Wuhan University Journal of Natural Sciences

2021, Vol.26 No.6, 453-458

Article ID 1007-1202(2021)06-0453-06

DOI https://doi.org/10.1051/wujns/2021266453

The Walsh Transform of a Class of Boolean Functions

□ JIANG Niu[1], ZHUO Zepeng[1,2], CHEN Guolong[1,3†], WANG Liting[1]

1. School of Mathematical Sciences, Huaibei Normal University, Huaibei 235000, Anhui, China;

2. School of Cyber Science, University of Science and Technology of China, Hefei 230027, Anhui, China;

3. School of Computer Engineering, Bengbu University, Bengbu 233030, Anhui, China

Abstract: The Walsh transform is an important tool to investigate cryptographic properties of Boolean functions. This paper is devoted to study the Walsh transform of a class of Boolean functions defined as $g(x)=f(x)\mathrm{Tr}_1^n(x)+h(x)\mathrm{Tr}_1^n(\delta x)$, by making use of the known conclusions of Walsh transform and the properties of trace function, and the conclusion is obtained by generalizing an existing result.

Key words: Boolean function; Walsh transform; trace function

CLC number: O 29

Received date: 2021-08-04

Foundation item: Supported by the Natural Science Foundation of Anhui Higher Education Institutions of China (KJ2020ZD008), Key Research and Development Projects in Anhui Province (202004a05020043) and the Graduate Innovation Fund of Huaibei Normal University (yx2021022)

Biography: JIANG Niu, female, Master candidate, research direction: cryptography. E-mail: 1401471403@qq.com

† To whom correspondence should be addressed. E-mail: cglbox@sina.com

0 Introduction

Boolean functions are important objects in discrete mathematics. They play a role in symmetric cryptography and error-correcting coding theory, and they also have a significant influence on the design and analysis of cryptographic algorithms. The Walsh transform is a vital tool to investigate cryptographic properties of Boolean functions. Some important properties of cryptographic functions, such as resiliency and nonlinearity can be characterized by their Walsh transform[1-3]. An interesting problem is to find Boolean functions with few Walsh transform values and determine their distributions.

Bent functions introduced by Rothaus[4] in 1976 are interesting combinatorial objects with maximum Hamming distance to the set of all affine functions, but they cannot be used in cryptography directly since they exist only in an even number of variables and are not be balanced. Such functions have been extensively studied because of their important applications in coding theory[5,6], cryptography[7], and sequence designs[8]. To get balanced functions with high nonlinearity in odd or even number of variable, Carlet[9] generalized the bent functions to plateaued functions and they take Walsh transform values 0, $\pm 2^k$ for a fixed positive integer k. Semi-bent, as a particular case, is an important kind of Boolean functions with three Walsh transform values. In Ref. [10], 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 this work, recently Jin *et al*[11] presented three classes of Boolean functions with six-valued Walsh spectra, which were derived from bent functions by complementing their values at the zero and another two nonzero points, and determined their Walsh spectrum distributions with a similar method. In Ref. [12], some classes of Boolean functions with five Walsh transform values were presented by adding the product of two or three linear functions into some known bent functions, and their Walsh spectrum distributions were determined finally. In Ref. [13], Tang *et al* gave a generic construction of bent functions defined as

$$f(x)=g(x)+F(\mathrm{Tr}_1^n(u_1x),\mathrm{Tr}_1^n(u_2x),\cdots,\mathrm{Tr}_1^n(u_\tau x)),$$

where $n=2m$, $g(x)$ is any known bent function over F_{2^n} satisfying some conditions, $F(X_1,X_2,\cdots,X_\tau)$ is an arbitrary polynomial in $F_2[X_1,X_2,\cdots,X_\tau]$. In particular, the cases of $F(X_1,X_2,X_3)=X_1X_2X_3$ and $F(X_1,X_2)=X_1X_2$ have been studied by Xu *et al*[12] and Mesnager[14], respectively. The purpose of this paper is to present the Walsh transform of the Boolean function defined as

$$g(x)=f(x)\mathrm{Tr}_1^n(x)+h(x)\mathrm{Tr}_1^n(\delta x) \tag{1}$$

where $f(x)$ and $h(x)$ are Boolean functions over F_{2^n} and $\delta\in F_{2^n}$. In particular, the case of

$$g(x)=f(x)\mathrm{Tr}_1^n(x)+(f(x)+1)\mathrm{Tr}_1^n(\delta x) \tag{2}$$

has been studied by Pang *et al*[15].

