin{cases}(b+d)\cdot v=g(b+d),\\ b\cdot v=a\cdot\pi(b)+g(b)+a\cdot\pi(b+d),\\ d\cdot v=c\cdot\pi(d)+g(d)+c\cdot\pi(b+d).\end{cases}\tag{10}$$

It is obvious that the number of (u,v) satisfying Eq.(10) is 2^{m-2} when $g(b+d)=a\cdot\pi(b)+g(b)+a\cdot\pi(b+d)+c\cdot\pi(d)+g(d)+c\cdot\pi(b+d)$, and is 0 otherwise.

Case 4: If $\pi^{-1}(u) \notin \{0, b, d, b+d\}$, $\pi^{-1}(u)$, b and d are linear independent, then for fixed u, the number of v satisfying Eq.(8) is 2^{m-3}, and thus $N = 2^{m-3}(2^m - 4) = 2^{n-3} - 2^{m-1}$.

From all the discussion above, we obtain the total number of (u, v) such that $W_h(u, v) = 2^m - 6$ is

$$2^{m-2} + 2 \cdot 2^{m-2} + 2^{m-2} + 2^{n-3} - 2^{m-1} = 2^{n-3} + 2^{m-1},$$

when $g(b+d) = a \cdot \pi(b) + g(b) + a \cdot \pi(b+d) + c \cdot \pi(d) + g(d) + c \cdot \pi(b+d)$, and is $2^{m-2} + 2 \cdot 2^{m-2} + 0 + 2^{n-3} - 2^{m-1} = 2^{n-3} + 2^{m-2}$ otherwise.

In a similar manner, we can get the spectrum distribution of the function $h(x, y)$. Thus we complete the proof of the theorem. □

3.2 Dillion $\mathcal{PS}_{ap}$ class

In this subsection, we will consider the Walsh spectrum of the Boolean function derived from Dillion $\mathcal{PS}_{ap}$ class. We begin this subsection by recalling Dillion $\mathcal{PS}_{ap}$ class.

Similar as in Section 3.1, we regard $\mathbb{F}_{2^n}$ as a two-dimensional vector space over $\mathbb{F}_{2^m}$. Dillon $\mathcal{PS}_{ap}$ class functions have the form $f(x, y) = g(xy^{2^m-2})$, or explicitly

$$f(x, y) = \begin{cases} 0, & \text{if } y = 0, \\ g(\frac{x}{y}), & \text{if } y \neq 0, \end{cases} \tag{11}$$

where $x, y \in \mathbb{F}_{2^m}$ and g is a balanced Boolean function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ with $g(0) = 0$. It is known that any such function is bent, and the dual of $f(x, y)$ is $\widetilde{f}(x, y) = g(yx^{2^m-2})$, see [2] for more details.

Let a, b, c, and $d \in \mathbb{F}_{2^m}^*$ with $ab^{-1} \neq cd^{-1}$. If we replace f by Dillion $\mathcal{PS}_{ap}$ class $f(x, y)$, replace u, ω and v by (u, v), (a, b), and (c, d) in Eq.(1), respectively, then Eq.(1) becomes

$$h(x, y) = \begin{cases} f(x, y), & \text{if } (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \\ & \backslash \{(0, 0), (a, b), (c, d)\}, \\ f(x, y) + 1, & \text{if } (x, y) \in \{(0, 0), (a, b), (c, d)\}. \end{cases} \tag{12}$$

For $h(x, y)$ defined above, we have the following theorem.

Theorem 3. *Let a, b, c, and $d \in \mathbb{F}_{2^m}^*$ with $ab^{-1} \neq cd^{-1}$. The spectrum distribution of the function $h(x, y)$ defined by Eq.(12) satisfies*

(i) if $f(a+c, b+d) = 0$ and $f(a, b) = f(c, d)$ or $f(a+c, b+d) = 1$ and $f(a, b) \neq f(c, d)$, then

$$W_h(u, v) = \begin{cases} (-1)^{\varepsilon} 2^m - 6, & 2^{n-3} + (-1)^{\varepsilon} 2^{m-1} \text{ times}, \\ (-1)^{\varepsilon} 2^m - 2, & 2^{n-2} \text{ times}, \\ (-1)^{\varepsilon} 2^m + 2, & 2^{n-3} \text{ times}, \end{cases}$$

