Arithmetic Walsh Transform of Boolean Functions with Linear Structures

Qinglan Zhao[1,2], Dong Zheng[2,*], Xiangxue Li[3],Xiaoli Dong[2]

[1] School of Information Engineering
Shanghai Jiaotong University, Shanghai 200240, China
[2] School of Telecommunication and Information Engineering,
Xi'an University of Post and Telecommunications, Xi'an 710121,China,
[3] Department of Computer Science and Technology,
East China Normal University, Shanghai 200241, China
*Corresponding author: zhengdong@xupt.edu.cn

Abstract. Arithmetic Walsh transform(AWT) of Boolean function caught our attention due to their arithmetic analogs of Walsh-Hadamard transform(WHT) recently. We present new results on AWT in this paper. Firstly we characterize the existence of linear structure of Boolean functions in terms of AWT. Secondly we show that the relation between AWT and WHT of a balanced Boolean function with a linear structure 1^n is sectionally linear. Carlet and Klapper's recent work showed that the AWT of a diagonal Boolean function can be expressed in terms of the AWT of a diagonal Boolean function of algebraic degree at most 3 in a larger number of variables.However their proof is right only when c has even weight.We complement their proof by considering the case of c with odd weight.

Keywords: Boolean functions; arithmetic Walsh transform; Walsh-Hadamard transform; linear structure

1 Introduction

In conventional cryptograpic systems, Boolean functions play an important role. Cryptographic transformations (pseudo-random generators in stream ciphers, S-boxes in block ciphers) are designed by appropriate composition of nonlinear Boolean functions [1]. To resist the known attacks, Boolean functions with cryptographic applications should satisfy a variety of criteria simultaneously. These are balancedness, nonlinearity, correlation immunity, algebraic degree, algebraic immunity etc [2]. The trade-off among these criteria have gotten many researches in Boolean function literature for a long time. The Walsh-Hadamard transform (WHT), which measure the proximity of a Boolean function to a cryptographically simple Boolean function [3], are often used to research on cryptographic properties of Boolean functions. In recent years, Klapper and Goresky defined an arithmetic or "with carry" analog of the WHT, known as the arithmetic Walsh transform (AWT) [4, 5]. It is a new one of with-carry analogs of without-carry phenomena, which have been studied for a long time, such as feedback with-carry shift registers, p-adic complexity [6]. Basic definitions of AWT were showed and the AWT of affine functions was determined in [4, 5]. Later the AWT of quadratic functions was determined in [7]. Carlet and Klapper generalized the classical Poisson summation formula to the AWT in [8]. The generalization maybe allow similar properties in the framework of addition with carry to be proved in the future. It was also showed that the AWT of a large class of Boolean functions(defined as diagonal function) can be expressed in terms of the AWT of a Boolean function of algebraic degree at most 3 in a larger number of variables in [8]. However the fact that they only proved the result for c with even weight makes this proof to be incomplete. The proof will be complemented in this paper.

Linear structure of Boolean functions has been investigated for their cryptanalytic significance [9–13]. Since the existence of linear structures of Boolean function is a weakness for block ciphers [10] and stream ciphers [14], the linear structure feature is an important criterion to measure cryptographic properties of a Boolean function in cryptographic applications. The WHT can give a characterization of linear structure of Boolean functions. Dubuc characterized the existence of linear structure by means of the WHT of Boolean function in [12].

In this paper we contribute some interesting results on the AWT of Boolean functions with linear structure. The remainder of the paper is organized as follows. In Sect.2, notations in this paper are listed, and some preliminaries about the n-variable Boolean functions, linear structure, the definition of AWT are reviewed. In Sect.3, the characterization of Boolean functions with linear structure by means of AHT is presented. In Sect.4, the linear relations of AWT and WHT of the balanced Boolean functions with 1^n complementary or invariant linear structure are established. In Sect.5, we complement Carlet and Klapper's proof in [8]. Sect.6 concludes the paper.

2 Preliminaries

2.1 Notations in this paper

In this paper we use the notations listed in table 1. Major of these notations are as same as used in [8].

