PAPER

Constructions of Boolean Functions with Five-Valued Walsh Spectra and Their Applications

Yingzhong ZHANG[†,††,†††a)], ***Nonmember***, **Xiaoni DU**[†,†††b)], ***Member***, **Wengang JIN**[††††], ***and*** **Xingbin QIAO**[†,††], ***Nonmembers***

SUMMARY Boolean functions with a few Walsh spectral values have important applications in sequence ciphers and coding theory. In this paper, we first construct a class of Boolean functions with at most five-valued Walsh spectra by using the secondary construction of Boolean functions, in particular, plateaued functions are included. Then, we construct three classes of Boolean functions with five-valued Walsh spectra using Kasami functions and investigate the Walsh spectrum distributions of the new functions. Finally, three classes of minimal linear codes with five-weights are obtained, which can be used to design secret sharing scheme with good access structures.

key words: *Boolean function, bent function, plateaued function, Walsh transform, minimal linear codes*

1. Introduction

Cryptographic functions are important components of cryptographic algorithms, and their cryptographic properties such as balance, nonlinearity, and differential uniformity are related to the security of cryptographic algorithms [1]–[3]. As the most important cryptographic functions, Boolean functions can be used in the design and analysis of symmetric cryptosystems. Some of these criteria can be characterized by the Walsh transform of Boolean functions, which is also a useful tool for studying Boolean functions. Bent functions introduced in [4] by Rothaus, are the maximally nonlinear Boolean functions. Plateaued functions [5] are generalization of bent functions. After that, in 2011 Tu et al. [6] characterized all Boolean functions with exactly two distinct Walsh transform values in terms of their spectrum. Recently, Jin et al. [7] presented three classes of Boolean functions with six-valued Walsh spectra and determined their Walsh spectrum distributions.

Manuscript received May 25, 2023.
Manuscript revised August 30, 2023.
Manuscript publicized October 31, 2023.

[†]The authors are with College of Mathematics and Statistics, Northwest Normal University, Lanzhou, Gansu, 730070, P.R. China.

[††]The authors are also with Gansu Provincial Research Center for Basic Disciplines of Mathematics and Statistics Lanzhou, Gansu 730070, China.

[†††]The author is with Key Laboratory of Cryptography and Data Analytics, Northwest Normal University, Lanzhou, Gansu, 730070, P.R. China.

[††††]The author is with School of Science, National University of Defense Technology, Changsha, Hunan, 710071, P.R. China.

a) E-mail: zhangyingzhongy@163.com

b) E-mail: ymldxn@126.com (Corresponding author)

DOI: 10.1587/transfun.2023EAP1064

Linear codes have wide applications in consumer electronics, communication and data storage system. Besides, linear codes with a few weights have been used in secret sharing scheme [8], [9], authentication codes [10], association schemes [11], and strongly regular graphs [11]. A sufficient condition for judging whether a linear code is minimal was first presented by Ashikhmin and Barg [12], which is called the AB condition. In 2018, Ding et al. [13], [14] derived a necessary and sufficient condition for a linear code to be minimal. Meanwhile they presented some infinite families of minimal linear codes violating the AB condition. Very recently, Bartoli and Bonini [15] provided infinite families of minimal linear codes violating the AB condition for any odd prime p.

The aim of this paper is to construct several classes of Boolean functions with at most five-valued Walsh spectra. More precisely, three classes of new Boolean functions with five-valued Walsh spectra are obtained, and we also investigate their Walsh spectrum distribution. As application, we construct three classes of minimal linear codes with five-weights, and the length, dimension and weight distribution of the codes are determined.

The rest of this paper is organized as follows. Section 2 introduces some notations and preliminary results on Boolean functions. Section 3 constructs a new class of Boolean functions with a few Walsh spectra including plateaued functions. Section 4 proposes three classes of Boolean functions with five-valued Walsh spectra by using Kasami functions and determines their Walsh spectrum distributions. Meanwhile, three classes of minimal codes are derived from the new functions. Section 5 concludes the paper.

2. Preliminaries

In this section, we present some basic notations and facts on Boolean functions, Walsh transform, and minimal linear codes.

Let n be a positive integer. Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements and $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$. An n-variable Boolean function is a mapping from finite field $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$. Denote by $\mathcal{B}_n$ the set of Boolean functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.

Let r be a positive integer with $r \mid n$. The trace function $\mathrm{Tr}_r^n(\cdot)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^r}$ is defined by

$$\mathrm{Tr}_r^n(x) = x + x^{2^r} + \ldots + x^{2^{(n/r-1)r}}, \text{ where } x \in \mathbb{F}_{2^n}.$$

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2$. There is a one-to-one correspondence between $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$, since every $a \in \mathbb{F}_{2^n}$ can be represented uniquely by $a = a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n$, where $a_i \in \mathbb{F}_2$, $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a basis of $\mathbb{F}_2^n$ over $\mathbb{F}_2$.

