The Walsh Transform of a Class of Boolean Functions

Jiang Niu, Zhuo Zepeng, Chen Guolong, Wang Liting
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
© Wuhan University 2021

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 $g(x) = f(x)\text{Tr}_1(x) + h(x)\text{Tr}_2(\delta x)$, 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

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 

\[ f(x) = g(x) + F(Tr^a(x), Tr^b(u,x), \ldots, Tr^e(u,x)) , \]

where \( n = 2m \), \( g(x) \) is any known bent function over \( F_2 \) satisfying some conditions, \( F(X_1, X_2, \ldots, X_m) \) is an arbitrary polynomial in \( F_2[x_1, x_2, \ldots, x_m] \). 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 

\[ g(x) = f(x)Tr^a(x) + h(x)Tr^b(\delta x) \quad (1) \]

where \( f(x) \) and \( h(x) \) are Boolean functions over \( F_2 \) and \( \delta \in F_2 \). In particular, the case of 

\[ g(x) = f(x)Tr^a(x) + (f(x) + 1)Tr^b(\delta x) \quad (2) \]

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 \( F_2^r \) denote the finite field with \( 2^r \) elements. For any set \( E, \ E' = E \setminus \{0\} \). By viewing each \( x = x_0 \xi_0 + x_1 \xi_1 + \cdots + x_n \xi_n \in F_2^r \) as a vector \( (x_0, x_1, \ldots, x_n) \in F_2^n \) where \( \{\xi_0, \xi_1, \ldots, \xi_n\} \) is a basis of \( F_2^n \) over \( F_2 \), we identify \( F_2^n \) with \( F_2^r \) 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 \( x \cdot y = Tr^a(xy) \).

For any positive integer \( k \mid n \), the trace function from \( F_2^n \) to \( F_2^k \) is the mapping defined as 

\[ Tr^a_k(x) = \sum_{j=0}^{k-1} x^{2^j} = x^2 + x^{2^2} + \cdots + x^{2^k}, \quad x \in F_2^n \]

When \( k = 1 \),

\[ Tr^a_1(x) = \sum_{j=0}^{n-1} x^{2^j} = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}} \]

is called the absolute trace function.

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

1) \( Tr^a_1(ax + by) = aTr^a_1(x) + bTr^a_1(y) \), \( \forall x, y \in F_2^r \) and \( a, b \in F_2 \).

2) \( Tr^a_1(x^2) = Tr^a_1(x) \) for any \( x \in F_2^r \).

3) For any \( \alpha \in F_2^r \), \( \sum_{a \in F_2^r} (-1)^{Tr^a_1(\alpha)} = 0 \) if \( \alpha \neq 0 \).

4) When \( F_2^r \subseteq F_2^r \subseteq F_2^r \), the trace function \( Tr^a_1(\alpha) \) satisfies the transitivity property, that is, \( Tr^a_1(\alpha) = Tr^a_1(Tr^a_1(\alpha)) \).

5) For any \( \alpha \in F_2^r \), \( (Tr^a_1(\alpha)^{2^j} = Tr^a_1(\alpha^{2^j}) \), \( j = 0, 1, \ldots \).

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 \( F_2^r \) is defined as 

\[ W_f(a) = \sum_{a \in F_2^r} (-1)^{Tr^a_1(\alpha)} \]

The values \( W_f(a), a \in F_2^r \), are called the Walsh coefficients of \( f \). The Walsh spectrum of a Boolean function \( f \) is the multiset \( \{W_f(a), a \in F_2^r\} \). A Boolean function \( f \) is said to be balanced if \( W_f(0) = 0 \).

The nega-Hadamard transform of \( f(x) \) at \( a \in F_2^r \) is the complex valued function 

\[ N_f(a) = \sum_{a \in F_2^r} (-1)^{\sigma(x) + Tr^a_1(\sigma(x))} i^{Tr^a_1(x)} \]

where \( \sigma(x) \) is the function defined by 

\[ \sigma(x) = \sum_{0 \leq i < j \leq n-1} (x^i)(x^j) \]

A function \( f \in B_n \) is negabent if \( |N_f(a)| = 1 \) for all \( a \in F_2^r \).