Table 1. notations in this paper

notation	meaning
f	a Boolean function on $\mathbb{F}_2^n$
V_n	the set of n dimensional Boolean vectors
B_n	the set of n-variable Boolean functions
$supp(f)$	the support of f
$\overline{supp}(f)$	the set of x such that $f(x) = 0$
$wt(f)$	the weight of f
$W(f)(\omega)$	the Walsh-Hadamard coefficient of f at ω
$W^A(f)(\omega)$	the arithmetic Walsh coefficient of f at ω
R_n	the set of all Boolean functions on $\mathbb{N}^n$
$\mathbf{f}$	the extension of f to $\mathbb{N}^n$
D_x	the diagonal $\{x + i \cdot 1^n : i = 0, 1, 2 \ldots\}$
$\bar{f}(x)$	the 2-adic number associated with values of f on diagonal D_x
$Z(\mathbf{f})$	the imbalance of an eventually periodic $\mathbf{f}$

2.2 Boolean functions

A Boolean function on n variables is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$, for some positive integer n. Here $\mathbb{F}_2 = \{0, 1\}$ is the field with 2 elements. Let B_n denote the set of n-variable Boolean functions and V_n denote the set of n dimensional Boolean vectors. The support of a Boolean function is defined as $supp(f) = \{(x_1, x_2 \ldots x_n)|f(x_1, x_2 \ldots x_n) = 1\}$. The weight of a function $f \in B_n$ is $wt(f) = |supp(f)|$. A function is balanced if $wt(f) = 2^{n-1}$. Any $f \in B$ can be uniquely represented as a multivariate polynomial over $\mathbb{F}_2$ called the algebraic normal form (ANF),

$$f(x_1, x_2 \ldots x_n) = a_0 \oplus \sum_{1 \le i \le j \le n} a_i x_i \oplus \sum_{1 \le i \le j \le n} a_{i,j} x_i x_j \oplus \ldots + a_{1,2 \ldots n} x_1 x_2 \ldots x_n$$

where the coefficients $a_0, a_i, a_j, \ldots a_{1,2 \ldots n} \in \{0, 1\}$. The algebraic degree $deg(f)$ is the number of variables in the highest order term with non-zero coefficient.

Let $x = (x_1, x_2 \dots x_n)$ and $\omega = (\omega_1, \omega_2 \dots \omega_n)$ both belong to V_n, and $[x]_2$ denote reduction of an integer x. Let $x \cdot \omega = x_1 \cdot \omega_1 \oplus \dots \oplus x_n \cdot \omega_n$ denote $\mathbb{F}_2$-inner product. The *Walsh-hadamard transform* of $f(x)$ is an integer valued function over V_n which is defined as

$$W_f(\omega) = \sum_{x \in V_n} (-1)^{f(x) \oplus [x \cdot \omega]_2}$$

The Walsh spectrum of f is the set $\{W_f(\omega) | \omega \in V_n\}$.
Let α be a vector in V_n. If a Boolean function f such that $f(x) \oplus f(x+\alpha) = c$ where $c \in \{0,1\}$ for all $x \in V_n$, then α is a linear structure of f. α is a complementary linear structure of f if $c = 1$. α is an invariant linear structure of f if $c = 0$.
Concerning a function $f \in B_n$ with a linear structure, the following sufficient and necessary conditions are presented in [12].

Proposition 1 [12] *α is an invariant linear structure of f if and only if $W(f)(\omega) = 0$ for all $\omega \notin \alpha^{\perp}$. α is a complementary linear structure of f if and only if $W(f)(\omega) = 0$ for all $\omega \in \alpha^{\perp}$.*

2.3 Arithmetic Walsh transform

For self-completeness, we give the definition of AWT in this section.
Let $\mathbb{N} = \{0, 1, 2 \dots\}$ denote the natural numbers including 0. Any $f \in B_n$ can be extended to a mapping $\mathbf{f} : \mathbb{N}^n \to \mathbb{F}_2$ by setting

$$\mathbf{f}(x_1, x_2, ...x_n) = f(x_1 \bmod 2, x_2 \bmod 2, ...x_n \bmod 2)$$

We call $\mathbf{f}$ the extension of f. Let denote by R_n the set of all Boolean functions $\mathbf{f} : \mathbb{N}^n \to \mathbb{F}_2$. The extension $\mathbf{f}$ of f is 2-periodic function in R_n, since $\mathbf{f}(x + 2a) = \mathbf{f}(x)$ for any $a \in \mathbb{N}^n$. By setting $\mathbf{f}(x_1, x_2, ...x_n) = f_{(x_1, x_2, ...x_n)}$, we identify an element $\mathbf{f} \in R_n$ with a multi 2-adic integer whose formal expression is

$$\sum_{x=(x_1,x_2,\ \dots\ ,x_n) \in \mathbb{N}^n} f_x {t_1}^{x_1} {t_2}^{x_2} \ \dots\ {t_n}^{x_n}$$