(ii) if $f(a+c,b+d)=0$ *and* $f(a,b)\neq f(c,d)$ *or* $f(a+c,b+d)=1$ *and* $f(a,b)=f(c,d)$*, then*

$$W_h(u,v)=\begin{cases}(-1)^{\varepsilon}2^m-6, & 2^{n-3}+(-1)^{\varepsilon}2^{m-2} \text{ times},\\ (-1)^{\varepsilon}2^m-2, & 2^{n-2}+(-1)^{\varepsilon}2^{m-1} \text{ times},\\ (-1)^{\varepsilon}2^m+2, & 2^{n-3}-(-1)^{\varepsilon}2^{m-2} \text{ times}.\end{cases}$$

Proof. According to Lemma 1 and Eqs.(5) and (6), to determine the spectrum distribution of the function $h(x,y)$, we need to examine the values of $|S_{\varepsilon j}|$ for $\varepsilon\in\{0,1\}$ and $0\leq j\leq 3$.

It is trivial that $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ is the union of the 2^m+1 m-dimensional subspaces $U_e=\{(x,ex)\mid x\in\mathbb{F}_{2^m}\}$ and $V_0=\{(0,y)\mid y\in\mathbb{F}_{2^m}\}$ with $e\in\mathbb{F}_{2^m}$. Note that any two of these subspaces intersection at $(0,0)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$.

Below we only prove the theorem under the condition $f(a+c,b+d)=0$ since the case for $f(a+c,b+d)=1$ can be proved with a similar idea.

We first determine the cardinality $|S_{13}|$ of

$$S_{13}=\{(u,v)\in\mathbb{F}_{2^m}^2\mid \widetilde{f}(u,v)=1, Tr_1^m(au+bv)=1, Tr_1^m(cu+dv)=1\},$$

for the case of $f(a,b)=f(c,d)=1$.

From the definitions of g and $\widetilde{f}(x,y)$, one can find that the restriction of $\widetilde{f}(x,y)$ to U_e is $g(e)$ and to V_0 is 0. Meanwhile, if $(u,v)\in S_{1j}$, then there exist some $e\in\mathbb{F}_{2^m}^*$ such that $(u,v)\in U_e$ and $g(e)=1$. Thus, $|S_{13}|$ is equal to the total number of $(u,v)\in U_e$ for $e\in\mathbb{F}_{2^m}$ satisfying the following equations

$$\begin{cases} g(e)=1,\\ Tr_1^m((a+be)u)=1,\\ Tr_1^m((c+de)u)=1.\end{cases}\tag{13}$$

Since $f(a,b)=f(c,d)=1$ means that $g(ab^{-1})=g(cd^{-1})=1$, in order to determine $|S_{13}|$, we divide the discussion into the following two steps.

(1) If $e=ab^{-1}$ or $e=cd^{-1}$, Eq.(13) has no solution in $\mathbb{F}_{2^m}$.

(2) If $e\neq ab^{-1}$ and $e\neq cd^{-1}$, since the restriction $f(a+c,b+d)=0$ means that $a+be\neq c+de$ holds for all $g(e)=1$, then for any fixed $e\in\mathbb{F}_{2^m}$, the number of solutions to Eq.(13) is

$$\begin{aligned} N &= \sum_{u\in\mathbb{F}_{2^m}}\left(\frac{1-(-1)^{Tr_1^m((a+be)u)}}{2}\right)\left(\frac{1-(-1)^{Tr_1^m((c+de)u)}}{2}\right)\\ &= \frac{1}{4}\Big(\sum_{u\in\mathbb{F}_{2^m}}1-\sum_{u\in\mathbb{F}_{2^m}}(-1)^{Tr_1^m((a+be)u)}-\sum_{u\in\mathbb{F}_{2^m}}(-1)^{Tr_1^m((c+de)u)}\\ &\quad+\sum_{u\in\mathbb{F}_{2^m}}(-1)^{Tr_1^m((a+be)u)+Tr_1^m((c+de)u)}\Big)\\ &= 2^{m-2}.\end{aligned}$$

Then it follows from the balancedness of g and the arguments above that $|S_{13}| = 2^{m-2}(2^{m-1}-2) = 2^{n-3}-2^{m-1}$.