The Walsh transform of $f \in \mathcal{B}_n$ calculates the correlations between this function and the linear functions, which is defined by

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

If $\hat{f}$ has only t different values, then we say f has t-valued Walsh spectrum. Let

$$N_i = |\{\alpha \in \mathbb{F}_{2^n} : \hat{f}(\alpha) = v_i\}|, 1 \le i \le t,$$

where $|S|$ denotes the cardinality of a set S. Then we have the following system of equations

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

The bivariate representation of a Boolean function $f(x)$ over $\mathbb{F}_{2^n}$ is based on the identification $\mathrm{F}_{2^n} \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^k}$ for $n = m + k$. For the bivariate trace representation over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^k}$, the Walsh transform of $f(y, z)$ at any $(a_1, a_2) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^k}$ is

$$\widehat{f}(a_1, a_2) = \sum_{y\in\mathbb{F}_{2^m}, z\in\mathbb{F}_{2^k}} (-1)^{f(y,z)+\mathrm{Tr}_1^m(a_1y)+\mathrm{Tr}_1^k(a_2z)}.$$

Definition 1: [16] Let $f \in \mathcal{B}_n$ with $n = 2m$ and m be a positive integer. If for any $\alpha \in \mathbb{F}_{2^n}$, $\hat{f}(\alpha) = \pm 2^m$, then $f(x)$ is called bent function.

If $f(x)$ is bent, then its dual function $\widetilde{f}$ is also bent and the relation between them is as follows:

$$\hat{f}(\alpha) = 2^m(-1)^{\tilde{f}(\alpha)}.$$

For even n, a function $f \in \mathcal{B}_n$ is said to be *semi-bent* if $\hat{f}(\omega) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ for all $\omega \in \mathbb{F}_{2^n}$. For odd n, a function $f \in \mathcal{B}_n$ is said to be semi-bent if $\hat{f}(\omega) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ for all $\omega \in \mathbb{F}_{2^n}$. A function $f \in \mathcal{B}_n$ is said to be rth-plateaued if $\hat{f}^2(\omega) \in \{0, 2^{2n-r}\}$. Obviously, bent function is nth-plateaued and semi-bent is $(n-2)$th-plateaued when n is even.

Lemma 1: [17] Let $n = 2m$ and $\lambda \in \mathbb{F}_{2^m}^*$. Then $f(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1})$ is a bent function, and satisfys

$$\hat{f}(a) = 2^m(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})+1}, a \in \mathbb{F}_{2^n}.$$

Lemma 2: [17] Let $n = 2m$ and $\lambda \in \mathbb{F}_{2^m}^*$. Let $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$ such that $a \neq b$ and $\mathrm{Tr}_1^n(\lambda^{-1}b^{2^m}a) = 0$. Then $h(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1}) + \mathrm{Tr}_1^n(ax)\mathrm{Tr}_1^n(bx)$ is bent and its dual h^* is given by

$$\begin{aligned} h^*(x) = &\prod_{t\in\{a,b\}} (\mathrm{Tr}_1^m(\lambda^{-1}t^{2^m+1}) + \mathrm{Tr}_1^n(\lambda^{-1}t^{2^m}u)) \\ &+\mathrm{Tr}_1^m(\lambda^{-1}x^{2^m+1}) + 1. \end{aligned} \tag{3}$$

3. The Construction of New Boolean Functions with a Few Walsh Spectral Values

In this section, we will construct a new class of Boolean functions with a few Walsh spectral values.

Let $\mathfrak{h}(x) = g(x) + \mathfrak{g}(x)$, $g(x), \mathfrak{g}(x) \in \mathcal{B}_n$. For any integer $n, k \ge 2$, we define

$$\mathfrak{f}(x, y) = g(x) + \mathrm{Tr}_1^k(c_1y)\mathrm{Tr}_1^k(c_2y)\mathfrak{g}(x), \tag{4}$$

where $c_1, c_2 \in \mathbb{F}_{2^k}^*$ and $c_1 \neq c_2$.

Now we present the main results of the paper.

Theorem 1: For any $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$, the Walsh transform of $f(x, y)$ in Eq. (4) satisfies

$$\widehat{\mathfrak{f}}(u, v) = \begin{cases} 2^{k-2}(3\widehat{g}(u) + \widehat{\mathfrak{h}}(u)), & v = 0, \\ 2^{k-2}(\widehat{g}(u) - \widehat{\mathfrak{h}}(u)), & v \in \{c_1, c_2\}, \\ -2^{k-2}(\widehat{g}(u) - \widehat{\mathfrak{h}}(u)), & v = c_1 + c_2, \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

Proof: For any $(\varepsilon_1, \varepsilon_2) \in \mathbb{F}_2^2$, we define the sets

$$T(\varepsilon_1, \varepsilon_2) = \{y \in \mathbb{F}_{2^k} : \mathrm{Tr}_1^k(c_1y) = \varepsilon_1, \mathrm{Tr}_1^k(c_2y) = \varepsilon_2\}.$$

It is easy to see that $H = T(0, 0)$ is a subspace of $\mathbb{F}_{2^k}$ with $dim(H) = k-2$, and $H^\perp = \{y \in \mathbb{F}_{2^k} : \forall x \in H, \mathrm{Tr}_1^k(yx) = 0\} = \{0, c_1, c_2, c_1 + c_1\}$. There exists $\alpha_{(\varepsilon_1,\varepsilon_2)} \in T(\varepsilon_1, \varepsilon_2)$ such that $\mathbb{F}_{2^k} = \bigcup_{(\varepsilon_1,\varepsilon_2)\in\mathbb{F}_2^2} (\alpha_{(\varepsilon_1,\varepsilon_2)} + H)$ for any $(\varepsilon_1, \varepsilon_2) \in \mathbb{F}_2^2$. Then for any $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$, we have