This paper is organized as follows. In Section 1, we give some basic concepts and results. In Section 2, we present the Walsh transform of the Eq. (1). In Section 3, we conclude this paper.

1 Preliminaries

Let F_2^n denote the n-dimensional vector space over F_2, and F_{2^n} denote the finite field with 2^n elements. For any set E, $E^*=E\setminus\{0\}$. By viewing each $x=x_1\xi_1+x_2\xi_2+\cdots+x_n\xi_n\in F_{2^n}$ as a vector $(x_1,x_2,\cdots,x_n)\in F_2^n$ where $\{\xi_1,\xi_2,\cdots,\xi_n\}$ is a basis of F_{2^n} over F_2, we identify F_2^n with F_{2^n} and then every function $f:F_{2^n}\to F_2$ is equivalent to a Boolean function. For $x,y\in F_{2^n}$, the inner product is defined as $x\cdot y=\mathrm{Tr}_1^n(xy)$.

For any positive integer $k\mid n$, the trace function from F_{2^n} to F_{2^k} is the mapping defined as

$$\mathrm{Tr}_k^n(x)=\sum_{i=0}^{\frac{n}{k}-1}x^{2^{ik}}=x+x^{2^k}+x^{2^{2k}}+\cdots+x^{2^{n-1}},\quad x\in F_{2^n}$$

When $k=1$,

$$\mathrm{Tr}_1^n(x)=\sum_{i=0}^{n-1}x^{2^i}=x+x^2+x^{2^2}+\cdots+x^{2^{n-1}}$$

is called the absolute trace function.

Some important and useful properties of the trace function are provided in the following:

1) $\mathrm{Tr}_1^n(ax+by)=a\mathrm{Tr}_1^n(x)+b\mathrm{Tr}_1^n(y)$, $\forall\, x,y\in F_{2^n}$ and $a,b\in F_2$.

2) $\mathrm{Tr}_1^n(x^2)=\mathrm{Tr}_1^n(x)$ for any $x\in F_{2^n}$.

3) For any $\alpha\in F_{2^n}$, $\sum_{x\in F_{2^n}}(-1)^{\mathrm{Tr}_1^n(\alpha x)}=0$ if $\alpha\neq 0$.

4) When $F_2\subset F_{2^m}\subset F_{2^n}$, the trace function $\mathrm{Tr}_1^n(\alpha)$ satisfies the transitivity property, that is, $\mathrm{Tr}_1^n(\alpha)=\mathrm{Tr}_1^m(\mathrm{Tr}_m^n(\alpha))$.

5) For any $\alpha\in F_{2^n}$, $(\mathrm{Tr}_1^n(\alpha))^{2^j}=\mathrm{Tr}_1^n(\alpha^{2^j})$, $j=0,1,\cdots$.

Let f be a Boolean function from F_{2^n} to F_2, and the set of which is denoted by B_n. The Walsh transform of $f\in B_n$ at F_{2^n} is defined as

$$W_f(a)=\sum_{x\in F_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n(ax)},\quad a\in F_{2^n}.$$

The values $W_f(a)$, $a\in F_{2^n}$ are called the Walsh coefficients of f. The Walsh spectrum of a Boolean function f is the multiset $\{W_f(a),a\in F_{2^n}\}$. A Boolean function f is said to be balanced if $W_f(0)=0$.

The nega-Hadamard transform of $f(x)$ at $a\in F_{2^n}$ is the complex valued function

$$N_f(a)=\sum_{x\in F_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n(ax)+\sigma(x)}i^{\mathrm{Tr}_1^n(x)}$$

where $\sigma(x)$ is the function defined by $\sigma(x)=\sum_{0\leqslant i<j\leqslant n-1}(x)^{2^i}(x)^{2^j}$. A function $f\in B_n$ is negabent if $|N_f(a)|=1$ for all $a\in F_{2^n}$.