The addition and Multiplication of R_n were defined similarly with the 2-adic integers[5, 6, 16]. However when the coefficient of $t^x = {t_1}^{x_1} {t_2}^{x_2} \ \dots\ {t_n}^{x_n}$ is 2 , one carry is induce to the t^{x+1^n}. The addition and Multiplication were as follows:

$$\sum_{x \in \mathbb{N}^n} f_x t^x + \sum_{x \in \mathbb{N}^n} g_x t^x = \sum_{x \in \mathbb{N}^n} h_x t^x$$

if there are carry integers $\{d_x | x \in \mathbb{N}^n\}$, such that $\{d_x\} = 0$ if any component of x is 0, and for all $x \in \mathbb{N}^n$ we have $f_x + g_x + d_x = h_x + 2d_{x+1^n}$.

$$\sum_{x\in\mathbb{N}^n} f_x t^x \cdot \sum_{x\in\mathbb{N}^n} g_x t^x = \sum_{x\in\mathbb{N}^n} h_x t^x$$

if there are carry integers $\{d_x | x \in \mathbb{N}^n\}$, such that $\{d_x\} = 0$ if any component of x is 0, and for all $x \in \mathbb{N}^n$ we have $\sum\limits_{x+y=z} f_x g_y + d_z = h_z + 2d_{z+1^n}$. Let$S_n = Z[[t_1, t_2, \ ... \ , t_n]]/(t_1 t_2 \ ... \ t_n - 2)$ which is isomorphic to the ring R_n. The sum of terms of a Boolean function $\mathbf{f} \in R_n$ in the diagonal $D_x = \{x + i \cdot 1^n : i = 0, 1, 2 \cdot\cdot\cdot\}$ defines a 2-adic integer:

$$\begin{aligned}\bar{f}(x) = \sum_{i=0}^{\infty} \mathbf{f}(x + i \cdot 1^n)(t_1 ... t_n)^i \\ = \sum_{i=0}^{\infty} \mathbf{f}(x + i \cdot 1^n) 2^i \qquad (1)\end{aligned}$$

There is a one to one correspondence between Boolean functions $\mathbf{f} \in R_n$ and functions $\bar{f} : \mathrm{H} \to Z_2$ where

$$\mathrm{H} = \{(x_1, x_2, \ ... \ , x_n) \in \mathbb{N}^n : \textit{some } i = 0\}.$$

Suppose that $\alpha = p/q$ is an arbitrary rational number. It is known that the 2-adic expansion for α is eventually periodic. The sum and difference of k-periodic numbers are eventually periodic. Based on the definition 1 in [5], it is clear that if $\mathbf{f} = \sum\limits_{i=0}^{\infty} f_i 2^i$ and $\mathbf{g} = \sum\limits_{i=0}^{\infty} g_i 2^i$ are 2-adic numbers with 2-periodic coefficient, the coefficients of index 2 of $-\mathbf{f}$, $\mathbf{f} - \mathbf{g}$, $\mathbf{f} + \mathbf{g}$, are eventually periodic.

If $\mathbf{f}$ is 2-peoriodic , then equation (1) can be expressed by

$$\begin{aligned}\bar{f}(x) &= \sum_{i=0}^{\infty} \mathbf{f}(x + i \cdot 1^n) 2^i \\ &= f(x) + f(x + 1^n)2 + f(x)2^2 + f(x + 1^n)2^3 + \ldots \\ &= -\frac{f(x) + 2f(x + 1^n)}{3}\end{aligned}$$

Definition 1 *Let* $\mathbf{f}$*∈* R_n *be eventually p-periodic. The imbalance of* $\mathbf{f}$ *is*

$$Z(\mathbf{f}) = \sum_{\mathbf{x}\in\mathbb{N}_\mathbf{n}} (-\mathbf{1})^{\mathbf{f(x)}}$$

where the sum is extended over one complete period of $\mathbf{f}$*.*

Definition 2 *The arithmetic Walsh transform of an eventually periodic* $\mathbf{f}\in R_n$ *is the real valued function* $W^A(\mathbf{f}):V_n \to \mathbb{R}$ *defined by* $W^A(\mathbf{f})(\omega) = Z(\mathbf{f} - \mathbf{l}_\omega)$*. If* f *is a Boolean function on* V_n*, then the arithmetic Walsh transform of* f *is the arithmetic Walsh transform of the extension* $\mathbf{f}$ *of* f*,* $W^A(\mathbf{f})(\omega)= W^A(f)(\omega)$*. The list of values of* $\langle \cdots, W^A(f)(\omega), \cdots\rangle$*,* $\omega \in V_n$ *is the arithmetic Walsh spectrum of* f*, and each* $W^A(f)(w)$ *is an arithmetic Walsh coefficient.*