With a similar proof idea, one can get $|S_{13}|$ for other values of $f(a,b)$ and $f(c,d)$, and so we have

$$|S_{13}| = \begin{cases} 2^{n-3}-2^{m-1}, & \text{if } f(a,b)=f(c,d)=1, \\ 2^{n-3}, & \text{if } f(a,b)=f(c,d)=0, \\ 2^{n-3}-2^{m-2}, & \text{if } f(a,b)\neq f(c,d). \end{cases}$$

The determination of $|S_{11}|$ for

$$S_{11} = \{(u,v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mid \widetilde{f}(u,v) = 1, Tr_1^m(au+bv) = 0, Tr_1^m(cu+dv) = 1\}$$

is very similar to that of $|S_{13}|$, we only present a sketch here. $|S_{11}|$ is equal to the number of solutions to equations

$$\begin{cases} g(e) = 1, \\ Tr_1^m((a+be)u) = 0, \\ Tr_1^m((c+de)u) = 1. \end{cases} \tag{14}$$

If $f(a,b) = f(c,d) = 1$, we divide the discussion into three steps.

(1) If $e = ab^{-1}$, there are 2^{m-1} many u satisfying Eq.(14).

(2) If $e = cd^{-1}$, there is no solution.

(3) If $e \neq ab^{-1}$ and $e \neq cd^{-1}$, since $f(a+c,b+d) = 0$, then for any fixed $e \in \mathbb{F}_{2^m}$, the number of solutions to Eq.(14) is

$$\begin{aligned} N &= \sum_{u \in \mathbb{F}_{2^m}} \left(\frac{1+(-1)^{Tr_1^m((a+be)u)}}{2}\right)\left(\frac{1-(-1)^{Tr_1^m((c+de)u)}}{2}\right) \\ &= 2^{m-2}. \end{aligned}$$

Thus, we have $|S_{11}| = 2^{m-2}(2^{m-1}-2)+2^{m-1} = 2^{n-3}$.

Similarly, we could determine the cardinality of S_{11} for the other cases, and we get

$$|S_{11}| = \begin{cases} 2^{n-3}, & \text{if } f(a,b)=f(c,d), \\ 2^{n-3}+(-1)^{\varepsilon}2^{m-2}, & \text{if } f(a,b)\neq f(c,d)=\varepsilon. \end{cases}$$

With a similar idea, we have

$$|S_{12}| = \begin{cases} 2^{n-3}, & \text{if } f(a,b)=f(c,d), \\ 2^{n-3}-(-1)^{\varepsilon}2^{m-2}, & \text{if } f(a,b)\neq f(c,d)=\varepsilon. \end{cases}$$

Thus, by Eq.(4), we have

$$|S_{10}| = \begin{cases} 2^{n-3}, & \text{if } f(a,b)=f(c,d)=1, \\ 2^{n-3}-2^{m-1}, & \text{if } f(a,b)=f(c,d)=0, \\ 2^{n-3}-2^{m-2}, & \text{if } f(a,b)\neq f(c,d). \end{cases}$$

Combining Eqs.(3), (5) and (6) and the above enumeration, we finish the proof of the theorem. □

3.3 The Monomial Function $Tr_1^n(\lambda x^{r(2^m-1)})$

In this subsection, we will present a class of Boolean functions with six-valued Walsh spectra which are derived from the bent function $f(x) = Tr_1^n(\lambda x^{r(2^m-1)})$, where r is a positive integer such that $gcd(r, 2^m+1) = 1$ and $\lambda \in \mathbb{F}_{2^m}$ with K-loosterman sums $K_m(\lambda) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(\lambda x + x^{2^{m-1}-1})} = 0$ [4], and in such case the dual of $f(x)$ is itself. We should mention that $Tr_1^n(\lambda x^{r(2^m-1)})$ is a known class of monomial functions with two or three-valued Walsh spectra and have tight connection with Kloosterman sums, which have been studied extensively by many researchers, e.g., Charpin and Gong [4], Leander [13], and Mesnager [16].