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 \( g(x) = f(x)Tr^a_1(x) + h(x)Tr^b_1(\delta x) \) can be written as
\[ g(x) = f(x)Tr^*_{\delta}(x) + h(x)Tr^*_{\delta}(\delta x) \]

where \( T_{ij} = \{ x \in F_{2^i}^* \mid Tr^*_{\delta}(x) = i \text{ and } Tr^*_{\delta}(\delta x) = j \} \) for \( i, j = 0,1 \).

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

**Theorem 1** Let \( \delta \in F_{2^i}^* \),

\[ g(x) = f(x)Tr^*_{\delta}(x) + h(x)Tr^*_{\delta}(\delta x) \]

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

\[
W_g(b) = \begin{cases} 
2^{n-2} + \frac{1}{4}[W_f(0) - W_f(1) + W_f(\delta) - W_f(\delta + 1) + W_h(0) - W_h(1) + W_h(\delta) - W_h(\delta + 1)], & \text{if } b = 0 \\
2^{n-2} + \frac{1}{4}[-W_f(0) + W_f(1) - W_f(\delta) + W_f(\delta + 1) + W_h(0) - W_h(1) - W_h(\delta) + W_h(\delta + 1)], & \text{if } b = 1 \\
2^{n-2} + \frac{1}{4}[W_f(0) + W_f(1) + W_f(\delta) - W_f(\delta + 1) - W_h(0) - W_h(1) + W_h(\delta) + W_h(\delta + 1)], & \text{if } b = \delta \\
2^{n-2} + \frac{1}{4}[W_f(0) - W_f(1) - W_f(\delta) - W_f(\delta + 1) + W_h(0) + W_h(1) + W_h(\delta) + W_h(\delta + 1)], & \text{if } b = \delta + 1 \\
1/4[W_f(b) - W_f(b + 1) + W_f(b + \delta) - W_f(b + \delta + 1) + W_h(b) + W_h(b + 1)] & \text{if } b \notin F_{2^i}^* \end{cases}
\]

**Proof** For simplicity, denote

\[
\theta_t = \sum_{x \in T_{ij}} (-1)^{f(x) + T^*_{\delta}(x) + T^*_{\delta}(b)}
\]

\[
\theta^* = \sum_{x \in T_{ij}} (-1)^{f(x) + 2T^*_{\delta}(x) + T^*_{\delta}(b)}
\]

where \( i, j \in \{0,1\} \), \( t = 2i + j \), \( 0 \leq t \leq 3 \).

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

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

\[ W_g(b) = \sum_{x \in F_{2^i}} (-1)^{f(x) + T^*_{\delta}(x) + T^*_{\delta}(b)} \]

\[ = \sum_{x \in F_{2^i}, T^*_{\delta}(x) = 0} (-1)^{T^*_{\delta}(b)} + \sum_{x \in F_{2^i}, T^*_{\delta}(x) = 1} (-1)^{f(x) + T^*_{\delta}(b)} \]

1) When \( \delta = 0 \),

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

2) When \( \delta = 1 \),

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

3) When \( \delta \in F_{2^i}^* \setminus \{1\} \),

\[ = A_1 + A_2, \]

where \( A_1 = \sum_{T^*_{\delta}(x) = 0} (-1)^{f(x) + T^*_{\delta}(b)}, A_2 = \sum_{T^*_{\delta}(x) = 1} (-1)^{f(x) + T^*_{\delta}(b)} \).

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

\[ W_f(b) = \sum_{x \in F_{2^i}} (-1)^{f(x) + T^*_{\delta}(b)} \]

\[ = \theta_0 + \theta_1 + \theta_2 + \theta_3 \]

and

\[ W_f(b + 1) = \sum_{x \in F_{2^i}} (-1)^{f(x) + T^*_{\delta}(b + 1)} \]

\[ = \theta_0 + \theta_1 - \theta_2 - \theta_3, \]
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 \( \delta \in F_B \setminus \{1\} \), then one obtains 

\[ W_g(b) = \sum_{x \in T_B} (-1)^{f(x)} + \sum_{x \in T_B} (-1)^{h(x)} + \sum_{x \in T_B} (-1)^{h(x)} + \sum_{x \in T_B} (-1)^{h(x)} \]

\[ = C_1 + \theta'_1 + \theta_2 + \theta'_3 \]

where \( C_1 = \sum_{x \in T_B} (-1)^{h(x)} \).