Let $U_n = \{x \in \mathbb{F}_2^n : x_1 = 0\}$. The imbalance of an eventually periodic function $\mathbf{f}$ is the sum of the imbalances of the restrictions of $\mathbf{f}$ to the diagonals D_x with $x \in U_n$.

$$Z(\mathbf{f}) = \sum_{\mathbf{x}\in\mathbf{U_n}} \mathbf{Z}(\bar{\mathbf{f}}(\mathbf{x}))$$

Now let $l_\omega = [x\cdot\omega]_2$ be a linear function for $\omega \in V_n$, and let $\mathbf{l}_\omega$ denote the extension of l_ω. Using Lagrange interpolation, the following proposition was proved in [5].

Proposition 2 *Let* $f \in B_n$ *be a Boolean function.*
if $[\omega \cdot 1^n]_2 = 0$*,*

$$W^A(f)(\omega) = \sum_{x\in U_n} 2(1 - f(x) - f(x+1) + 2f(x)f(x+1^n)[x\cdot\omega]_2) \quad (2)$$
$$= 2^n - 2\sum_{x\in V_n} f(x) + 2\sum_{x\in V_n} f(x)f(x+1^n)[x\cdot\omega]_2 \quad (3)$$

if $[\omega \cdot 1^n]_2 = 1$*,*

$$W^A(f)(\omega) = 2\sum_{x\in U_n} (f(x+1^n) - f(x)f(x+1^n) + (f(x) - f(x+1^n))[x\cdot\omega]_2) \quad (4)$$
$$= \sum_{x\in V_n} (f(x+1^n) - f(x)f(x+1^n) + (f(x) - f(x+1^n))[x\cdot\omega]_2) \quad (5)$$

3 Characterization of Boolean functions with linear structures

Dubuc [12] have given the characterization of function with linear structure by means of its WHT. He showed that 1^n is an invariant linear structure of f if and only if $W(f)(\omega) = 0$ for all $\omega \notin (1^n)^\perp$, and 1^n is a complementary linear structure of f if and only if $W(f)(\omega) = 0$ for all $\omega \in (1^n)^\perp$. We generalize this result to AWT in this section. We firstly give the definition of linear structure of $\mathbf{f} \in R_n$. Then we characterize a Boolean functions with linear structure in terms of its AWT and get the similar results. Three class Boolean functions are discussed: Boolean functions with a 1^n invariant linear structure (theorem 1), Boolean functions with a $\alpha(\alpha \in V_n)$ invariant linear structure (theorem 2), and Boolean functions with a 1^n complementary linear structure (theorem 3).

Definition 3 *let $\boldsymbol{f} \in R_n$ be a function and $\alpha \in \mathbb{N}^n$ be a vector. We say* $\mathbf{f}$ *has an invariant linear structure α if $\mathbf{f}(x) = \mathbf{f}(x+\alpha)$ for all $x \in \mathbb{N}^n$.* $\mathbf{f}$ *eventually has an invariant linear structure α if there is a certain natural integer z such that $\mathbf{f}(x) = \mathbf{f}(x+\alpha)$ for all $x = (x_1, x_2 ... x_n) \in \mathbb{N}^n$ and $x_i \geq z$.*
we say $\mathbf{f}$ *has a complementary linear structure α if $\mathbf{f}(x+\alpha) \oplus \mathbf{f}(x) = 1$ for all $x \in \mathbb{N}_n$.*$\mathbf{f}$ *eventually has a complementary linear structure α if there is a certain natural integer z such that $\mathbf{f}(x) \oplus \mathbf{f}(x+\alpha) = 1$ for all $x = (x_1, x_2 ... x_n) \in \mathbb{N}^n$ and $x_i \geq z$.*

If α is an invariant or complementary linear structure of f , α is an invariant or complementary linear structure of the extension $\mathbf{f}$ of f. Especially as described in [8], $\mathbf{f}$ is diagonal if 1^n is an invariant linear structure of $\mathbf{f}$. Similarly $\mathbf{f}$ is eventually diagonal if 1^n is eventually an invariant linear structure of $\mathbf{f}$.
Next we give some lemmas that will be used later.