$$\begin{aligned} \widehat{\mathfrak{f}}(u, v) &= \sum_{x\in\mathbb{F}_{2^n}, y\in\mathbb{F}_{2^k}} (-1)^{\mathfrak{f}(x,y)+\mathrm{Tr}_1^n(ux)+\mathrm{Tr}_1^k(vy)} \\ &= \sum_{x\in\mathbb{F}_{2^n}, y\in\mathbb{F}_{2^k}} (-1)^{g(x)+\mathrm{Tr}_1^k(c_1y)\mathrm{Tr}_1^k(c_2y)\mathfrak{g}(x)} \\ &\quad \cdot(-1)^{\mathrm{Tr}_1^n(ux)+\mathrm{Tr}_1^k(vy)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} \sum_{(\varepsilon_1,\varepsilon_2)\in\mathbb{F}_2^2} \sum_{y\in\alpha_{(\varepsilon_1,\varepsilon_2)}+H} (-1)^{g(x)} \\ &\quad \cdot(-1)^{\varepsilon_1\varepsilon_2\mathfrak{g}(x)+\mathrm{Tr}_1^n(ux)+\mathrm{Tr}_1^k(vy)} \\ &= \widehat{\mathfrak{h}}(u) \sum_{y\in\alpha_{(1,1)}+H} (-1)^{\mathrm{Tr}_1^k(vy)} \\ &\quad +\hat{g}(u) \sum_{(\varepsilon_1,\varepsilon_2)\in\mathbb{F}_2^2\setminus(1,1)} \sum_{y\in\alpha_{(\varepsilon_1,\varepsilon_2)}+H} (-1)^{\mathrm{Tr}_1^k(vy)} \\ &= \begin{cases} 2^{k-2}(3\widehat{g}(u) + \widehat{\mathfrak{h}}(u)), & v = 0, \\ 2^{k-2}(\widehat{g}(u) - \widehat{\mathfrak{h}}(u)), & v \in \{c_1, c_2\}, \\ 2^{k-2}(\widehat{\mathfrak{h}}(u) - \widehat{g}(u)), & v = c_1 + c_2, \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{6}$$

Thus, we complete the proof. □

Corollary 1: Let $g(x)$ be bent, and $\mathfrak{g}(x) = 1$. Then $\mathfrak{f}(x, y)$ in Eq. (4) is $(k-2)$th-plateaued, and $\widehat{\mathfrak{f}}(u, v) \in \{0, \pm 2^{\frac{n+2k-2}{2}}\}$. In particular, if $k = 2$, then $\mathfrak{f}(x, y)$ is bent, and if $k = 3$ or 4, then $\mathfrak{f}(x, y)$ is semi-bent.

4. Construction of the Five-Valued Walsh Spectra Boolean Function and Its Application

In this section, based on the functions in Sect. 3, we will construct three classes five-valued Walsh spectra Boolean functions by using Kasami function and determine the Walsh spectrum distributions, then investigate the applications in linear codes.

Below, we always put $n = 2m > 4$, $g(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1})$, where $\lambda \in \mathbb{F}_{2^m}^*$. We introduce the following notations for clarity.

$$\begin{aligned} A &= \mathrm{Tr}_1^m(\lambda^{-1}u^{2^m+1}), \text{ for any } u \in \mathbb{F}_{2^n},\\ N_1 &= |\{(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k} : \widehat{\mathfrak{f}}(u,v) = 0\}|,\\ N_{2+i} &= |\{(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k} : \widehat{\mathfrak{f}}(u,v) = (-1)^i 2^{\frac{n}{2}+k-1}\}|,\\ N_{4+i} &= |\{(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k} : \widehat{\mathfrak{f}}(u,v) = (-1)^{i+1} 2^{\frac{n}{2}+k}\}|, \end{aligned}$$

where $i \in \{0,1\}$.

According to Lemma 1, it is easy to get

$$\sum_{u\in\mathbb{F}_{2^n}} (-1)^A = 2^{\frac{n}{2}}(-1)^{\mathrm{Tr}_1^m(\lambda 0^{2^m+1})+1} = -2^{\frac{n}{2}}. \tag{7}$$

4.1 The Spectrum Distributions for $\mathfrak{g}(x) = \mathrm{Tr}_1^m(rx^{2^m+1})$

In this subsection, let $\mathfrak{g}(x) = \mathrm{Tr}_1^m(rx^{2^m+1})$, $r \in \mathbb{F}_{2^m}^*$ in Eq. (4). Then

$$\begin{aligned} \mathfrak{f}(x,y) &= \mathrm{Tr}_1^k(c_1y)\mathrm{Tr}_1^k(c_2y)\mathrm{Tr}_1^m(rx^{2^m+1})\\ &\quad +\mathrm{Tr}_1^m(\lambda x^{2^m+1}), \end{aligned} \tag{8}$$

where $\lambda \neq r$, $c_1, c_2 \in \mathbb{F}_{2^k}^*$ and $c_1 \neq c_2$.

For this function we have the following lemma which will be used in the sequel.

Lemma 3: For any $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$, the Walsh transform of $\mathfrak{f}(x,y)$ in Eq. (8) is as following

$\widehat{\mathfrak{f}}(u,v) =$

$$\begin{cases} -2^{\frac{n}{2}+k-2}(3(-1)^A + (-1)^B), & v = 0,\\ -2^{\frac{n}{2}+k-2}((-1)^A - (-1)^B), & v \in \{c_1, c_2\},\\ 2^{\frac{n}{2}+k-2}((-1)^A - (-1)^B), & v = c_1 + c_2,\\ 0, & \text{otherwise.} \end{cases} \tag{9}$$

where $B = \mathrm{Tr}_1^m((r+\lambda)^{-1}u^{2^m+1})$.