Let $b, c \in \mathbb{F}_{2^n}^*$ with $b \neq c$. Define Boolean function $h(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ by

$$h(x) = f(x) + x^{2^n-1} + ((x+b)(x+c))^{2^n-1},$$

i.e.

$$h(x) = \begin{cases} f(x), & \text{if } x \in \mathbb{F}_{2^n}^* \backslash \{b, c\}, \\ f(x)+1, & \text{if } x \in \{0, b, c\}. \end{cases} \tag{15}$$

For $h(x)$ defined above, we have the following.

Theorem 4. *With the notation as above. Suppose $(b,c) \in \mu_0\mathbb{F}_{2^m}^* \times \mu_0\mathbb{F}_{2^m}^*$, where $b \neq c$ and $\mu_0 \in \{x \in \mathbb{F}_{2^n} \mid x^{2^m+1} = 1\}$, then $h(x)$ defined in Eq.(15) is a function with six-valued Walsh spectra and its spectrum distribution is*

$$W_h(u) = \begin{cases} (-1)^{\varepsilon}2^m - 6, & 2^{n-3} + (-1)^{\varepsilon}2^{m-1} \text{ times}, \\ (-1)^{\varepsilon}2^m - 2, & 2^{n-2} \text{ times}, \\ (-1)^{\varepsilon}2^m + 2, & 2^{n-3} \text{ times}, \end{cases}$$

if $f(b) = 0$, and

$$W_h(u) = \begin{cases} (-1)^{\varepsilon}2^m - 6, & 2^{n-3} + (-1)^{\varepsilon}2^{m-2} \text{ times}, \\ (-1)^{\varepsilon}2^m - 2, & 2^{n-2} + (-1)^{\varepsilon}2^{m-1} \text{ times}, \\ (-1)^{\varepsilon}2^m + 2, & 2^{n-3} - (-1)^{\varepsilon}2^{m-2} \text{ times}, \end{cases}$$

if $f(b) = 1$.

Proof. To determine the Walsh spectrum distribution of $h(x)$, we first introduce the polar decomposition of the elements in $\mathbb{F}_{2^n}^*$. As a cyclic multiplicative group of order 2^n-1, $\mathbb{F}_{2^n}^*$ is a direct product of its two subgroups of orders 2^m+1 and 2^m-1, respectively, and the two subgroups are given by $U = \{x \in \mathbb{F}_{2^n} \mid x^{2^m+1} = 1\}$ and $\mathbb{F}_{2^m}^*$. Thus, any element x of $\mathbb{F}_{2^n}^*$ has a unique polar decomposition of the form $x = \mu y$, where $\mu \in U$ and $y \in \mathbb{F}_{2^m}^*$, and more precisely, $\mu = x^{(2^m-1)2^{m-1}}$ and $y = x^{(2^m+1)2^{m-1}}$.

Similarly, we can rewrite $b, c \in \mu_0\mathbb{F}_{2^m}^*$ as $b = \mu_0 y_0$, $c = \mu_0 y_1$, where $\mu_0 = b^{(2^m-1)2^{m-1}} \in U$, $y_0 = b^{(2^m+1)2^{m-1}}$, and $y_1 = c^{(2^m+1)2^{m-1}} \in \mathbb{F}_{2^m}^*$, then we have

$$Tr_1^n(bx) = Tr_1^m((\mu_0\mu + (\mu_0\mu)^{-1})y_0 y),$$

and $Tr_1^n(cx) = Tr_1^m((\mu_0\mu + (\mu_0\mu)^{-1})y_1 y)$.

Now we are ready to examine the values of $|S_{\varepsilon j}|$ for $0 \le j \le 3$. We first calculate $|S_{13}|$, i.e., the number of $x = \mu y \in \mathbb{F}_{2^n}^*$ with $\mu \in U$ and $y \in \mathbb{F}_{2^m}^*$ satisfying S_{13} which is given as

$$\begin{cases} f(\mu) = 1, \\ Tr_1^m((\mu_0\mu + (\mu_0\mu)^{-1})y_0 y) = 1, \\ Tr_1^m((\mu_0\mu + (\mu_0\mu)^{-1})y_1 y) = 1. \end{cases} \tag{16}$$

To solve Eq.(16), we proceed in the following steps.

(1) If $\mu_0\mu = 1$, Eq.(16) has no solution.

