Designs, Codes, and Cryptography manuscript No.
(will be inserted by the editor)

On the Arithmetic Walsh Coefficients of Boolean Functions

Claude Carlet · Andrew Klapper

Received: date / Accepted: date

Abstract We generalize to the arithmetic Walsh transform (AWT) some results which were previously known for the Walsh Hadamard transform of Boolean functions. We first generalize the classical Poisson summation formula to the AWT. We then define a generalized notion of resilience with respect to an arbitrary statistical measure of Boolean functions. We apply the Poisson summation formula to obtain a condition equivalent to resilience for one such statistical measure. Last, we show that the AWT of a large class of Boolean functions can be expressed in terms of the AWT of a Boolean function of algebraic degree at most 3 in a larger number of variables.

Keywords Arithmetic Walsh transform; Boolean function; Poisson summation formula; Resilience.

Mathematics Subject Classification (2000) 11E95; 94A55; 94A60; 94C10.

1 Introduction

The (standard) *imbalance* of a Boolean function is the number of times it takes the value 0 minus the number of times it takes the value 1. The *Walsh-Hadamard transform (WHT)* of a Boolean function f is the set of imbalances of functions of the form $f + l$ where l is linear and the addition is in $\mathbb{F}_2$. The WHT of a Boolean

This material is based upon work supported by the National Science Foundation under Grant No. CCF-0514660. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

Claude Carlet
LAGA, Department of Mathematics, University of Paris 8 (and Paris 13 and CNRS),
2 rue de la liberté, 93526 Saint–Denis cedex 02, France.
E-mail: claude.carlet@univ-paris8.fr

Andrew Klapper
Dept. of Computer Science, 307 Marksbury Building, University of Kentucky, Lexington, KY, 40506-0633. www.cs.uky.edu/
E-mail: klapper@cs.uky.edu

function has been a subject of considerable study for several decades. Much of the recent interest stems from its role in cryptography, where it can be used to measure resistance to certain cryptanalytic attacks. The WHT also gives a characterization of bent functions (meaning that all the Walsh-Hadamard coefficients are $\pm 2^{n/2}$, where n is the number of variables). It is desirable to have an understanding of what values can be taken on by the WHT of Boolean functions with particular properties (and not much is known in this respect).

Recently Mark Goresky and the second author defined an arithmetic or "with carry" analog of the WHT, known as the *arithmetic Walsh transform (AWT)* [5]. Its description, reviewed in Section 2 of this paper, is related to the arithmetic correlation of sequences, which plays an important role for the sequence generators called FCSRs [4, page 69], which are used in stream ciphers [1], and for arithmetic codes [9,10]. Many basic facts on AWTs were found by Goresky and Klapper [5]. In a later paper, the second author obtained the AWT of certain quadratic functions [6]. This paper continues the study of AWTs.

In earlier work, the first author of this paper showed that the imbalance of any Boolean function (and hence any Walsh-Hadamard coefficient) can be expressed in terms of the imbalance of a related Boolean function of degree at most 3, but depending on additional variables [2]. This result showed that the weights (and WHT values) of cubic functions (that is, of functions of algebraic degree 3) are much more complex than those of quadratic functions (of algebraic degree 2, see [8]). It was also used to construct a family of bent functions of degree 4 from a bent function of degree 3.

The well-known *Poisson summation formula* (in brief, PSF) for WHTs expresses weighted sums of Walsh-Hadamard coefficients $W(f)(a)$ with weightings of the form $(-1)^{d \cdot a}$, summed over a linear subspace of $\{0,1\}^n$ [3,8], in terms of sums of function values, summed over the dual space. This formula has been instrumental in the proof of many important results on Boolean functions, such as bounds on the algebraic degree of a Boolean function from divisibility properties of its WHT, characterization of correlation immune and resilient functions by their WHTs, relations between bent functions and their duals, and the study of propagation criteria [3].

In this paper we present results along lines of inquiry for AWTs analogous to those in the preceding two paragraphs. Although not explicitly connected to each other, both lines of inquiry are analogs of well known results on the WHT. First, in Section 3, we generalize the Poisson summation formula (PSF) to the AWT. Then in Section 4 we generalize the notions of correlation immunity and resilience to measures of security based on the average behavior of statistical measures of Boolean functions. We show that the arithmetic PSF can be used to characterize optimal behavior with respect to one such measure, a variant of resilience. We hope our generalization of the PSF will allow other properties in the framework of addition with carry to be studied in the future; such properties may be more difficult to guess (and finding them is probably a long term project) since the formula for the AWT is more complex than the formula for the WHT and has different expressions depending on the relations between certain parameters. Last, in Section 5 we show that the AWT of a function f can be expressed in terms of AWTs of functions with low degrees (similarly to the case of the WHT, observed by the first author [2]), under some restrictive condition on f.

1.1 Notation

We include here a list of major notation for the reader's convenience, along with the section in which each notation is introduced.