2 Main Results

Let n be a positive integer and f be a Boolean function from F_{2^n} to F_2. For any $\delta\in F_{2^n}$, the Boolean function $g(x)=f(x)\mathrm{Tr}_1^n(x)+h(x)\mathrm{Tr}_1^n(\delta x)$ can be written as

$$g(x)=f(x)\mathrm{Tr}_1^n(x)+h(x)\mathrm{Tr}_1^n(\delta x)$$
$$=\begin{cases}0, & x\in T_{0,0}\\ h(x), & x\in T_{0,1}\\ f(x), & x\in T_{1,0}\\ f(x)+h(x), & x\in T_{1,1}\end{cases}$$

where $T_{i,j}=\{x\in F_{2^n}\mid \mathrm{Tr}_1^n(x)=i \text{ and } \mathrm{Tr}_1^n(\delta x)=j\}$ for $i,j=0,1$.

The relationship between $W_g(b)$ and $W_f(b)$, $W_h(b)$, $W_{f+h}(b)$ is given in Theorem 1.

Theorem 1 Let $\delta\in F_{2^n}$,

$$g(x)=f(x)\mathrm{Tr}_1^n(x)+h(x)\mathrm{Tr}_1^n(\delta x)$$

Then, the Walsh transform of $g(x)$ at $b\in F_{2^n}$ is given by

1) When $\delta=0$,

$$W_g(b)=\begin{cases}2^{n-1}+\frac{1}{2}[W_f(0)-W_f(1)], & \text{if } b=0\\ 2^{n-1}-\frac{1}{2}[W_f(0)-W_f(1)], & \text{if } b=1\\ \frac{1}{2}[W_f(b)-W_f(b+1)], & \text{if } b\in F_{2^n}^*\setminus\{1\}\end{cases}$$

2) When $\delta=1$,

$$W_g(b)=\begin{cases}2^{n-1}+\frac{1}{2}[W_{f+h}(0)-W_{f+h}(1)], & \text{if } b=0\\ 2^{n-1}-\frac{1}{2}[W_{f+h}(0)-W_{f+h}(1)], & \text{if } b=1\\ \frac{1}{2}[W_{f+h}(b)-W_{f+h}(b+1)], & \text{if } b\in F_{2^n}^*\setminus\{1\}\end{cases}$$

3) When $\delta\in F_{2^n}^*\setminus\{1\}$,

$$W_g(b)=\begin{cases}2^{n-2}+\frac{1}{4}[W_f(0)-W_f(1)+W_f(\delta)-W_f(\delta+1)+W_h(0)+W_h(1)-W_h(\delta)-W_h(\delta+1)\\ \quad +W_{f+h}(0)-W_{f+h}(1)-W_{f+h}(\delta)+W_{f+h}(\delta+1)], & \text{if } b=0\\ 2^{n-2}+\frac{1}{4}[-W_f(0)+W_f(1)-W_f(\delta)+W_f(\delta+1)+W_h(0)+W_h(1)-W_h(\delta)-W_h(\delta+1)\\ \quad -W_{f+h}(0)+W_{f+h}(1)+W_{f+h}(\delta)-W_{f+h}(\delta+1)], & \text{if } b=1\\ 2^{n-2}+\frac{1}{4}[W_f(0)-W_f(1)+W_f(\delta)-W_f(\delta+1)-W_h(0)-W_h(1)+W_h(\delta)+W_h(\delta+1)\\ \quad -W_{f+h}(0)+W_{f+h}(1)+W_{f+h}(\delta)-W_{f+h}(\delta+1)], & \text{if } b=\delta\\ 2^{n-2}+\frac{1}{4}[-W_f(0)+W_f(1)-W_f(\delta)+W_f(\delta+1)-W_h(0)-W_h(1)+W_h(\delta)+W_h(\delta+1)\\ \quad +W_{f+h}(0)-W_{f+h}(1)-W_{f+h}(\delta)+W_{f+h}(\delta+1)], & \text{if } b=\delta+1\\ \frac{1}{4}[W_f(b)-W_f(b+1)+W_f(b+\delta)-W_f(b+\delta+1)+W_h(b)+W_h(b+1)\\ \quad -W_h(b+\delta)-W_h(b+\delta+1)+W_{f+h}(b)-W_{f+h}(b+1)-W_{f+h}(b+\delta)+W_{f+h}(b+\delta+1)], & \text{if } b\in F_{2^n}^*\setminus\{1,\delta,\delta+1\}\end{cases}$$

Proof For simplicity, denote

$$\theta_t=\sum_{x\in T_{i,j}}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)},\ \theta_t'=\sum_{x\in T_{i,j}}(-1)^{h(x)+\mathrm{Tr}_1^n(bx)},$$
$$\theta_t''=\sum_{x\in T_{i,j}}(-1)^{f(x)+h(x)+\mathrm{Tr}_1^n(bx)}$$

where $i,j\in\{0,1\}$, $t=2i+j$, $0\leqslant t\leqslant 3$.