(2) If $\mu_0\mu \neq 1$, there are 2^{m-2} y satisfy Eq.(16). So we only need to examine the number of $\mu \in U$ such that $\mu_0\mu \neq 1$ and $f(\mu) = 1$, which we denote by N. Put $T = \{\mu \in U \mid f(\mu) = 1\}$. Note the fact that $f(x)$ is constant on each coset $\mu\mathbb{F}_{2^m}^*$ since $f(x) = f(\mu y) = f(\mu)$, hence, $|T| = wt(f)/(2^m - 1) = 2^{m-1}$. If $f(\mu_0^{-1}) = 0$, then $\mu_0^{-1} \notin T$, so $\mu_0\mu \neq 1$ holds for all $\mu \in T$, and thus $N = 2^{m-1}$. If $f(\mu_0^{-1}) = 1$, that is $\mu_0^{-1} \in T$, so $\mu_0\mu \neq 1$ holds for all $\mu \in T \setminus \{\mu_0^{-1}\}$, and thus, $N = 2^{m-1} - 1$.

Combining the arguments above, we get

$$|S_{13}| = \begin{cases} 2^{m-2}2^{m-1} = 2^{n-3}, & \text{if } f(\mu_0^{-1}) = 0, \\ 2^{m-2}(2^{m-1} - 1) = 2^{n-3} - 2^{m-2}, & \text{if } f(\mu_0^{-1}) = 1. \end{cases}$$

With a similar argument, we have $|S_{11}| = |S_{12}| = |S_{13}|$, and then by Eq.(4),

$$|S_{10}| = \begin{cases} 2^{n-3} - 2^{m-1}, & \text{if } f(\mu_0^{-1}) = 0, \\ 2^{n-3} + 2^{m-2}, & \text{if } f(\mu_0^{-1}) = 1. \end{cases}$$

It is clear to see that

$$f(\mu_0^{-1}) = f(b^{-1}),$$

then we have $f(b) = f(b^{-1})$ for all $b \in \mu_0\mathbb{F}_{2^m}^*$ by the definition of $f(x)$.

Combining Eqs.(3), (5) and (6) and the arguments above, we finish the proof of the theorem. □

4 Application

In this section, we will give some applications by using the Walsh spectrum value of the new Boolean functions. We first introduce some notation and preliminary results on linear codes.

An $[n,k,\delta]$ linear code $\mathcal{C}$ over $\mathbb{F}_2$ is a k-dimensional subspace of $\mathbb{F}_2^n$ with minimum Hamming distance δ. Let A_i be the number of codewords with Hamming weight i in a code $\mathcal{C}$. The weight enumerator of $\mathcal{C}$ is defined by $1+A_1z+A_2z^2+\ldots+A_nz^n$, and the sequence $(1,A_1,\ldots,A_n)$ is called the weight distribution of the code $\mathcal{C}$.

A classical construction of linear codes is based on the defining set, that is, let defining set D

$$D=\{d_1,d_2,\ldots,d_n\}\subseteq\mathbb{F}_{2^n}.$$

The linear code $\mathcal{C}_D$ of length n over $\mathbb{F}_2$ is defined by

$$\mathcal{C}_D=\{(Tr_1^n(xd_1),Tr_1^n(xd_2),\ldots,Tr_1^n(xd_n)):x\in\mathbb{F}_{2^n}\}. \tag{17}$$

For a Boolean function f from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, the support of f is defined as

$$D_f=\{x\in\mathbb{F}_{2^n}:f(x)=1\}, \tag{18}$$

and we denote by $n_f=|D_f|$. In the following we will study the relationship between the Boolean function and the binary linear code $\mathcal{C}_{D_f}$ with length n_f and dimension at most n.

The following theorem is well known [9] and it implies the relationship between the weight distribution of a linear code and the Walsh spectrum distribution of a Boolean function.