Section 2:

V_n: The set of n dimensional Boolean vectors.
B_n: The set of Boolean valued functions on V_n.
R_n: The ring of Boolean functions on $\mathbb{N}^n$.
D_c: The diagonal $\{c + i \cdot 1^n : i = 0, 1, \cdots\}$.
$\mathbf{f}$: The 2-periodic extension of $f \in B_n$ to $\mathbb{N}^n$.
$z(a)$: The imbalance of a 2-adic number $a = \sum_{i=0}^{\infty} a_i 2^i$, $z(a) = \sum(-1)^{a_i}$.
$U_n = \{c = (c_1, \cdots, c_n) \in \{0,1\}^n : c_1 = 0\}$.
$\bar{f}(c)$: The 2-adic number associated with the values of f on diagonal D_c.
$Z(\mathbf{f})$: The imbalance of an eventually periodic $\mathbf{f} \in R_n$.
$W^A(f)(c)$: The arithmetic Walsh coefficient of f at c.

Section 3:

$W(f)(c)$: The Walsh-Hadamard coefficient of f at c.
$S^{\perp}$: The dual space to sub-vector space S.
$\Gamma_{S,d}(f) = \sum_{a \in S}(-1)^{d \cdot a} W^A(f)(a)$.
$\delta_{a,b} = z(\bar{f}(b) - \bar{l}_a(b))$.
$\psi_{b,x} = z(\bar{f}(b) + x)$.
$H_T(f) = \sum_{b \in T} f(b)$.
$Q_T(f) = \sum_{b \in T} f(b) f(b + 1^n)$.

Section 4:

$Z_U(f) = \sum_{a \in U}(-1)^{f(a)}$.

Section 5:

$\Delta f(a) = f(a) + f(a + 1^n)$.

2 Basics of Arithmetic Walsh Transforms

Arithmetic Walsh transforms (AWTs), a with-carry analog of WHTs, were first considered by Goresky and Klapper [5]. Let $[x]_2$ denote the reduction modulo 2 of x, where x is an integer[1]. Let B_n denote the set of Boolean functions on $V_n = \mathbb{F}_2^n = \{0,1\}^n$. Recall that R_n is the ring of Boolean valued functions $\mathbf{f}$ on $\mathbb{N}^n$, the set of n-tuples of nonnegative integers, with an algebraic structure based on arithmetic with carry as follows. In this algebra, to add $\mathbf{f}$ and $\mathbf{g}$, we add the values of $\mathbf{f}$ and $\mathbf{g}$ at $c \in \mathbb{N}^n$ modulo 2, but we retain a "carry" to the value of $\mathbf{f} + \mathbf{g}$ at $c + 1^n$. More precisely, we have $\mathbf{f} + \mathbf{g} = \mathbf{h}$ if there exist integers $\{d_a : a \in \mathbb{N}^n\}$ so that $d_a = 0$ if any component of a is zero and for all $a \in \mathbb{N}^n$, we have $\mathbf{f}(a) + \mathbf{g}(a) + d_a = \mathbf{h}(a) + 2d_{a+1^n}$.

Let us see a small example with $n = 2$. We can describe a Boolean function $f \in B_2$ by a 2 by 2 Boolean matrix indexed by $\{0,1\}$ in each dimension, whose (i,j) entry is $f(i,j)$. Similarly, an element of R_2 is represented by an $\mathbb{N}$ by $\mathbb{N}$ Boolean matrix. Let

$$f = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } g = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

[1] Since we sometimes treat Boolean values as integers, it is helpful to indicate when we want to reduce an expression involving such values modulo 2.

(so that, for example, $f(1,0)=0$). Then

$$\mathbf{f}+\mathbf{g}=\begin{pmatrix} 0\,1\,0\,1\cdots \\ 1\,0\,1\,0 \\ 0\,1\,1\,1 \\ 1\,0\,1\,0 \\ \vdots \end{pmatrix}.$$

Here the main diagonal of $\mathbf{f}+\mathbf{g}$ (and all diagonals offset by multiples of 2) arises by adding the 2-adic numbers with coefficient sequences $1111\cdots$ and $1010\cdots$, and each remaining diagonal arises by adding the 2-adic numbers with coefficient sequences $0101\cdots$ and $1010\cdots$

In general, to multiply $\mathbf{f}$ and $\mathbf{g}$, we sum (modulo 2) the products of all pairs of values of $\mathbf{f}$ at $a\in\mathbb{N}^n$ and $\mathbf{g}$ at $b\in\mathbb{N}^n$ with $a+b=c$, but we retain a "carry" to the value of $\mathbf{fg}$ at $c+1^n$. More precisely, we have $\mathbf{fg}=\mathbf{h}$ if there exist integers $\{d_c : c\in\mathbb{N}^n\}$ so that $d_c=0$ if any component of a is zero and for all $a\in\mathbb{N}^n$, we have

$$\sum_{a+b=c\in\mathbb{N}^n}\mathbf{f}(a)+\mathbf{g}(b)+d_c=\mathbf{h}(c)+2d_{c+1^n}.$$