The proof proceeds in terms of three cases: $\delta=0$, $\delta=1$ and $\delta\in F_{2^n}^*\setminus\{1\}$.

1) If $\delta=0$, then one obtains

$$W_g(b)=\sum_{x\in F_{2^n}}(-1)^{f(x)\mathrm{Tr}_1^n(x)+\mathrm{Tr}_1^n(bx)}$$
$$=\sum_{x\in F_{2^n},\mathrm{Tr}_1^n(x)=0}(-1)^{\mathrm{Tr}_1^n(bx)}+\sum_{x\in F_{2^n},\mathrm{Tr}_1^n(x)=1}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}$$
$$=A_1+A_2,$$

where $A_1=\sum_{\mathrm{Tr}_1^n(x)=0}(-1)^{\mathrm{Tr}_1^n(bx)}$, $A_2=\sum_{\mathrm{Tr}_1^n(x)=1}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}$.

Note that

$$A_1=\begin{cases}2^{n-1}, & \text{if } b=0,1\\ 0, & \text{otherwise}\end{cases}$$

and $A_2=\theta_2+\theta_3$.

Then by

$$W_f(b)=\sum_{x\in F_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}$$
$$=\theta_0+\theta_1+\theta_2+\theta_3$$

and

$$W_f(b+1)=\sum_{x\in F_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n((b+1)x)}$$
$$=\theta_0+\theta_1-\theta_2-\theta_3,$$

we have

$$A_2=\frac{1}{2}[W_f(b)-W_f(b+1)]$$

2) The proof of 2) is obvious from 1).

3) If $\delta\in F_{2^n}^*\setminus\{1\}$, then one obtains

$$\begin{aligned}W_g(b)&=\sum_{x\in F_{2^n}}(-1)^{f(x)\mathrm{Tr}_1^n(x)+h(x)\mathrm{Tr}_1^n(\delta x)+\mathrm{Tr}_1^n(bx)}\\&=\sum_{x\in T_{0,0}}(-1)^{\mathrm{Tr}_1^n(bx)}+\sum_{x\in T_{0,1}}(-1)^{h(x)+\mathrm{Tr}_1^n(bx)}\\&+\sum_{x\in T_{1,0}}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}+\sum_{x\in T_{1,1}}(-1)^{f(x)+h(x)+\mathrm{Tr}_1^n(bx)}\\&=C_1+\theta_1'+\theta_2+\theta_3''\end{aligned}$$

where $C_1=\sum_{x\in T_{0,0}}(-1)^{\mathrm{Tr}_1^n(bx)}$.

Note that

$$C_1=\begin{cases}2^{n-2}, & \text{if } b=0,\ 1,\ \delta,\ \delta+1,\\ 0, & \text{otherwise.}\end{cases}$$

Together with the fact

$$\begin{aligned}W_f(b+\delta)&=\sum_{x\in F_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n((b+\delta)x)}\\&=\sum_{x\in T_{0,0}}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}-\sum_{x\in T_{0,1}}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}\\&+\sum_{x\in T_{1,0}}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}-\sum_{x\in T_{1,1}}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}\\&=\theta_0-\theta_1+\theta_2-\theta_3\end{aligned}$$

and

$$\begin{aligned}W_f(b+\delta+1)&=\sum_{x\in F_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n((b+\delta+1)x)}\\&=\sum_{x\in T_{0,0}}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}-\sum_{x\in T_{0,1}}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}\\&-\sum_{x\in T_{1,0}}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}+\sum_{x\in T_{1,1}}(-1)^{f(x)+\mathrm{Tr}_1^n(bx)}\\&=\theta_0-\theta_1-\theta_2+\theta_3\end{aligned}$$