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 

\[ W_f(b + \delta) = \sum_{x \in T_B} (-1)^{f(x)} + \sum_{x \in T_B} (-1)^{f(x)} + \sum_{x \in T_B} (-1)^{f(x)} + \sum_{x \in T_B} (-1)^{f(x)} \]

\[ = \theta_2 - \theta_1 + \theta_2 - \theta_3 \]

and

\[ W_f(b + \delta + 1) = \sum_{x \in T_B} (-1)^{f(x)} + \sum_{x \in T_B} (-1)^{f(x)} + \sum_{x \in T_B} (-1)^{f(x)} + \sum_{x \in T_B} (-1)^{f(x)} \]

\[ = \theta_2 - \theta_1 - \theta_2 + \theta_3 \]

Similarly,

\[ W_f(b) = (\theta'_1 + \theta'_2 + \theta'_3 + \theta'_4) \]

\[ W_f(b + 1) = (\theta'_1 + \theta'_3 - \theta'_2 - \theta'_4) \]

\[ W_f(b + \delta) = (\theta'_1 - \theta'_2 + \theta'_3 - \theta'_4) \]

\[ W_f(b + \delta + 1) = (\theta'_1 - \theta'_2 - \theta'_3 + \theta'_4) \]

\[ W_{f,ab}(b) = (\theta'_6 + \theta'_7 + \theta'_8 + \theta'_9) \]

\[ W_{f,ab}(b + 1) = (\theta'_6 - \theta'_7 - \theta'_8 + \theta'_9) \]

\[ W_{f,ab}(b + \delta) = (\theta'_6 - \theta'_7 + \theta'_8 - \theta'_9) \]

\[ W_{f,ab}(b + \delta + 1) = (\theta'_6 - \theta'_7 - \theta'_8 + \theta'_9) \]

Then by

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

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

we have

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

by

\[ \theta'_1 + \theta'_2 + \theta'_3 + \theta'_4 = \frac{1}{2} [W_f(b + \delta) - W_f(b + \delta + 1)] \]

we have

\[ \theta'_1 = \frac{1}{2} [W_f(b + \delta) - W_f(b + \delta + 1)] \]

Similarly, we have

\[ \theta'_2 = \frac{1}{2} [W_f(b + \delta) - W_f(b + \delta + 1)] \]

One immediately gets that

\[ \theta'_1 + \theta'_2 + \theta'_3 + \theta'_4 \]

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

when \( b = 0 \),

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

\[ + W_f(0) + W_f(1) - W_f(\delta) - W_f(\delta + 1) \]

\[ + W_{f,ab}(0) - W_{f,ab}(1) - W_{f,ab}(\delta) + W_{f,ab}(\delta + 1) \]

when \( b = 1 \),

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

\[ + W_f(0) + W_f(1) - W_f(\delta) - W_f(\delta + 1) \]

\[ - W_{f,ab}(0) + W_{f,ab}(1) + W_{f,ab}(\delta) - W_{f,ab}(\delta + 1) \]

when \( b = \delta \),

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

\[ - W_f(0) + W_f(1) + W_f(\delta) - W_f(\delta + 1) \]

\[ - W_{f,ab}(0) + W_{f,ab}(1) + W_{f,ab}(\delta) - W_{f,ab}(\delta + 1) \]

when \( b = \delta + 1 \),

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

\[ - W_f(0) + W_f(1) + W_f(\delta) - W_f(\delta + 1) \]

\[ - W_{f,ab}(0) + W_{f,ab}(1) + W_{f,ab}(\delta) - W_{f,ab}(\delta + 1) \]
The Walsh transform of a Class of Boolean functions is obtained from calculating the dual of bent functions, the Walsh transform value distribution of \( g(x) \) is presented. Ref. [15] indicates that the Walsh spectrum distribution of \( g(x) \) is negabent on \( F_2^n \), where any of the following conditions is satisfied:

1. \( \text{Tr}^u(x) = 0 \) and \( \text{Tr}^v(uv) = 0 \).
2. \( \text{Tr}^u(x) = 1 \) and \( \text{Tr}^v(u + 1v) = 0 \).

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

\[
f(x) = \text{Tr}^u((\lambda x^{2^t+1}) + \text{Tr}^v(ux)\text{Tr}^v(vx), \quad 0 < k < n.
\]

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.