It can be seen that under these operations R_n is isomorphic to the quotient ring $\mathbb{F}_2[[t_1,\cdots,t_n]]/(t_1t_2\cdots t_n-2)$ (see [5]). Using this identification, it was shown that an element $\mathbf{f}$ of R_n corresponds to a choice of a 2-adic integer

$$\bar{f}(c)=\sum_{i=0}^{\infty}\mathbf{f}(c+i\cdot 1^n)2^i$$

for every $c\in X_n=\{c\in\mathbb{N}^n : c_i=0 \text{ for some } i\}$. That is, we can gather together all the values on the diagonal $D_c=\{c+i\cdot 1^n : i=0,1,\cdots\}$. Addition in R_n then corresponds to 2-adic addition of corresponding 2-adic diagonal elements. Note that the addition and subtraction of 2-adic numbers are not the same operation. If

$$a=\sum_{i=0}^{\infty}a_i2^i$$

and

$$b=\sum_{i=0}^{\infty}b_i2^i,$$

then

$$c=a-b=\sum_{i=0}^{\infty}c_i2^i$$

can be found iteratively as follows:

- $c_0\in\{0,1\}$ is defined by $a_0+2d_0=b_0+c_0$, where $d_0\in\{0,1\}$;
- $c_1\in\{0,1\}$ is defined by $a_1+2d_1=b_1+c_1+d_0$, where $d_1\in\{0,1\}$;
- continue infinitely in this way.

A 2-adic number is *(eventually) periodic* if its sequence of coefficients is (eventually) periodic. It is well known that the sum and difference of k-periodic 2-adic numbers are eventually k-periodic. Since this plays an important role in the paper, we recall the idea of the proof, for differences. Two 2-adic numbers a and b are k-periodic if $a = -u/(2^k - 1)$ and $b = -v/(2^k - 1)$ with $u, v \in \{0, 1, ..., 2^k - 1\}$. Then $a - b = (v - u)/(2^k - 1)$. The result then follows from Theorem 4.2.4 of Goresky and Klapper's book [4, page 75]: we know that $-(2^k - 1) \leq v - u \leq 2^k - 1$; if $v - u \leq 0$, then $(v - u)/(2^k - 1)$ is k-periodic; otherwise it can be written as $1 + w/(2^k - 1)$ with $-(2^k - 1) < w \leq 0$. The 2-adic expansion of $w/(2^k - 1)$ for such w is k-periodic, and is not the all 1 sequence (which would give $w = -(2^k - 1)$). Thus in adding 1 to $w/(2^k - 1)$ the carries cannot propagate past the first 0 coefficient, hence cannot propagate beyond the first k coefficients. Beyond that the coefficients of $1 + w/(2^k - 1)$ are the same as the coefficients of $w/(2^k - 1)$, hence are periodic. In fact we have shown that the difference of two k-periodic 2-adic numbers is k-periodic from the kth coefficient on. The same holds for sums of k-periodic 2-adic numbers.

If

$$a = \sum_{i=0}^{\infty} a_i 2^i$$

is an eventually k-periodic 2-adic number, then the (2-adic) *imbalance* of a is

$$z(a) = \sum (-1)^{a_i}$$

where the sum is extended over one complete period of a. If $k = 2$ and $a_i = a_{i+2}$ for all $i \geq j$, then

$$a = \sum_{i=0}^{j-1} a_i 2^i - \frac{a_j + 2a_{j+1}}{3} 2^j,$$

so

$$z(a) = (-1)^{a_j} + (-1)^{a_{j+1}} = z\left(-\frac{a_j + 2a_{j+1}}{3}\right).$$

Now we extend these ideas to elements of R_n. An element $\mathbf{f} \in R_n$ is *2-periodic* if $\mathbf{f}(c + 2d) = \mathbf{f}(c)$ for every $c, d \in \mathbb{N}^n$. It is *eventually* 2-periodic if there is a natural number z so that $\mathbf{f}(c + 2d) = \mathbf{f}(c)$ for all $c = (c_1, \cdots, c_n) \in \mathbb{N}^n$ with each $c_i \geq z$, and for all d. It follows that the sum and difference of two 2-periodic elements of R_n are eventually 2-periodic with $z = 2$. This follows from the analogous fact for 2-adic numbers and the fact that sums and differences of elements of R_n can be computed by adding or subtracting the 2-adic numbers associated with each diagonal.

If $\mathbf{f}$ is eventually 2-periodic, then a *complete period* of $\mathbf{f}$ is any set S of 2^n vectors c such that

1. for every $d \in \mathbb{N}^n$, $\mathbf{f}(c + 2d) = \mathbf{f}(c)$ (that is, c is in the periodic part of $\mathbf{f}$), and
2. for every $d \in \mathbb{N}^n$, there is a (necessarily unique) $c \in S$ so that $c \equiv d \mod 2$.