Theorem 2: With the notations above. The Walsh spectrum distribution of $\mathfrak{f}(x,y)$ in Eq. (8) satisfies

$\widehat{\mathfrak{f}}(u,v) =$

$$\begin{cases} 0, & 2^{n+k} - 5\cdot 2^{n-1} - 3\cdot 2^{\frac{n}{2}-1}\text{times},\\ -2^{\frac{n}{2}+k}, & 2^{n-2} - 3\cdot 2^{\frac{n}{2}-2} \text{ times},\\ 2^{\frac{n}{2}+k}, & 2^{n-2} + 2^{\frac{n}{2}-2} \text{ times},\\ \pm 2^{\frac{n}{2}+k-1}, & 2^n + 2^{\frac{n}{2}} \text{ times}. \end{cases} \tag{10}$$

Proof: By Lemma 3, we discuss the Walsh transform of function $\mathfrak{f}(x,y)$ in two cases:

(1) If $A = B$, then

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} (-1)^{A+1}2^{\frac{n}{2}+k}, & v = 0,\\ 0, & \text{otherwise.} \end{cases}$$

(2) If $A \neq B$, then

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} (-1)^{A+1}2^{\frac{n}{2}+k-1}, & v \in \{0, c_1, c_2\},\\ (-1)^A 2^{\frac{n}{2}+k-1}, & v = c_1 + c_2,\\ 0, & \text{otherwise.} \end{cases}$$

Now we discuss the Walsh spectrum distribution of $\mathfrak{f}(x,y)$. We first consider N_4, the number of $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$ such that $\widehat{\mathfrak{f}}(u,v) = -2^{\frac{n}{2}+k}$, and this will happen if $v = 0$ and $A = B = 0$. So we have

$$N_4 = \frac{1}{2^2}\sum_{u\in\mathbb{F}_{2^n}} (1+(-1)^A)(1+(-1)^B).$$

Since it follows from Lemma 1 and Eq. (7) that $\sum_{u\in\mathbb{F}_{2^n}} (-1)^B = \sum_{u\in\mathbb{F}_{2^n}} (-1)^{A+B} = -2^{\frac{n}{2}}$, we can get

$$N_4 = \frac{1}{2^2}(2^n - 2^{\frac{n}{2}} - 2^{\frac{n}{2}} - 2^{\frac{n}{2}}) = 2^{n-2} - 3\cdot 2^{\frac{n}{2}-2}.$$

Next, we will calculate N_5, which corresponding to $v = 0$ and $A = B = 1$. Then

$$\begin{aligned} N_5 &= \frac{1}{2^2}\sum_{u\in\mathbb{F}_{2^n}} (1-(-1)^A)(1-(-1)^B)\\ &= 2^{n-2} + 2^{\frac{n}{2}-2}. \end{aligned}$$

Since $\mathfrak{f}(0,0) = 0$, then by applying the value of N_4 and N_5 to Eq. (2), and solving the system of linear equations yields that

$$\begin{cases} N_1 = 2^{n+k} - 5\cdot 2^{n-1} - 3\cdot 2^{\frac{n}{2}},\\ N_2 = N_3 = 2^{\frac{n}{2}} + 2^n. \end{cases}$$

Therefore, we have completed the proof. □

Example 1: Let $n = 8$, $k = 2$, and ζ be a primitive element in $\mathbb{F}_{2^8}$ such that $\zeta^8 + \zeta^6 + \zeta^5 + \zeta + 1 = 0$. Let $c_1 = 1$, $c_2 = \zeta^{85}$, $\lambda = \zeta^{17}$, $r = \zeta^{34}$. It was verified by a Magma program that

$$\mathfrak{f}(x,y) = \mathrm{Tr}_1^4(\lambda x^{17}) + \mathrm{Tr}_1^2(c_1y)\mathrm{Tr}_1^2(c_2y)\mathrm{Tr}_1^4(rx^{17})$$

has the Walsh spectrum distribution as following

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} 0, & 2^{10} - 83\cdot 2^3 \text{ times},\\ -2^6, & 2^6 - 3\cdot 2^2 \text{ times},\\ 2^6, & 2^6 + 2^2 \text{ times},\\ \pm 2^5, & 2^8 + 2^4 \text{ times}, \end{cases}$$

which is consistent with Theorem 2.

4.2 The Spectrum Distributions for $\mathfrak{g}(x) = \mathrm{Tr}_1^n(ax)$

In this subsection, let $\mathfrak{g}(x) = \mathrm{Tr}_1^n(ax)$ in Eq. (4). Then

$$\begin{aligned} \mathfrak{f}(x,y) &= \mathrm{Tr}_1^k(c_1y)\mathrm{Tr}_1^k(c_2y)\mathrm{Tr}_1^n(ax)\\ &\quad +\mathrm{Tr}_1^m(\lambda x^{2^m+1}), \end{aligned} \tag{11}$$

where $a \in \mathbb{F}_{2^n}^*$, $c_1, c_2 \in \mathbb{F}_{2^k}^*$ and $c_1 \neq c_2$.

By Theorem 1, the following lemma is obtained.