Similarly,

$$\begin{aligned}&W_h(b)=(\theta_0'+\theta_1'+\theta_2'+\theta_3')\\&W_h(b+1)=(\theta_0'+\theta_1'-\theta_2'-\theta_3')\\&W_h(b+\delta)=(\theta_0'-\theta_1'+\theta_2'-\theta_3')\\&W_h(b+\delta+1)=(\theta_0'-\theta_1'-\theta_2'+\theta_3')\\&W_{f+h}(b)=(\theta_0''+\theta_1''+\theta_2''+\theta_3'')\\&W_{f+h}(b+1)=(\theta_0''+\theta_1''-\theta_2''-\theta_3'')\\&W_{f+h}(b+\delta)=(\theta_0''-\theta_1''+\theta_2''-\theta_3'')\\&W_{f+h}(b+\delta+1)=(\theta_0''-\theta_1''-\theta_2''+\theta_3'')\end{aligned}$$

Then by

$$\theta_2-\theta_1=\frac{1}{2}[W_f(b+\delta)-W_f(b+1)]$$

$$\theta_1+\theta_3=\frac{1}{2}[W_f(b)-W_f(b+\delta)]$$

$$\theta_2-\theta_3=\frac{1}{2}[W_f(b+\delta)-W_f(b+\delta+1)]$$

we have

$$\theta_2=\frac{1}{4}[W_f(b)-W_f(b+1)+W_f(b+\delta)-W_f(b+\delta+1)]$$

by

$$\theta_1'+\theta_3'=\frac{1}{2}[W_h(b)-W_h(b+\delta)]$$

$$\theta_1'-\theta_3'=\frac{1}{2}[W_h(b+1)-W_h(b+\delta+1)]$$

we have

$$\theta_1'=\frac{1}{4}[W_h(b)+W_h(b+1)-W_h(b+\delta)-W_h(b+\delta+1)]$$

Similarly, we have

$$\theta_3''=$$

$$\frac{1}{4}[W_{f+h}(b)-W_{f+h}(b+1)-W_{f+h}(b+\delta)+W_{f+h}(b+\delta+1)]$$

One immediately gets that

$$\begin{aligned}&\theta_1'+\theta_2+\theta_3''\\&=\frac{1}{4}[W_f(b)-W_f(b+1)+W_f(b+\delta)\\&-W_f(b+\delta+1)+W_h(b)+W_h(b+1)\\&-W_h(b+\delta)-W_h(b+\delta+1)+W_{f+h}(b)\\&-W_{f+h}(b+1)-W_{f+h}(b+\delta)+W_{f+h}(b+\delta+1)]\end{aligned}$$

when $b=0$,

$$\begin{aligned}W_g(0)=2^{n-2}&+\frac{1}{4}[W_f(0)-W_f(1)+W_f(\delta)-W_f(\delta+1)\\&+W_h(0)+W_h(1)-W_h(\delta)-W_h(\delta+1)\\&+W_{f+h}(0)-W_{f+h}(1)-W_{f+h}(\delta)+W_{f+h}(\delta+1)]\end{aligned}$$

when $b=1$,

$$\begin{aligned}W_g(1)=2^{n-2}&+\frac{1}{4}[-W_f(0)+W_f(1)-W_f(\delta)+W_f(\delta+1)\\&+W_h(0)+W_h(1)-W_h(\delta)-W_h(\delta+1)\\&-W_{f+h}(0)+W_{f+h}(1)+W_{f+h}(\delta)-W_{f+h}(\delta+1)]\end{aligned}$$

when $b=\delta$,

$$\begin{aligned}W_g(\delta)=2^{n-2}&+\frac{1}{4}[W_f(0)-W_f(1)+W_f(\delta)-W_f(\delta+1)\\&-W_h(0)-W_h(1)+W_h(\delta)+W_h(\delta+1)\\&-W_{f+h}(0)+W_{f+h}(1)+W_{f+h}(\delta)-W_{f+h}(\delta+1)]\end{aligned}$$

when $b=\delta+1$,

$$W_g(\delta+1)=$$

$$2^{n-2}+\frac{1}{4}[-W_f(0)+W_f(1)-W_f(\delta)+W_f(\delta+1)$$

$$-W_h(0)-W_h(1)+W_h(\delta)+W_h(\delta+1)$$
$$+W_{f+h}(0)-W_{f+h}(1)-W_{f+h}(\delta)+W_{f+h}(\delta+1)]$$

The proof is completed.

In particular, when $h(x)=f(x)+1$, the function $g(x)=f(x)\mathrm{Tr}_1^n(x)+(f(x)+1)\mathrm{Tr}_1^n(\delta x)$ is exactly the ones studied by Pang *et al*[15]. Note that our generic construction works for any $f(x)$ and $h(x)$. Therefore, our construction contains the previous ones in Ref. [15] as special cases.