Let $U_n = \{c = (c_1, \cdots, c_n) \in \{0, 1\}^n : c_1 = 0\}$. If $\mathbf{f}$ is 2-periodic, then it is determined by the values $\bar{f}(c)$ with $c \in U_n$. For example, if $n = 2$ then $\mathbf{f}(1, 0) =$

$\mathbf{f}(1,2)$ (by 2-periodicity) $= \mathbf{f}((0,1)+1^n)$ so $\mathbf{f}(1,0)$ is determined by a value on the diagonal starting at $(0,1)$. In general if $\mathbf{f}$ is 2-periodic, then

$$\begin{aligned}\bar{f}(c) &= f(c) + f(c+1^n)2 + f(c)2^2 + f(c+1^n)2^3 + \cdots \\ &= (f(c) + 2f(c+1^n))(1 + 4 + 4^2 + \cdots) \\ &= -\frac{f(c) + 2f(c+1^n)}{3} \\ &= \frac{-u}{3},\end{aligned}$$

where $u \in \mathbb{Z}$ satisfies $0 \le u \le 3$. Note that in the third line we treat $f(c)$ and $f(c+1^n)$ as ordinary integers. We have used the fact that $1 + 4 + 4^2 + \cdots = 1/(1-4) = -1/3$.

We define the *2-adic imbalance* $Z(\mathbf{f})$ of an eventually 2-periodic $\mathbf{f} \in R_n$ to be the integer sum

$$Z(\mathbf{f}) = \sum (-1)^{\mathbf{f}(c)}$$

where the sum is extended over one complete period of $\mathbf{f}$ modulo 2. If $\mathbf{f}$ is periodic, then

$$Z(\mathbf{f}) = \sum_{c \in V_n} (-1)^{\mathbf{f}(c)} = \sum_{c \in U_n} (-1)^{\mathbf{f}(c)} + (-1)^{\mathbf{f}(c+1^n)}.$$

More generally, by the considerations above, if $\mathbf{f} \in R_n$ is eventually 2-periodic, then

$$Z(\mathbf{f}) = \sum_{c \in U_n} z(\bar{f}(c)).$$

As recalled in the introduction, this definition is related to the arithmetic correlation of sequences [4, page 178], [9,10] in which only the periodic part is taken into account as well. This may seem rather restrictive since the non-periodic part also plays a role but this definition captures the main behavior of the sequences and gives nice properties, as for instance the fact that the shifted arithmetic autocorrelations of an ℓ-sequence are identically zero. Also, the size and circuit complexity of an FCSR are determined by the connection integer, which equals the denominator of the rational representation of the 2-adic integer, and this is determined by the periodic part.

Note that

$$(-1)^{\mathbf{f}(c)} + (-1)^{\mathbf{f}(c+1^n)} = z\left(-\frac{\mathbf{f}(c) + 2\mathbf{f}(c+1^n)}{3}\right). \tag{1}$$

Thus if $\mathbf{f} \in R_n$ is eventually 2-periodic, then

$$Z(\mathbf{f}) = \sum_{c \in U_n} z\left(-\frac{\mathbf{f}(c + e_c 1^n) + 2\mathbf{f}(c + (e_c+1)1^n)}{3}\right),$$

where each e_c is chosen sufficiently large that $c + e_c 1^n$ is in the periodic part of $\mathbf{f}$.

It may seem unnecessarily complex to consider the right hand side of equation (1) rather than its left hand side. However, we shall have to work with such expressions when $\mathbf{f}$ is defined as a sum or a difference, which is the situation when dealing with the AWT.

Let $f \in B_n$. We extend f to a 2-periodic function $\mathbf{f} \in R_n$ by letting

$$\mathbf{f}(a) = f(a \mod 2).$$

We also let $l_c(a) = c \cdot a$ denote the inner product modulo 2 of c and a. This is a linear function whose extension to $\mathbb{N}^n$ is denoted $\mathbf{l}_c$, and whose associated 2-adic number on the diagonal based at b is $\bar{l}_a(b)$. Note that $\mathbf{f} - \mathbf{l}_c \in R_n$ is eventually 2-periodic. Then the *arithmetic Walsh coefficient of f at c* is

$$W^A(f)(c) = Z(\mathbf{f} - \mathbf{l}_c) = \sum_{b \in U_n} z(\bar{f}(b) - \bar{l}_a(b)) = \frac{1}{2} \sum_{b \in V_n} z(\bar{f}(b) - \bar{l}_a(b)),$$

and the *arithmetic Walsh transform (AWT) of f* is $\mathcal{W}^A(f) = \{W^A(f)(c) : c \in \{0,1\}^n\}$.

In previous work Goresky and Klapper showed that distinct Boolean functions have distinct AWTs [5]. This means, in particular, that the AWT is invertible, hence is a transform in the usual sense. However no simple formula for inverting the AWT is known. In the same paper they obtained explicit formulas for the expected AWT (the average over all c of $W^A(f)(c)$ for a fixed $f \in B_n$), and the second moment of the AWT (an arithmetic Parseval's identity) and obtained explicit formulas for the AWT of affine functions. In further work Klapper obtained explicit formulas for certain well behaved quadratic functions — those that are equivalent to one of the standard types by a change of basis $x \mapsto xN$ where N is a nonsingular matrix with $1^n N = 1^n$ [6].