Lemma 4: For any $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$, the Walsh transform of $\mathfrak{f}(x, y)$ in Eq. (11) is as following

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} -2^{\frac{n}{2}+k-2}(3(-1)^A + (-1)^B), & v = 0, \\ -2^{\frac{n}{2}+k-2}((-1)^A - (-1)^B), & v \in \{c_1, c_2\}, \\ 2^{\frac{n}{2}+k-2}((-1)^A - (-1)^B), & v = c_1 + c_2, \\ 0, & \text{otherwise.} \end{cases}$$

where $B = \mathrm{Tr}_1^m(\lambda^{-1}(u + a)^{2^m+1})$.

Theorem 3: The Walsh spectrum distribution of $\mathfrak{f}(x, y)$ in Eq. (11) is as following

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} 0, & 2^{n+k} - 5 \cdot 2^{n-1} \text{ times}, \\ \pm 2^{\frac{n}{2}+k}, & 2^{n-2} \pm 2^{\frac{n}{2}-1} \text{ times}, \\ \pm 2^{\frac{n}{2}+k-1}, & 2^n \text{ times}. \end{cases} \tag{12}$$

Proof: The proof is similar to that of Theorem 2, so we only give a sketch. By Lemma 4, for any $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$, we have

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} (-1)^{A+1}2^{\frac{n}{2}+k}, & A = B,\ v = 0, \\ (-1)^{A+1}2^{\frac{n}{2}+k-1}, & A \neq B, v \in \{0, c_1, c_2\}, \\ (-1)^A 2^{\frac{n}{2}+k-1}, & A \neq B,\ v = c_1 + c_2, \\ 0, & \text{otherwise.} \end{cases}$$

Now we discuss the Walsh spectrum distribution of $\mathfrak{f}(x, y)$. We first consider N_4, the number of $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$ such that $\widehat{\mathfrak{f}}(u, v) = -2^{\frac{n}{2}+k}$. It follows from the equation above and Lemma 1 that

$$\begin{aligned} N_4 &= \frac{1}{2^2} \sum_{u \in \mathbb{F}_{2^n}} (1 + (-1)^A)(1 + (-1)^B) \\ &= \frac{1}{2^2} \sum_{u \in \mathbb{F}_{2^n}} (1 + (-1)^A + (-1)^B + (-1)^{A+B}) \\ &= \frac{1}{2^2}(2^n - 2^{\frac{n}{2}} - 2^{\frac{n}{2}} - 0) \\ &= 2^{n-2} - 2^{\frac{n}{2}-1}. \end{aligned}$$

Next, we examine N_5, which correspond to the case of $v = 0$ and $A = B = 1$. Then with the similar calculation of N_4, we get

$$N_5 = 2^{n-2} + 2^{\frac{n}{2}-1}.$$

Using the same argument as in the proof of Theorem 2, we obtain

$$\begin{cases} N_1 = 2^{n+k} - 5 \cdot 2^{n-1}, \\ N_2 = N_3 = 2^n. \end{cases}$$

Therefore, the spectrum distribution of $\mathfrak{f}(x, y)$ is

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} 0, & 2^{n+k} - 5 \cdot 2^{n-1} \text{ times}, \\ \pm 2^{\frac{n}{2}+k}, & 2^{n-2} \pm 2^{\frac{n}{2}-1} \text{ times}, \\ \pm 2^{\frac{n}{2}+k-1}, & 2^n \text{ times}. \end{cases}$$

This completes the proof. □

Example 2: Let $n = 8$, $k = 2$, and ζ be a primitive element in $\mathbb{F}_{2^8}$ such that $\zeta^8 + \zeta^6 + \zeta^5 + \zeta + 1 = 0$. Let $c_1 = 1$, $c_2 = \zeta^{85}$, $\lambda = \zeta^{17}$, $a = \zeta^2$. It was verified by a Magma program that

$$\mathfrak{f}(x, y) = \mathrm{Tr}_1^4(\lambda x^{17}) + \mathrm{Tr}_1^2(c_1 y)\mathrm{Tr}_1^2(c_2 y)\mathrm{Tr}_1^8(ax)$$

has the Walsh spectrum distribution as follows

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} 0, & 2^{10} - 5 \cdot 2^7 \text{ times}, \\ \pm 2^6, & 2^6 \pm 2^3 \text{ times}, \\ \pm 2^5, & 2^8 \text{ times}. \end{cases}$$

This is consistent with Theorem 3.

4.3 The Spectrum Distributions for $\mathfrak{g}(x) = \mathrm{Tr}_1^n(ax)\mathrm{Tr}_1^n(bx)$

In this subsection, let $\mathfrak{g}(x) = \mathrm{Tr}_1^n(ax)\mathrm{Tr}_1^n(bx)$, $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$ such that $a \neq b$ in Eq. (4). Then

$$\begin{aligned} \mathfrak{f}(x, y) = \ & \mathrm{Tr}_1^k(c_1 y)\mathrm{Tr}_1^k(c_2 y)\mathrm{Tr}_1^n(ax)\mathrm{Tr}_1^n(bx) \\ & + \mathrm{Tr}_1^m(\lambda x^{2^m+1}), \end{aligned} \tag{13}$$

where $r \in \mathbb{F}_{2^m}^*$, and $\mathrm{Tr}_1^n(\lambda^{-1}b^{2^m}a) = 0$, $c_1, c_2 \in \mathbb{F}_{2^k}^*$ and $c_1 \neq c_2$.