Corollary 1 Let $\delta\in F_{2^n}\setminus\{1\}$, and

$$g(x)=f(x)\mathrm{Tr}_1^n(x)+(f(x)+1)\mathrm{Tr}_1^n(\delta x)$$

The Walsh transform of $g(x)$ at $b\in F_{2^n}$ is given by

$$W_g(b)=\begin{cases}2^{n-1}+\dfrac{1}{2}[W_f(\delta+1)-W_f(0)], & \text{if } b=1\\ 2^{n-1}-\dfrac{1}{2}[W_f(\delta+1)-W_f(0)], & \text{if } b=\delta\\ \dfrac{1}{2}[W_f(b+\delta)-W_f(b+1)], & \text{if } b\in F_{2^n}\setminus\{1,\delta\}\end{cases}$$

In the following, pang proposed three new classes of Boolean functions having the form as Eq. (2) by suitable choices of $f(x)$. The first class is obtained from bent functions, including Dillon bent, kasami bent and Gold-like bent functions, and from the definition of the dual of bent functions, the Walsh transform value distribution of such class is presented. Ref. [15] indicates that the Walsh spectrum distribution of $g(x)$ derived from bent functions is obtained from calculating the dual function of f and the values of $\#H_1$, $\#H_2$ and $\#H_3$. Therefore, the Walsh spectrum distribution of

$$g(x)=\mathrm{Tr}_1^n(ax^{2^m-1})\mathrm{Tr}_1^n(x)+(\mathrm{Tr}_1^n(ax^{2^m-1})+1)\mathrm{Tr}_1^n(\delta x)$$

is presented.

The second class is derived from Gold functions $f(x)=\mathrm{Tr}_1^n(ax^{2^i+1})$ and their Walsh spectrum distribution is obtained by making use of the Walsh transform property of Gold functions and the known conclusions of Weil sums in characteristic 2. The Walsh spectrum distribution of $g(x)$ which is obtained by Gold functions is discussed in the following three cases.

Case 1 n/d is even and $a\neq\alpha^{t(2^d+1)}$ for any integer t. It is known that in this case $f(x)=\mathrm{Tr}_1^n(ax^{2^i+1})$ is bent. Then the Walsh spectrum distribution of

$$g(x)=\mathrm{Tr}_1^n(ax^{2^i+1})\mathrm{Tr}_1^n(x)+(\mathrm{Tr}_1^n(ax^{2^i+1})+1)\mathrm{Tr}_1^n(\delta x)$$

is given in Ref. [15].

Case 2 n/d is even and $a=\alpha^{t(2^d+1)}$ for some integer t. In this case the Walsh spectrum distribution of

$$g(x)=\mathrm{Tr}_1^n(ax^{2^i+1})\mathrm{Tr}_1^n(x)+(\mathrm{Tr}_1^n(ax^{2^i+1})+1)\mathrm{Tr}_1^n(\delta x)$$

depends on whether $h(x)=(\delta+1)^{2^i}$ is solvable.

Case 3 n/d is odd. In this case we only need to consider $f(x)=\mathrm{Tr}_1^n(x^{2^i+1})$, then the Walsh spectrum distribution of

$$g(x)=\mathrm{Tr}_1^n(ax^{2^i+1})\mathrm{Tr}_1^n(x)+(\mathrm{Tr}_1^n(ax^{2^i+1})+1)\mathrm{Tr}_1^n(\delta x)$$

is presented in Ref. [15].

The last class comes from the product of linearized polynomials which have three or four Walsh transform values. With the help of k-tuple balance property, the Walsh spectrum distribution of such functions are determined. Ref. [15] present the Walsh transform of $f(x)=\prod_{i=1}^{k}\mathrm{Tr}_1^n(a_ix)$ together with the Walsh transform of Eq. (2), the Walsh spectrum distribution of

$$g(x)=\prod_{i=1}^{k}\mathrm{Tr}_1^n(a_ix)\mathrm{Tr}_1^n(x)+(\prod_{i=1}^{k}\mathrm{Tr}_1^n(a_ix)+1)\mathrm{Tr}_1^n(\delta x)$$

is given.