3 Poisson Summation Formula

In this section we obtain an arithmetic analog of the classical PSF. We first establish some notation and recall the classical formula. Let S be a linear subspace of $V_n = \mathbb{F}_2^n = \{0,1\}^n$ (that is, an $\mathbb{F}_2$-vector space under addition modulo 2, or equivalently a binary linear code). Let $S^\perp$ denote the set of vectors that are orthogonal to every vector in S (the dual of code S). Recall that $\dim(S^\perp) = n - \dim(S)$. For any $d \subseteq V_n$, let $\langle d \rangle = \{0^n, d\}$ denote the linear subspace generated by d. If $d \in V_n$ and S and T are linear subspaces of V_n then $d + S = \{d + a : a \in S\}$ and $S + T = \{a + b : a \in S, b \in T\}$.

Let

$$W(f)(a) = \sum_{x \in V_n} (-1)^{f(x) + a \cdot x}$$

be the Walsh-Hadamard transform of f at input $a \in V_n$. In classical theory of Boolean functions [3,8], the PSF says that if $f \in B_n$ is a Boolean valued function on V_n, then for any $d \in V_n$,

$$\sum_{a \in S} (-1)^{d \cdot a} W(f)(a) = 2^{\dim(S)} \sum_{b \in d + S^\perp} (-1)^{f(b)} = 2^n - 2\,|S| \sum_{b \in d + S^\perp} f(b).$$

In this section, we consider similar summation formulas for the arithmetic Walsh transform $W^A(f)(a)$. For $d \in V_n$, let

$$\Gamma_{S,d}(f) = \sum_{a \in S} (-1)^{d \cdot a} W^A(f)(a) = \frac{1}{2} \sum_{a \in S} (-1)^{d \cdot a} \sum_{b \in V_n} z(\bar{f}(b) - \bar{l}_a(b)).$$

We write this as

$$\Gamma_{S,d}(f) = \frac{1}{2} \sum_{b \in V_n} \sum_{a \in S} (-1)^{d \cdot a} \delta_{a,b},$$

where

$$\delta_{a,b} = z(\bar{f}(b) - \bar{l}_a(b)) = z\left(-\frac{f(b) + 2f(b+1^n)}{3} + \frac{l_a(b) + 2l_a(b+1^n)}{3} \right).$$

Denoting $\psi_{b,x} = z(\bar{f}(b) + x)$, we can analyze $\delta_{a,b}$ in four cases:

1. If $a \cdot 1^n = 0$ and $a \cdot b = 0$, then
$$\delta_{a,b} = \psi_{b,0}, \tag{2}$$
2. If $a \cdot 1^n = 0$ and $a \cdot b = 1$, then
$$\delta_{a,b} = \psi_{b,1}, \tag{3}$$
3. If $a \cdot 1^n = 1$ and $a \cdot b = 0$, then
$$\delta_{a,b} = \psi_{b,2/3}, \tag{4}$$
4. If $a \cdot 1^n = 1$ and $a \cdot b = 1$, then
$$\delta_{a,b} = \psi_{b,1/3}. \tag{5}$$

In order to calculate these expressions, we first determine the values of $z(w/3)$ when $w \in \{-3, -2, -1, 0, 1, 2, 3\}$. These are given in Table 1.

w	-3	-2	-1	0	1	2	3
$z(w/3)$	-2	0	0	2	0	0	2

Table 1 Possible imbalances of some rational numbers with denominator 3.

This allows us to calculate the value of $\psi_{b,x}$ in each of the four cases $x = 0$, 1, 2/3, or 1/3 and for each pair $(f(b), f(b+1^n))$. These values are listed in Table 2.

$f(b)$	0	0	1	1
$f(b+1^n)$	0	1	0	1
$\psi_{b,0}$	2	0	0	-2
$\psi_{b,1}$	2	0	0	2
$\psi_{b,2/3}$	0	2	0	0
$\psi_{b,1/3}$	0	0	2	0

Table 2 $\psi_{b,x}$, when $x = 0$, 1, 2/3, 1/3.

We then obtain the expression of $\psi_{b,x}$ in each case as a polynomial in $f(b)$ and $f(b+1^n)$. We have

$$\psi_{b,0} = (-1)^{f(b)} + (-1)^{f(b+1^n)} = 2(1 - f(b) - f(b+1^n)).$$

The expressions for $\psi_{b,x}$ in the three other cases are obtained by doing Lagrange interpolation: treat $f(b)$ and $f(b+1^n)$ as variables u and v; then (for example) to find $\psi_{b,1}$ we want a polynomial $h(u,v)$ so that (by Table 2)

$$h(0,0) = h(1,1) = 2, h(0,1) = h(1,0) = 0.$$

Using Lagrange interpolation, one finds that

$$h(u,v) = 2uv + 2(1-u)(1-v) = 2(1-u-v+2uv).$$

Thus

$$\psi_{b,1} = 2(1 - f(b) - f(b+1^n) + 2f(b)f(b+1^n)).$$

By a similar calculation in the other cases, we have

$$\psi_{b,x} = \begin{cases} 2(1 - f(b) - f(b+1^n)) & \text{if } x = 0 \\ 2(1 - f(b) - f(b+1^n) + 2f(b)f(b+1^n)) & \text{if } x = 1 \\ 2(1 - f(b))f(b+1^n) & \text{if } x = 2/3 \\ 2f(b)(1 - f(b+1^n)) & \text{if } x = 1/3. \end{cases}$$