lemma 1 *If $w \in V_n$,*

$$\sum_{u \in V_n} (-1)^{u \cdot w} = \begin{cases} 2^n \ if \ w = 0^n, \\ 0 \ \ else. \end{cases}$$

lemma 2 *f is a balanced function if f has a complementary linear structure 1^n.*

lemma 3 *let f be a Boolean function and 1^n be a complementary linear structure of f, then*

$$W(f)(w) = \begin{cases} -2 \sum\limits_{x \in \mathrm{supp}(f)} (-1)^{[x \cdot w]_2} \qquad if \ \omega \notin (1^n)^\perp \\ 0 \qquad if \ \omega \in (1^n)^\perp. \end{cases}$$

lemma 4 [5] *Every Boolean function on V_n is uniquely determined by its arithmetic Walsh transform.*

From now on, let 10^{n-1} denote the vector with 1 values at the first place and 0 values at the other $n-1$ places. The following theorem characterize the Boolean function with 1^n complementary linear structure in terms of its AWT.

Theorem 1 *Let f be a boolean function on n variables. 1^n is an invariant linear structure of f if and only if $W^A(f)(w) = W^A(f)(10^{n-1})$ for all $\omega \notin (1^n)^\perp$.*

Using the above theorem 1 and proposition 2, we have the following corollary.

Corollary 1 *If 1^n is an invariant linear structure of a Boolean function f, $W^A(f)(\omega) = 0$ for all $\omega \notin (1^n)^\perp$.*

Theorem 2 *Let f be a boolean function on n variables, and α be a vector in V_n and $\alpha \neq 1^n$. Let $g(x) = f(x)f(x+1)$. α is an invariant linear structure of f if and only if*

$$W^A(f)(\omega) = \begin{cases} W^A(f)(10^{n-1}) \quad \text{if } \omega \in (1^n)^\perp \text{ and } \omega \notin \alpha^\perp\,, \\ \frac{2^n - W^A(g)(0^n)}{2} + W^A(f)(0^n) \quad \text{if } \omega \notin (1^n)^\perp \text{ and } \omega \notin \alpha^\perp. \end{cases}$$

Theorem 3 *Let f be a Boolean function in B_n. 1^n be a complementary linear structure of f if and only if $W^A(f)(\omega) = 0$ for all $\omega \in (1^n)^\perp$ and $W^A(f)(10^{n-1}) = 2^{n-1}$.*

4 Relation between AWT and WHT of functions with the linear structure 1^n

In this section we analysis the arithmetic Walsh coefficient of Boolean function with a 1^n invariant or complementary linear structure. We give the new expressions of the arithmetic Walsh coefficient of these functions using lemma 5 and lemma 6, and then establish the linear relation between the AWT and WHT based on theorem 4 and theorem 5.

lemma 5 *Let f be a Boolean function in B_n, and 1^n be an invariant linear structure of f. Then*

$$W^A(f)(\omega) = \begin{cases} 0, \qquad \omega \notin (1^n)^\perp, \\ 2^n - \text{supp}(f) - \sum\limits_{x \in \text{supp}(f)} (-1)^{[x \cdot \omega]_2}, \quad \omega \in (1^n)^\perp. \end{cases}$$

Proof. Let $\mathbf{f}$ denote the extension of f.
For $\omega \in V_n$, if $\omega \in (1^n)^{\perp}$,

$$\begin{aligned} W^A(f)(\omega) &= \sum_{x \in U_n} Z((\overline{\mathbf{f}} - \overline{\mathbf{1}_\omega})(x)) \\ &= \sum_{x \in U_n} Z(-\frac{f(x) + 2f(x+1^n)}{3} + [x \cdot \omega]_2). \end{aligned}$$

Let v be an integer and $u = v/3$. Table 2 lists the possible values of $Z(u)$. Let $Z^x = Z((\overline{\mathbf{f}} - \overline{\mathbf{1}}_\omega)(x))$. Using the table 2 we calculate the value of Z^x listed in table 3 for $\omega \cdot 1^n = 0$. From table 3, we can conclude that the value of $(f(x), f(x+1^n), [x \cdot w]_2)$ only can take $(0,0,0)$, $(1,1,0)$, $(0,0,1)$, $(1,1,1)$ for $f(x) = f(x+1^n)$, and they all contribute to the value of $\sum_{x \in U_n} Z^x$. Denote $n_{i,j,k}$ the number of $(f(x), f(x+1^n), [x \cdot w]_2) = (i,j,k)$ for all $x \in V_n$, where $i,j,k \in \{0,1\}$. So