By Theorem 1, we have the following result.

Lemma 5: Let $\mathfrak{f}(x, y)$ be defined as in Eq. (13). For any $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$, the Walsh transform of $\mathfrak{f}(x, y)$ is as following

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} 2^{\frac{n}{2}+k-2}(-1)^{A+1}(3 + (-1)^\Gamma), & v = 0, \\ 2^{\frac{n}{2}+k-2}((-1)^{A+1} - (-1)^\Gamma), & v \in \{c_1, c_2\}, \\ 2^{\frac{n}{2}+k-2}(-1)^A(1 - (-1)^\Gamma), & v = c_1 + c_2, \\ 0, & \text{otherwise.} \end{cases}$$

where $\Gamma = \prod_{t \in \{a,b\}} (\mathrm{Tr}_1^m(\lambda^{-1}t^{2^m+1}) + \mathrm{Tr}_1^n(\lambda^{-1}t^{2^m}u))$.

Theorem 4: The Walsh spectrum distribution of $\mathfrak{f}(x, y)$ defined by Eq. (13) is as following

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} 0, & 2^{n+k} - 7 \cdot 2^{n-2} \text{ times}, \\ \pm 2^{\frac{n}{2}+k}, & 3 \cdot 2^{n-3} \pm 2^{\frac{n}{2}-1} \text{ times}, \\ \pm 2^{\frac{n}{2}+k-1}, & 2^{n-1} \text{ times}. \end{cases}$$

Proof: The proof is similar to that of Theorem 2, so we give a brief proof. By Lemma 5, for any $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$, we have

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} (-1)^{A+1}2^{\frac{n}{2}+k}, & \Gamma = 0, v = 0, \\ (-1)^{A+1}2^{\frac{n}{2}+k-1}, & \Gamma = 1, v \in \{0, c_1, c_2\}, \\ (-1)^A 2^{\frac{n}{2}+k-1}, & \Gamma = 1, v = c_1 + c_2, \\ 0, & \text{otherwise.} \end{cases}$$

Now we discuss the Walsh spectrum distribution of $\mathfrak{f}(x, y)$. Let

$$\begin{aligned} \Gamma_0 &= \mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1}) + \mathrm{Tr}_1^n(\lambda^{-1}a^{2^m}u), \\ \Gamma_1 &= \mathrm{Tr}_1^m(\lambda^{-1}b^{2^m+1}) + \mathrm{Tr}_1^n(\lambda^{-1}b^{2^m}u). \end{aligned}$$

First, considering N_4, the number of $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$ such that $\widehat{\mathfrak{f}}(u,v) = -2^{\frac{n}{2}+k}$, which correspond to $v = 0$ and $A = \Gamma = 0$. It is obvious that $(\Gamma_0, \Gamma_1) \in \{(0,0),(0,1),(1,0)\}$ when $\Gamma = 0$. Let N_{4j} be the number of $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$ such that $\widehat{\mathfrak{f}}(u,v) = -2^{\frac{n}{2}+k}$ when $(\Gamma_0, \Gamma_1) = (j_0, j_1)$, where $0 \le j \le 2$ and $j = 2j_0 + j_1$. Then

$$N_4 = N_{40} + N_{41} + N_{42}.$$

Next, we calculate N_{40}, N_{41}, N_{42}.

$$\begin{aligned} N_{40} &= \frac{1}{2^3} \sum_{u \in \mathbb{F}_{2^n}} (1+(-1)^A)(1+(-1)^{\Gamma_0})(1+(-1)^{\Gamma_1}) \\ &= \frac{1}{2^3} \sum_{u \in \mathbb{F}_{2^n}} (1+(-1)^{\Gamma_0}+(-1)^{\Gamma_1} \\ &\quad +(-1)^A + (-1)^{A+\Gamma_0} + (-1)^{\Gamma_0+\Gamma_1} \\ &\quad +(-1)^{A+\Gamma_1} + (-1)^{A+\Gamma_0+\Gamma_1}). \end{aligned} \tag{14}$$

Due to the definition of Γ_0, Γ_1 and $a \neq b$, we can get

$$\sum_{u \in \mathbb{F}_{2^n}} (-1)^{\Gamma_0} = \sum_{u \in \mathbb{F}_{2^n}} (-1)^{\Gamma_1} = \sum_{u \in \mathbb{F}_{2^n}} (-1)^{\Gamma_0+\Gamma_1} = 0.$$

By Lemma 1, we have $\sum_{u \in \mathbb{F}_{2^n}} (-1)^{A+\Gamma_i} = -2^{\frac{n}{2}}$, $i = 0, 1$.