When $a \cdot 1^n = 0$ and $a \cdot b = 0$, it follows from equation (2) that

$$\delta_{a,b} = \psi_{b,0} = 2(1 - f(b) - f(b+1^n)).$$

When $a \cdot 1^n = 0$ and $a \cdot b = 1$, it follows from equation (3) that

$$\delta_{a,b} = \psi_{b,1} = 2(1 - f(b) - f(b+1^n) + 2f(b)f(b+1^n)).$$

When $a \cdot 1^n = 1$ and $a \cdot b = 0$, it follows from equation (4) that

$$\delta_{a,b} = \psi_{b,2/3} = 2(1 - f(b))f(b+1^n).$$

When $a \cdot 1^n = 1$ and $a \cdot b = 1$, it follows from equation (5) that

$$\delta_{a,b} = \psi_{b,1/3} = 2f(b)(1 - f(b+1^n)).$$

In the sequel we use the following notation. For any set $T \subseteq V_n$, let

$$H_T(f) = \sum_{b \in T} f(b) \quad \text{and} \quad Q_T(f) = \sum_{b \in T} f(b)f(b+1^n).$$

We simply write H_T and Q_T for $H_T(f)$ and $Q_T(f)$ when there is no possibility of confusion.

3.1 *When* $S \cdot 1^n = \{0\}$

Suppose that $a \cdot 1^n = 0$ for every $a \in S$, so that $1^n \in S^\perp$. We have

$$\Gamma_{S,d}(f) = \frac{1}{2} \sum_{b \in V_n} \sum_{a \in S, a \cdot b = 0} (-1)^{d \cdot a} \psi_{b,0} + \frac{1}{2} \sum_{b \in V_n} \sum_{a \in S, a \cdot b = 1} (-1)^{d \cdot a} \psi_{b,1}.$$

Let $T_{b,d} = \sum_{a \in S, a \cdot b = 1} (-1)^{d \cdot a}$. Then

$$\begin{aligned}
\Gamma_{S,d}(f) &= \sum_{b \in V_n} (1 - f(b) - f(b + 1^n)) \sum_{a \in S, a \cdot b = 0} (-1)^{d \cdot a} \\
&\quad + (1 - f(b) - f(b + 1^n) + 2 f(b) f(b + 1^n)) \sum_{a \in S, a \cdot b = 1} (-1)^{d \cdot a} \\
&= \sum_{b \in V_n} (1 - f(b) - f(b + 1^n)) \sum_{a \in S} (-1)^{d \cdot a} + 2 f(b) f(b + 1^n) T_{b,d} \\
&= (2^n - 2H_{V_n}) \sum_{a \in S} (-1)^{d \cdot a} + 2 \sum_{b \in V_n} f(b) f(b + 1^n) T_{b,d}. \qquad (6)
\end{aligned}$$

Lemma 1 *If $d \in S^\perp$, then $T_{b,d} = 0$ if $b \in S^\perp$ and $T_{b,d} = |S|/2$ if $b \notin S^\perp$. If $d \notin S^\perp$, then $T_{b,d} = 0$ if $b \in S^\perp$ or $b \in V_n \setminus (\langle d \rangle + S^\perp)$ and $T_{b,d} = -|S|/2$ if $b \in (\langle d \rangle + S^\perp) \setminus S^\perp = d + S^\perp$. Also,*

$$\sum_{a \in S} (-1)^{d \cdot a} = \begin{cases} |S| & \text{if } d \in S^\perp \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $b \in S^\perp$, then the sum is empty, hence zero, so suppose $b \notin S^\perp$. If $d \in S^\perp$, then $T_{b,d} = |\{a \in S : a \cdot b = 1\}| = |S|/2$. If $d \notin S^\perp$ and $b \in V_n \setminus (\langle d \rangle + S^\perp)$, then d is an independent parity check on $\{a \in S : a \cdot b = 1\}$, so $T_{b,d} = 0$. If $d \notin S^\perp$ and $b = d + c$ with $c \in S^\perp$, then all terms in the sum are -1, so $T_{b,d} = -|S|/2$.

The proof of the last statement is well-known and similar. □

Applying Lemma 1 to equation (6) gives the following theorem.