Theorem 5. *Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ and n_f the cardinality of the support of f. If $2n_f+W_f(\omega)\neq 0$ for all $\omega\in\mathbb{F}_{2^n}^*$, then $\mathcal{C}_{D_f}$ is a binary code with the parameter $[n_f,m]$, and its weight distribution is given by the following multiset:*

$$\{\{\frac{2n_f+W_f(\omega)}{4}:\omega\in\mathbb{F}_{2^n}^*\}\}\cup\{\{0\}\}.$$

Next, we will apply Theorem 5 to construct linear codes from the three classes of Boolean functions with six Walsh spectrum. Without loss of generality, we consider the function $h(x)$ given in Theorem 4. By the definition of $h(x)$, we have $n_h\in\{2^{n-1}-2^{\frac{n}{2}-1}-1,2^{n-1}-2^{\frac{n}{2}-1}+1,2^{n-1}-2^{\frac{n}{2}-1}+3\}$, and thus it is obvious that $2n_h+W_h(\omega)\neq 0$ for all $\omega\in\mathbb{F}_{2^n}^*$.

Theorem 6. *If $f(b)=1$, then the weight distribution of the code $\mathcal{C}_{D_f}$ with the parameter $[2^{n-1}-2^{\frac{n}{2}-1}+1-2f(c),n]$ is shown in Table 1. If $f(b)=0$, then the weight distribution of the code $\mathcal{C}_{D_f}$ with the parameter $[2^{n-1}-2^{\frac{n}{2}-1}+3-2f(c),n]$ is shown in Table 2.*

Table 1: The weight distribution of $\mathcal{C}_{D_f}$ when $f(b)=1$

Weight	Multiplicity
0	1
$2^{n-2}-1-f(c)$	$2^{n-3}+2^{\frac{n}{2}-2}$
$2^{n-2}-2^{\frac{n}{2}-1}-1-f(c)$	$2^{n-3}-2^{\frac{n}{2}-2+f(c)}$
$2^{n-2}-f(c)$	$2^{n-2}+2^{\frac{n}{2}-1}$
$2^{n-2}-2^{\frac{n}{2}-1}-f(c)$	$2^{n-2}-2^{\frac{n}{2}-1}$
$2^{n-2}+1-f(c)$	$2^{n-3}-2^{\frac{n}{2}-2}-1$
$2^{n-2}-2^{\frac{n}{2}-1}+1-f(c)$	$2^{n-3}+2^{\frac{n}{2}-2}$

Table 2: The weight distribution of $\mathcal{C}_{D_f}$ when $f(b)=0$

Weight	Multiplicity
0	1
$2^{n-2}-f(c)$	$2^{n-3}+2^{\frac{n}{2}-1}-1$
$2^{n-2}-2^{\frac{n}{2}-1}-f(c)$	$2^{n-3}-2^{\frac{n}{2}-1}$
$2^{n-2}+1-f(c)$	2^{n-2}
$2^{n-2}-2^{\frac{n}{2}-1}+1-f(c)$	2^{n-2}
$2^{n-2}+2-f(c)$	2^{n-3}
$2^{n-2}-2^{\frac{n}{2}-1}+2-f(c)$	2^{n-3}

Let w_{min} and w_{max} denote the minimum and maximum non-zero weight of linear code $\mathcal{C}_{D_f}$, respectively. When $n \geq 6$, the codes $[2^{n-1}-2^{\frac{n}{2}-1}-1,n]$, $[2^{n-1}-2^{\frac{n}{2}-1}+1,n]$, $[2^{n-1}-2^{\frac{n}{2}-1}+3,n]$ all have

$$\frac{w_{\min}}{w_{\max}} > \frac{1}{2}.$$

From the results in [1] these codes are minimal. Minimal linear codes could be decode with the minimum distance decoding method, and have applications in secret sharing [1].

5 Conclusion

In this paper, we presented three classes of Boolean functions with six-valued Walsh spectra by modifying bent functions by complementing their values at the

zero point and other two nonzero points. The Walsh spectrum distribution of these classes of functions were also determined. Results shows that all the new Boolean functions possess the same Walsh spectrum distribution. As applications of the Walsh spectrum of the Boolean function we presented, some classes of binary linear codes were constructed, which can be used to construct secret sharing schemes with interesting access structure. Furthermore, all the codes we constructed are new according to the code table [11].

References

[1] A. Ashiknmi, A. Barg, Minimal vectors in linear codes IEEE Trans. Inf. Theory, 1998, 44(5): 2010-2017.