Table 2. possible values of imbalances of some rational numbers

u	-1	-2/3	-1/3	0	1/3	2/3	1
$Z(u)$	-2	0	0	2	0	0	2

Table 3. possible values of imbalances of Z^x for $\omega \cdot 1^n = 0$

$f(x)$	0	1	0	1	0	1	0	1
$f(x+1^n)$	0	0	1	1	0	0	1	1
$[x \cdot \omega]_2$	0	0	0	0	1	1	1	1
Z^x	2	0	0	-2	2	0	0	2

$$\begin{aligned} W^A(f)(\omega) &= \sum_{x \in U_n} Z^x \\ &= \frac{1}{2} \cdot 2 \cdot (n_{0,0,0} - n_{1,1,0} + n_{0,0,1} + n_{1,1,1}) \\ &= (2^n - |\mathrm{supp}(f)|) - |\{x | x \in \mathrm{supp}(f), \mathit{and}\ [x \cdot w]_2 = 0\}| \\ &+ |\{x | x \in \mathrm{supp}(f), \mathit{and}\ [x \cdot w]_2 = 1\}| \\ &= (2^n - |supp(f)|) - \sum_{x \in supp(f)} (-1)^{[x \cdot w]_2} \end{aligned}$$

The last equation holds because $|\{x|x \in \mathrm{supp}(f), and\ [x \cdot w]_2 = 0\}| - |\{x|x \in \mathrm{supp}(f), and\ [x \cdot w]_2 = 1\}| = \sum\limits_{x \in \mathrm{supp}(f)} (-1)^{[x \cdot w]_2}$.

For $\omega \notin (1^n)^\perp$, we have $W^A(f)(\omega) = 0$ by corollary 1. □

Corollary 2 *Let f be a balanced Boolean function in B_n and 1^n be a invariant linear structure of f. Then*

$$W^A(f)(w) = \begin{cases} 0, & \omega \notin (1^n)^\perp, \\ = 2^{n-1} - \sum\limits_{x \in \mathrm{supp}(f)} (-1)^{[x \cdot w]_2}, & \omega \in (1^n)^\perp. \end{cases}$$

Theorem 4 *Let f be a balanced Boolean function in B_n, and 1^n be a invariant linear structure of f. Then*

$$W^A(f)(\omega) = \begin{cases} \frac{1}{2}W(f)(w) + 2^{n-1}, & \omega \in (1^n)^\perp\, and\, \omega \neq (0^n), \\ W(f)(\omega) = 0, & others. \end{cases}$$

Proof. We discuss in the following three cases.
Case 1. if $\omega = 0^n$, $W^A(f)(\omega) = W(f)(\omega) = 0$ for f is balanced,.
Case 2. if $\omega \notin (1^n)^\perp$, according to corollary 2 and proposition 1, we have $W^A(f)(\omega) = W(f)(\omega) = 0$ if $\omega \cdot 1^n = 1$.
Case 3. if $\omega \in (1^n)^\perp$ and $\omega \neq 0^n$, by lemma 1, if $\omega \neq 0^n$, the following equation holds.

$$\sum_{x \in \sup p(f)} (-1)^{x \cdot w} + \sum_{x \in \overline{\sup p}(f)} (-1)^{x \cdot w} = 0.$$

Then

$$\begin{aligned} W(f)(\omega) &= \sum_{x \in V_n} (-1)^{f(x) + [x \cdot \omega]_2} \\ &= -\sum_{x \in supp(f)} (-1)^{x \cdot w} + \sum_{x \in \overline{supp}(f)} (-1)^{[x \cdot \omega]_2} \\ &= -2 \sum_{x \in supp(f)} (-1)^{[x \cdot \omega]_2}. \end{aligned}$$

Using corollary 2, $W^A(f)(\omega) = \frac{1}{2}W(f)(w) + 2^{n-1}$. □

lemma 6 *Let f be a Boolean function in B_n, and 1^n be a complementary linear structure of f. Then*

$$W^A(f)(\omega) = \begin{cases} 0 & if\ \omega \in (1^n)^\perp, \\ 2^{n-1} - \sum\limits_{x \in \mathrm{supp}(f)} (-1)^{[x \cdot w]_2} & if\ \omega \notin (1^n)^\perp. \end{cases}$$

Table 4. possible values of imbalances ofZ^x for $\omega \cdot 1^n = 1$

$f(x)$	0	1	0	1	0	1	0	1
$f(x+1^n)$	0	0	1	1	0	0	1	1
$[x \cdot w]_2$	0	0	0	0	1	1	1	1
Z^x	0	0	2	0	0	2	0	0