Theorem 2 *Let S be a linear subspace of V_n. Suppose that 1^n is a parity check for S. Then*

$$\Gamma_{S,d}(f) = \begin{cases} |S|(2^n - 2H_{V_n} + Q_{V_n \setminus S^\perp}) & \text{if } d \in S^\perp \\ -|S| Q_{d + S^\perp} & \text{if } d \notin S^\perp. \end{cases}$$

3.2 *When* $S \cdot 1^n = \{0, 1\}$

Suppose that $a \cdot 1^n = 1$ for some $a \in S$. Let $S_0 = \{a \in S : a \cdot 1^n = 0\}$ (the set of even weight vectors in S) and $S_1 = S \setminus S_0 = c + S_0$ for any $c \in S_1$. For $i \in \{0, 1\}$, let

$$W_i = \sum_{a \in S_i} (-1)^{a \cdot d}.$$

We have $W_0 = |S|/2$ if $d \in S_0^\perp$ and $W_0 = 0$ otherwise. We have $W_1 = |S|/2$ if $d \in S^\perp$, $W_1 = -|S|/2$ if $d \in S_0^\perp \setminus S^\perp$, and $W_1 = 0$ otherwise. Let

$$T_{b,d,i} = \sum_{a \in S_i, a \cdot b = 1} (-1)^{a \cdot d},$$

so

$$\sum_{a \in S_i, a \cdot b = 0} (-1)^{a \cdot d} = W_i - T_{b,d,i}.$$

Then

$$\begin{aligned}
\Gamma_{S,d}(f) &= \frac{1}{2} \sum_{b \in V_n} ((W_0 - T_{b,d,0})\psi_{b,0} + T_{b,d,0}\psi_{b,1} + (W_1 - T_{b,d,1})\psi_{b,2/3} \\
&\quad + T_{b,d,1}\psi_{b,1/3}) \\
&= \sum_{b \in V_n} ((W_0 - T_{b,d,0})(1 - f(b) - f(b + 1^n)) \\
&\quad + T_{b,d,0}(1 - f(b) - f(b + 1^n) + 2f(b)f(b + 1^n)) \\
&\quad + (W_1 - T_{b,d,1})(1 - f(b))f(b + 1^n) + T_{b,d,1}f(b)(1 - f(b + 1^n))) \\
&= \sum_{b \in V_n} (W_0(1 - f(b) - f(b + 1^n)) + 2T_{b,d,0}f(b)f(b + 1^n) \\
&\quad + W_1(f(b + 1^n) - f(b)f(b + 1^n)) + T_{b,d,1}(f(b) - f(b + 1^n))) \\
&= W_0(2^n - 2H_{V_n}) + W_1(H_{V_n} - Q_{V_n}) + 2 \sum_{b \in V_n} T_{b,d,0}f(b)f(b + 1^n) \\
&\quad + \sum_{b \in V_n} T_{b,d,1}(f(b) - f(b + 1^n)). \qquad (7)
\end{aligned}$$

Lemma 3 *For all $d \in V_n$ we have $T_{b,d,0} = 0$ if $b \in S_0^\perp$ and $T_{b,d,1} = 0$ if $b \in S^\perp$. If $d \in S^\perp$, then*

$$T_{b,d,0} = |S|/4 \text{ if } b \notin S_0^\perp$$

and

$$T_{b,d,1} = \begin{cases} |S|/2 \text{ if } b \in S_0^\perp \setminus S^\perp \\ |S|/4 \text{ if } b \notin S_0^\perp. \end{cases}$$

If $d \in S_0^\perp \setminus S^\perp$, then

$$T_{b,d,0} = 0 \text{ if } b \notin S_0^\perp$$

and

$$T_{b,d,1} = \begin{cases} -|S|/2 \text{ if } b \in S_0^\perp \setminus S^\perp \\ 0 \qquad \text{if } b \notin S_0^\perp. \end{cases}$$

If $d \notin S_0^\perp$, then

$$T_{b,d,0} = \begin{cases} 0 \qquad \text{if } b \notin \langle d \rangle + S_0^\perp \\ -|S|/4 \text{ if } b \in d + S_0^\perp \end{cases}$$

and

$$T_{b,d,1} = \begin{cases} 0 & \text{if } b \notin \langle d \rangle + S_0^\perp \\ -|S|/4 & \text{if } b \in d + S^\perp \\ |S|/4 & \text{if } b \in d + (S_0^\perp \setminus S^\perp). \end{cases}$$

Proof. In the first assertion the sums are empty, hence 0. Let $A_{b,i} = |\{a \in S_i : a \cdot b = 1\}|$ and $B_{b,d,i} = |\{a \in S_i : a \cdot b = a \cdot d = 1\}|$ so $T_{b,d,i} = A_{b,i} - 2B_{b,d,i}$.

Suppose $d \in S^\perp$. Then $T_{b,d,i} = A_{b,i}$. If $b \notin S_0^\perp$, then $a \cdot b = 1$ for half the $a \in S_i$, so $A_{b,i} = |S_i|/2 = |S|/4$. Hence, $T_{b,d,0} = T_{b,d,1} = |S|/4$. If $b \in S_0^\perp \setminus S^\perp$, then $a \cdot b = 1$ if $a \in S_1$. Hence, $T_{b,d,1} = |S_1| = |S|/2$.