[2] C. Carlet, Boolean functions for cryptography and error correcting codes, Chapter of the monography, Boolean Models and Methods in Mathematics, Computer Science and Engineering, ed. by Crammma Y and Hammer P, Cambridge University Preess, 2010, 257-397.

[3] C. Carlet, S. Mesnager, Four decades of research on bent functions, Des. Codes Cryptogr, 2016, 78(1): 5-50.

[4] P. Charpin, G. Gong, Hypertbent functions, Kloosterman sum, and Dickson polynomials, IEEE Trans. Inf. Theory, 2008, 54(9): 4230-4238.

[5] S. Chee, S. Lee, and K. Kim, Semi-bent functions, Lecture Notes in Computer Science, 1995, 917:107-118.

[6] J. Dillion, Elementary hadamard difference sets, Ph.D. Thesis, Univ. of Maryland, City of College Park, 1974.

[7] H. Dobbertin, One-to-one highly nonlinear power functions on $GF(2^n)$, Appl. Algebra Eng. Comm. Comput., 1998, 9(2): 139-152.

[8] P. Delsarte, J. Goethals, Irreducible binary cyclic codes of even dimension, Combinatorial Mathematics and Its Applications, Proc. 2nd Chapel Hill Conf., Univ. North Carolina, Chapel Hill, NC, 1970, 100-113.

[9] C. Ding, Linear codes from some 2-designs, IEEE Trans. Inf. Theory, 2015, 60(6): 3265-3275.

[10] C. Ding, Z. Heng, Z. Zhou, Minimal Binary Linear Codes, IEEE Trans. Inf. Theory, 2018, 64(10): 6536-6545.

[11] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, online available at http://www.codetables.de/.

[12] T. Helleseth, P. Rosendahl, New pairs of m-sequences with 4-level cross-correlation, Finite Fields Appl, 2005, 11(4): 674-683.

[13] N. Leander, Monomial bent functions, IEEE Trans. Inf. Theory, 2006, 52(2): 738-743.

[14] G. Lachaud, J. Wolfmann, The weights of the orthogonals of the extended quadratic binary goppa codes, IEEE Trans. Inf. Theory, 1990, 36(3): 686-692.

[15] R. Lidl, H. Niederreiter, "Finite fields", Addison-Wesley Publishing Inc., Boston, 1983.

[16] S. Mesnager, Semi-bent functions from Dillon and Niho exponents, K-loosterman sums and Dickson polynomials, IEEE Trans. Inf. Theory, 2011, 57(11): 7443-7458.

[17] S. Mesnager, Bent Functions Fundamentals and Results, Springer 2016, ISBN 978-3-319-32593-4, 2016: 1-554.

[18] S. Mesnager, On Semi-bent Functions and Related Plateaued Functions Over the Galoia Field $\mathbb{F}_{2^n}$, Open Problems in Mathematics and Computational Science 2014: 243-273.

[19] S. Mesnager, Y. Qi, H. Ru and C. Tang, Minimal Linear Codes From Characteristic Functions, IEEE Trans. Inf. Theory, 2020, 66(9): 5404-5413.

[20] D. Pei, W. Qin, The correlation of a Boolean function with its variables, in INDOCRYPT 2000, Lecture Notes in Computer Science, 2000, 1977: 1-8.

[21] O. Rothaus, On bent functions, Int. J. Combin. Theory, Sreies A, 1976, 20: 300-305.

[22] Z. Sun, L. Hu, Boolean functions with four-valued Walsh spectra, J Syst Sci Complex, 2015, 28(3):743-754.

[23] Z. Tu, D. Zheng, X. Zeng, and L. Hu, Boolean functions with two distinct Walsh coefficients, AAECC, 2011, 22(5-6):359-366.

[24] F. Zhang, C. Carlet, Y. Hu and T. Cao, Secondary constructions of highly nonlinear Boolean functions and disjoint spectra plateaued functions, Inf. Science, 2014, 283(1): 94-106.

[25] Y. Zheng, X. M. Zheng, "Plateaued functions", Advances in Cryptology-ICICS'99, LNCS, Heidelberg, Ed., Springer-Verlag,1999, 1726: 284-300.

[26] X. Zeng, L. Hu, A composition construction of bent-like Boolean functions from quadratic polynomials, available: http://eprint.iacr.org/2003/204.