Proof. If $\omega \in (1^n)^\perp$, by theorem 3, it is obvious that $W^A(f)(\omega) = 0$.
If $\omega \notin (1^n)^\perp$, as listed in table 4, the value of Z^x is 2 only when the value of $(f(x), f(x+1), x \cdot \omega)$ takes $(0,1,0)$,$(1,0,1)$. So

$$\begin{aligned} W^A(f)(\omega) &= \frac{1}{2} \cdot 2(n_{0,1,0} + n_{1,0,1}) \\ &= |\{x | x \in \mathrm{supp}(f), \mathit{and}\ xw = 1\}| + |\{x | x \in \overline{\mathrm{supp}}(f), \mathit{and}\ [x \cdot \omega]_2 = 0\}| \end{aligned}$$

Because $[\omega \cdot 1^n]_2 = 1$, we can deduce the following equation:

$$|\{x | x \in \overline{\mathrm{supp}}(f), \mathit{and}\ [x \cdot \omega]_2 = 0\}| = |\{x | x \in \mathrm{supp}(f), \mathit{and}\ [x \cdot \omega]_2 = 1\}|.$$

By applying lemma 2, then

$$\begin{aligned} W^A(f)(\omega) &= 2|\{x | x \in \mathit{supp}(f), \mathit{and}\ [x \cdot \omega]_2 = 1\}| \\ &= 2 \cdot \frac{1}{2}(|\mathit{supp}(f)| - \sum_{x \in \mathrm{supp}(f)} (-1)^{[x \cdot w]_2}) \\ &= 2^{n-1} - \sum_{x \in \mathrm{supp}(f)} (-1)^{[x \cdot w]_2} \qquad . \end{aligned}$$

□

Theorem 5 *Let f be a Boolean function in B_n, and 1^n be a complementary linear structure of f. Then*

$$W^A(f)(\omega) = \begin{cases} \frac{1}{2} W(f)(w) + 2^{n-1} & \omega \notin (1^n)^\perp, \\ W(f)(\omega) = 0 & \omega \in (1^n)^\perp. \end{cases}$$

Proof. by proposition 1 and lemma 6, we can obtain $W^A(f)(\omega) = W(f)(\omega) = 0$ if $\omega \in (1^n)^\perp$. Using lemma 3 and lemma 6, it can be deduced that $W^A(f)(\omega) = \frac{1}{2}W(f)(w) + 2^{n-1}$ if $\omega \notin (1^n)^\perp$. □

5 Complementation of Carlet and Klapper's proof

Carlet and Klapper [8] have studied the AWT of diagonal functions. They have firstly proved that the 2-adic imbalance of diagonal functions can be expressed in terms of the the 2-adic imbalance of diagonal functions of algebraic degree at most 3 in a larger number of variables, as scribed in the following theorem 6.

Theorem 6 *Let $g \in R_n$ be eventually 2-periodic and eventually diagonal. Then there are an integer $p \geq 1$ and a diagonal Boolean function $h \in B_{n+2p}$ such that $Z(h) = 2^p Z(g)$ and $deg(h) \leq 3$.*

By applying theorem 6, they have got the next corollary 3. However, the proof of this corollary is true only if c has even weight. If c has odd weight, theorem 6 can not be applied to $\mathbf{g} = \mathbf{f} - \mathbf{l_c}$ because $\mathbf{g}$ is not eventually diagonal.

Corollary 3 *Let $f \in B_n$ be a diagonal boolean function and let $c \in V_n$. Then there are an integer $P \geq 0$ and a Boolean function $h \in B_{n+2p}$ so that h has algebraic degree at most 3 and $Z(h) = 2^p W^A(f)(c)$.*

For self-consistent, we have ω replace c. We demonstrate the next corollary which is true for both ω with even weight and ω with odd weight based on their work.

Corollary 4 *Let $f \in B_n$ be a diagonal boolean function and let $\omega \in V_n$. Then there is an integer $P \geq 0$ and a diagonal Boolean function $h \in B_{n+2p}$ so that h has algebraic degree at most 3 and $W^A(h)(\omega) = 2^p W^A(f)(\omega)$.*

Proof. If ω has even weight, applying theorem 6 to $\mathbf{g} = \mathbf{f} - \mathbf{l}_\omega$, then there is an integer $p \geq 0$ and a diagonal Boolean function $h \in B_{n+2p}$ so that h has algebraic degree at most 3 and $Z(h - l_\omega) = 2^p W^A(f)(\omega)$. Here $h - l_\omega$ is also a diagonal function. It is implied that $W^A(h)(\omega) = 2^p W^A(f)(\omega)$ for ω has even weight.
By corollary 1, we can get that $W^A(f)(\omega) = 0$ if ω has odd weight. So if ω has odd weight, there is a diagonal Boolean function $h \in B_{n+2p}$ such that h has algebraic degree at most 3 and $W^A(h)(\omega) = 0 = 2^p W^A(f)(\omega)$.
□