Notice that $\mathrm{Tr}_1^n(\lambda^{-1}b^{2^m}a) = \mathrm{Tr}_1^n(\lambda^{-1}(b^{2^m}a + a^{2^m}b)) = 0$. For convenience, let $A_a = \mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})$. Then

$$\begin{aligned} &\sum_{u \in \mathbb{F}_{2^n}} (-1)^{A+\Gamma_0+\Gamma_1} \\ &= \sum_{u \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\lambda^{-1}u^{2^m+1})} \\ &\quad \cdot (-1)^{\mathrm{Tr}_1^n(\lambda^{-1}(a+b)^{2^m}u)+A_a+A_b} \\ &= (-1)^{A_a+A_b} 2^{\frac{n}{2}} (-1)^{\mathrm{Tr}_1^n(\lambda(\lambda^{-1}(a+b)^{2^m})^{2^m+1})+1} \\ &= 2^{\frac{n}{2}} (-1)^{2(A_a+A_b)+1} \\ &= -2^{\frac{n}{2}}. \end{aligned}$$

Taking the above results into Eq. (14) yields

$$N_{40} = 2^{n-3} - 2^{\frac{n}{2}-1}.$$

Similarly, $N_{41} = N_{42} = 2^{n-3}$. In summary, it can be seen that

$$N_4 = 3 \cdot 2^{n-3} - 2^{\frac{n}{2}-1}.$$

Secondly, considering N_5, the number of $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$ such that $\widehat{\mathfrak{f}}(u,v) = 2^{\frac{n}{2}+k}$ where $v = 0$ and $(A,\Gamma) = (1,0)$. With the same discussion as that for N_4, we have

$$N_5 = 3 \cdot 2^{n-3} + 2^{\frac{n}{2}-1}.$$

Using the same argument as in the proof of Theorem 2, we obtain

$$\begin{cases} N_1 = 2^{n+k} - 7 \cdot 2^{n-2}, \\ N_2 = N_3 = 2^{n-1}. \end{cases}$$

This completes the proof. □

Example 3: Let $n = 6$, $k = 2$, and ζ be a primitive element in $\mathbb{F}_{2^6}$ such that $\zeta^6 + \zeta^4 + \zeta^3 + \zeta + 1 = 0$. Let $c_1 = 1$, $c_2 = \zeta^9$, $\lambda = \zeta^{54}$, $a = \zeta^3, b = \zeta^2$. Then $\mathrm{Tr}_1^6(\lambda^{-1}b^8a) = 0$. It was verified by a Magma program that

$$\mathfrak{f}(x,y) = \mathrm{Tr}_1^3(\lambda x^9) + \mathrm{Tr}_1^2(c_1 y)\mathrm{Tr}_1^2(c_2 y)\mathrm{Tr}_1^6(ax)\mathrm{Tr}_1^6(bx)$$

has the Walsh spectrum distribution as following

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} 0, & 2^4 \cdot 9 \text{ times}, \\ -2^5, & 2^2 \cdot 5 \text{ times}, \\ 2^5, & 2^2 \cdot 7 \text{ times}, \\ \pm 2^4, & 2^5 \text{ times}, \end{cases}$$

which is consistent with Theorem 4.

Remark 1: It is easy to see that the Walsh spectrum distribution of the functions constructed in Eqs. (8), (11) and (13) are different from known functions etc., see for example [18], [19]. Therefore the Boolean functions with five-valued Walsh spectra in this paper are new.

4.4 Application of the New Functions in Linear Codes

The main object of this subsection is to design three classes of minimal linear codes from the constructed functions.

Let $f(x) \in \mathcal{B}_n$ with $f(0) = 0$. For all $v \in \mathbb{F}_{2^n}$, $f(x) \neq v \cdot x$, then the linear code $\mathcal{C}_f \in \mathbb{F}_2$ is defined by

$$\mathcal{C}_f = \{(uf(x) + \mathrm{Tr}(v \cdot x))_{x \in \mathbb{F}_{2^n}^*} : u \in \mathbb{F}_2,\ v \in \mathbb{F}_{2^n}\}. \tag{15}$$

The lemma below called AB condition is use to determine a linear code being minimal.

Lemma 6: [12] Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$, and w_{min} and w_{max} denote the minimum and maximum nonzero Hamming weights in $\mathcal{C}$, respectively. If

$$w_{min}/w_{max} > q - 1/q, \tag{16}$$

then $\mathcal{C}$ is minimal.

We will say that a binary linear code is narrow if it satisfies the condition of Lemma 6, namely, $w_{min}/w_{max} > 1/2$. Otherwise, a binary linear code is called wide.

Lemma 7: [13] The binary code $\mathcal{C}_f$ in Eq. (15) has length $2^n - 1$ and dimension $n + 1$. In addition, the weight distribution of $\mathcal{C}_f$ is given by the following multiset:

$$\{\{\frac{2^n - \hat{f}(\omega)}{2} : \omega \in \mathbb{F}_{2^n}\} \cup \{2^{n-1} : \omega \in \mathbb{F}_{2^n}^*\} \cup \{0\}\}.$$

Theorem 5: With the notations above. The binary codes $\mathcal{C}_f$ from $\mathfrak{f}(x,y)$ in Eqs. (8), (11) and (13) have length 2^{n+k-1}, dimension $n + k + 1$, and minimum weight $2^{n+k-1} - 2^{m+k-1}$. Furthermore, $\mathcal{C}_f$ are minimal and the weight distributions of $\mathcal{C}_f$ are given by Table 1,

(1) where $A_1 = -5 \cdot 2^{n-1} - 3 \cdot 2^{m-1} + 2^{n+k+1} - 1, A_2 = 2^{n-2} - 3 \cdot 2^{m-2}, A_3 = 2^{n-2} + 2^{m-2}, A_4 = 2^n + 2^m$, if $\mathfrak{f}(x,y)$ is defined by Eq. (8).

Table 1 The weight distribution of $\mathcal{C}_f$.