In another particular case, when $f(x)=0$ and $h(x)=\mathrm{Tr}_1^n(ux)$, the function $g(x)=\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$ is studied by Wu *et al*[16]. They give the necessary and sufficient conditions for $g(x)$ to be negabent.

Corollary 2 Let $g(x)=\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)$, where $(u,v)\in F_{2^n}^*\times F_{2^n}^*$. Then $g(x)$ is negabent on F_{2^n} if and only if one of the following conditions is satisfied:

1) $\mathrm{Tr}_1^n(u)=0$ and $\mathrm{Tr}_1^n(uv)=0$.

2) $\mathrm{Tr}_1^n(u)=1$ and $\mathrm{Tr}_1^n((u+1)v)=0$.

In Ref. [16], first they presented the necessary and sufficient conditions for the functions

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

to be negabent, where $n=2k$, $(u,v)\in F_{2^n}^*\times F_{2^n}^*$, $\lambda\in F_{2^k}$, when $\lambda=0$ it is the one discussed in Ref. [16]. Further, by using some permutation trinomials over F_{2^n}, they presented some classes of negabent functions of the form

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

where $0<k<n$.

3 Conclusion

In this paper, we proposed the Walsh transform of a class of Boolean functions by using the properties of the

Walsh transform and the trace function. Then, we hope that we can deduce the Walsh spectrum distributions of $g(x)$ defined as Eq. (1) by suitable choices of $f(x)$ and $h(x)$. Further, several new classes of Boolean functions with few Walsh transform values are obtained.

References

[1] Carlet C, Mesnager S. Four decades of research on bent functions [J]. *Designs*, *Codes and Cryptography*, 2016, **78**(1): 5-50.

[2] Mesnager S. *On Semi-Bent Functions and Related Plateaued Functions over the Galois Field* [M]. Berlin: Springer-Verlag, 2014.

[3] Tu Z B, Zheng D B, Zeng X Y, *et al*. Boolean functions with two distinct Walsh coefficients [J]. *Applicable Algebra in Engineering Communication and Computing*, 2011, **22**(5-6): 359-366.

[4] Rothaus O S. On "bent" functions [J]. *Journal of Combinatorial Theory*, 1976, **20**(3): 300-305.

[5] Frances M, Litman A. On covering problems of codes [J]. *Theory of Computing Systems*, 1997, **30**(2): 113-119.

[6] Calderbank R, Kantor W M. The geometry of two-weight codes [J]. *Bulletin of the London Mathematical Society*, 1986, **18**(2): 97-122.

[7] Carlet C. Boolean functions for cryptography and error-correcting codes [J]. *Encyclopedia of Mathematics and Its Applications*, 2016, **78**(1): 5-50.

[8] Olsen J, Scholtz R, Welch L. Bent-function sequences [J]. *IEEE Transactions on Information Theory*, 1982, **28**(6): 858-864.

[9] Carlet C. Boolean and vectorial plateaued functions and APN functions [J]. *IEEE Transactions on Information Theory*, 2015, **61**(11): 6272-6289.

[10] Sun Z Q, Hu L. Boolean functions with four-valued Walsh spectra [J]. *Journal of Systems Science and Complexity*, 2015, **28**(3): 743-754.

[11] Jin W G, Du X N, Sun Y Z, *et al*. Boolean functions with six-valued Walsh spectra and their application [J]. *Cryptography and Communications*, 2021, **13**(5): 393-405.

[12] Xu G K, Cao X W, Xu S D. Several new classes of Boolean functions with few Walsh transform values [J]. *Applicable Algebra in Engineering Communication and Computing*, 2017, **28**(2): 155-176.

[13] Tang C M, Zhou Z C, Qi Y F, *et al*. Generic construction of bent functions and bent idempotents with any possible algebraic degrees [J]. *IEEE Transactions on Information Theory*, 2017, **63**(10): 6149-6157.

[14] Mesnager S. Several new infinite families of bent functions and their duals [J]. *IEEE Transactions on Information Theory*, 2014, **60**(7): 4397-4407.

[15] Pang T T, Li N, Zhang L, *et al*. Several new classes of (balanced) Boolean functions with few Walsh transform values [J]. *Advances in Mathematics of Communications*, 2021, **15**(4): 757-775.

[16] Wu G F, Li N , Zhang Y Q, *et al*. Several classes of negabent functions over finite fields [J]. *Science China. Information Sciences*, 2018, **61**(3): 1-3.

□