6 Conclusion

In this paper, we have prensented the characterizations of the existence of linear struction of Boolean functions by means of AWT. Although the results on AWT is more complex than the results on WHT, the prensented characterizations are another analogs of well known results on WHT. Our study also have leaded to a linear relation between AWT and WHT of a large class of Boolean functions. This means that AWT of these functions can characterize the cryptographic properties of these functions as long as WHT can characterize the cryptographic properties of these functions. However functions of this result only include functions with 1^n complementary linear structure and balanced functions with 1^n invariant linear structure. It need further research on whether there are other functions whose AWT and WHT have linear relation. In addition, We have complemented Carlet and Klapper's proof of the result that the AWT of a large class of Boolean function can be expressed in terms of the AWT of a Boolean function of algebraic degree at most 3 in a larger number of variables.

Acknowledgements

We are grateful to Professor Claude Carlet for useful e-mail discussion. The work was supported in part by the National Science Foundation of China (NSFC) under Grant NO. 61472472,61272037,61402366.

References

1. Carlet C.: Boolean functions for cryptography and error correcting codes. In: Crama Y., Hammer P.(eds.) Boolean Methods and Models, pp. 257-397. Cambridge University Press, Cambridge.(2010).
2. Cusick T., Stanica P.: Cryptographic Boolean Functions and Applications, Academic Press, San Diego(2009).
3. Meier W., Staffelbach O.: Nonlinearity Criteria for Cryptographic Functions. In EUROCRYPT 89, Lecture Notes in Computer Science vol.434, pp.549-562(1990).
4. Klapper A., Goresky M.: A With-Carry Walsh Transform (Extended Abstract). In: C.Carlet, A.Pott, (eds.), SETA 2010. LNCS, vol.6338, pp.217-228.Springer, Heidelberg(2010).
5. Klapper A., Goresky M.: Arithmetic correlations and Walsh transforms, IEEETrans. Info. Theory 58, pp.479-492(2012).
6. Goresky M., Klapper A.: Algebraic Shift Register Sequences, Cambridge University Press: Cambridge(2012).
7. Klapper A.: Arithmetic Walsh transform of quadratic Boolean functions (extended abstract), In T. Helleseth and J. Jedwab eds., Sequences and Their Applications -SETA 2012, Lecture Notes in Computer Science, vol.7280, pp. 65-76.(2012)
8. Carlet C., Klapper A.: On the Arithmetic Walsh Coeffients of Boolean Functions. Designs Codes Cryptography, vol. 73, pp 299-318(2014).
9. Lai X.: Additive and Linear Structures of Cryptographic Functions. In Bart Preneel(eds.), Fast Software Encryption, Lecture Notes in Computer Science, Vol. 1008, pp 75-85(1995)

10. Evertse J.: Linear structures in block ciphers. In: Advances in Crptology-EUROCRYPT'87. LNCS 304, Berlin:Springer-Verlag, pp.249-266(1988).
11. Chaum D., Evertse J.: Cryptanalysis of DES with a reduced number of rounds sequences of linear factors in block cipher. In: Advances in Cryptology-CRYPTO85. LNCS 218, Berlin:Springer-Verlag, pp.192-211(1986).
12. Dubuc S.: Characterization of Linear Structures. Designs,Codes and Cryptography, vol.22, pp.33-45(2001).
13. Charpin P., Sarkar S.: Polynomials With Linear Structure and MaioranaCMcFarland Construction. Information Theory, IEEE Transactions on, vol.57(6), pp.3796-3804(2011).
14. Siegenthaler T.: Cryptanalyst representation of nonlinearly filtered ML-sequences. Advances in Cryptology, EUROCRYPT 85, Lecture Notes in Computer Science, pp.103-110(1986).
15. Carlet C.: A Transformation on Boolean functions, its consequences on some problems related to Reed-Muller codes. In Proceedings of EUROCODES'90, Lecture Notes in Computer Science vol. 514, pp.42-50, Springer-Verlag (1991).
16. Klapper A., Goresky M.: Feedback Shift Registers, Combiners with Memory, and 2-Adic Span. J. Cryptology, vol.10, pp. 111-147(1997).