Weight	Multiplicity
0	1
2^{n+k-1}	A_1
$2^{n+k-1}+2^{m+k-1}$	A_2
$2^{n+k-1}-2^{m+k-1}$	A_3
$2^{n+k-1}\pm 2^{m+k-2}$	A_4

(2) where $A_1 = -5\cdot 2^{n-1}+2^{n+k+1}-1, A_2 = 2^{n-2}-2^{m-1}, A_3 = 2^{n-2}+2^{m-1}, A_4 = 2^n$, if $\mathfrak{f}(x,y)$ is defined by Eq. (11).

(3) where $A_1 = -7\cdot 2^{n-2}+2^{n+k+1}-1, A_2 = 3\cdot 2^{n-3}-2^{m-1}, A_3 = 3\cdot 2^{n-3}+2^{m-1}, A_4 = 2^{n-1}$, if $\mathfrak{f}(x,y)$ is defined by Eq. (13).

Proof: According to Theorems 2–4 and Lemma 7, we have the weight distribution of $\mathcal{C}_f$ is in Table 1. Obviously, $w_{\min}/w_{\max} > 1/2$. Thus, $\mathcal{C}_f$ satisfies AB condition according to Lemma 6, that is, $\mathcal{C}_f$ is narrow minimal. □

5. Conclusion

In this paper, a family of Boolean functions with a few Walsh spectrum was promoted. Moreover, we constructed three classes of Boolean functions with five-valued Walsh spectra and investigated the distributions of Walsh spectrum. As application, three classes of minimal linear codes with five-weights were obtained from the new functions, and the length, dimension and weight distribution were determined. The results show that the new codes are all minimal and thus they can be used to design the secret sharing scheme with sound access structures.

References

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," J. Cryptol., vol.4, no.1, pp.3–72, 1991.
[2] M. Matsui, "Linear cryptanalysis method for DES cipher," Proc. Eurocrypt'93 Advances in Cryptology, Berlin, Heidelberg, pp.386–397, 1993.
[3] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," IEEE Trans. Comput., vol.34, no.1, pp.81–85, 2006.
[4] O. Rothaus, "On "bent" functions," Journal of Combinatorial Theory, Ser. A, vol.A20, no.3, pp.300–305, 1976.
[5] Y. Zheng and X. Zheng, "Plateaued functions," IEEE Trans. Inf. Theory, vol.41, no.3, pp.1215–1223, 2001.
[6] Z. Tu, D. Zheng, X. Zeng, and L. Hu, "Boolean functions with two distinct Walsh coefficients," Applicable Algebra in Engineering Communication and Computing, vol.22, no.5-6, pp.359–366, 2011.
[7] W. Jin, X. Du, Y. Sun, and C. Fan, "Boolean functions with six-valued Walsh spectra and their application," Cryptogr. Commun., vol.13, pp.393–405, 2021.
[8] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," IEEE Trans. Inf. Theory, vol.51, no.6, pp.2089–2102, 2005.
[9] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," IEEE Trans. Inf. Theory, vol.52, no.1, pp.206–212, 2006.
[10] C. Ding and X. Wang, "A coding theory construction of new systematic authentication codes," Theoretical Computer Science, vol.330, no.1, pp.81–99, 2005.
[11] A.R. Calderbank and J.M. Goethals, "Three-weight codes and association schemes," Philips J. Res., vol.39, pp.143–152, 1984.
[12] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes," IEEE Trans. Inf. Theory, vol.44, no.5, pp.2010–2017, 1998.
[13] C. Ding, Z. Heng, and Z. Zhou, "Minimal binary linear codes," IEEE Trans. Inf. Theory, vol.64, no.10, pp.6536–6545, 2018.
[14] Z. Heng, C. Ding, and Z. Zhou, "Minimal linear codes over finite fields," Finite Fields and Their Applications, vol.54, pp.176–196, 2018.
[15] D. Bartoli and M. Bonini, "Minimal linear codes in odd characteristic," IEEE Trans. Inf. Theory, vol.65, no.7, pp.4152–4155, 2019.
[16] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, Bent functions and permutations suitable for DES-like cryptosystems," Designs, Codes and Cryptography, vol.15, no.2, pp.125–156, 1998.
[17] S. Mesnager, "Several new infinite families of bent functions and their duals," IEEE Trans. Inf. Theory, vol.60, no.7, pp.4397–4407, 2014.
[18] S. Hodžić, E. Pasalic, and W. Zhang, "Generic constructions of five-valued spectra Boolean functions," IEEE Trans. Inf. Theory, vol.65, no.11, pp.7554–7565, Nov. 2019.
[19] X. Cao and L. Hu, "Two Boolean functions with five-valued Walsh spectra and high nonlinearity," International Journal of Foundations of Computer Science, vol.26, no.05, pp.537–556, 2015.

Yingzhong Zhang is currently a graduate student at Northwest Normal University. Her research interests include coding theory, cryptography and information security.

Xiaoni Du received PhD from Xidian University, China in 2008. Since 2011, she has been a professor in the College of Mathematics and Statistics, Northwest Normal University. Her research interests include coding theory, cryptography and information security. She is a member of IEICE.

Wengang Jin received PhD from School of Mathematics and Statistics of Northwest Normal University, China in 2022. He is currently a doctoral candidate at National University of Defense Technology. His research interests include coding theory, cryptography and information security.

Xingbin Qiao received the M.S. degree from School of Mathematics and Statistics of Northwest Normal University, China in 2022. He is currently a doctoral candidate at Northwest Normal University. His research interests include coding theory, cryptography and information security.