Suppose $d \in S_0^\perp \setminus S^\perp$. If $b \in S_0^\perp \setminus S^\perp$, then $a \cdot b = 0$ for $a \in S_0$ and $a \cdot b = 1$ for $a \in S_1$; hence, $A_{b,1} = B_{b,d,1} = |S_1| = |S|/2$ and therefore $T_{b,d,1} = -|S|/2$. If $b \notin S_0^\perp$, then $T_{b,d,0} = 0$, $A_{b,1} = |S|/4$, $B_{b,d,1} = |S|/8$ and therefore $T_{b,d,1} = 0$.

Suppose $d \notin S_0^\perp$. If $b \notin \langle d \rangle + S_0^\perp$, then $A_{b,0} = |S_0|/2 = |S|/4$, $A_{b,1} = |S_1|/2 = |S|/4$, $B_{b,d,0} = A_{b,0}/2 = |S|/8$ and $B_{b,d,1} = A_{b,1}/2 = |S|/8$, so $T_{b,d,i} = 0$, $i = 0, 1$. If $b \in S_0^\perp \setminus S^\perp$, then $A_{b,1} = |S_1| = |S|/2$ and $B_{b,d,1} = |S_1|/2 = |S|/4$, so $T_{b,d,1} = 0$. If $b \in d + S^\perp$, then $A_{b,0} = A_{b,1} = B_{b,d,0} = B_{b,d,1} = |S_i|/2 = |S|/4$, so $T_{b,d,0} = T_{b,d,1} = -|S|/4$. If $b \in d + (S_0^\perp \setminus S^\perp)$, then $A_{b,0} = A_{b,1} = B_{b,d,0} = |S_i|/2 = |S|/4$ and $B_{b,d,1} = 0$, so $T_{b,d,0} = -|S|/4$ and $T_{b,d,1} = |S|/4$. □

Applying Lemma 3 to equation (7) and observing that $1^n \in S_0^\perp$ so that $d + S_0^\perp = 1^n + d + S_0^\perp$, and so $H_{d+S_0^\perp} = H_{1^n+d+S_0^\perp}$, we obtain the following theorem.

Theorem 4 *Let S be a linear subspace of V_n. Suppose that 1^n is not a parity check for S. Then, with the notation above:*

$$\Gamma_{S,d}(f) = \begin{cases} \frac{|S|}{2}(2^n - H_{V_n} - Q_{S_0^\perp} - H_{S^\perp} + H_{1^n+S^\perp}) & \text{if } d \in S^\perp \\ \frac{|S|}{2}(2^n - 3H_{V_n} + Q_{V_n} - H_{1^n+S^\perp} + H_{S^\perp}) & \text{if } d \in S_0^\perp \setminus S^\perp \\ -\frac{|S|}{2}(Q_{d+S_0^\perp} + H_{d+S^\perp} - H_{1^n+d+S^\perp}) & \text{if } d \notin S_0^\perp. \end{cases}$$

3.3 Example: Computing AWTs

As a simple example of the application of the PSF, consider the case when $S = V_n$. Then 1^n is not a parity check for S, so Theorem 4 applies. Suppose we are given the function $f \in B_n$ and want to compute the AWT of f. The theorem gives us a system of 2^n equations in the 2^n unknowns $W^A(f)(a)$. We can formulate this system of equations as a matrix equation $LW^A(f) = v_f$, where L is the $2^n \times 2^n$ matrix indexed in both dimensions by V_n. The vector $W^A(f)$ is the column vector whose ath term is $W^A(f)(a)$, and the column vector v_f is given by the righthand sides of the equations in Theorem 4. Note that v_f can be computed in time $O(2^n)$ from f. Indeed, $S^\perp = \{0^n\}$ and $S_0^\perp = \{0^n, 1^n\}$. Thus we have, for example, $H_{d+S^\perp} = f(d)$ and $Q_{d+S_0^\perp} = 2f(d)f(d+1^n)$. The (d, a) entry in L is $(-1)^{d \cdot a}$, so L is a Hadamard matrix. This means that

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

Thus the AWT can be computed as

$$W^A(f) = \frac{1}{2^n} L v_f.$$

This matrix product takes time $O(2^{2n})$ to compute by general methods. However we can do better using the method of fast Walsh transforms (FWT) to compute the product Lv_f. The classical Walsh-Hadamard transform amounts to the product LF where F is the column vector indexed by $a \in V_n$ whose ath term is $(-1)^{f(a)}$. The FWT method exploits the special structure of L to decompose it into a product of n sparse matrices. The method does not depend on properties of the vector F. It is thus applicable to computing the product Lv_f, which can be done in time $O(n2^n)$. See MacWilliams and Sloane's book for details on FWTs [8, p. 419-423].

3.4 Example: Inverting AWTs

As a second example of the application of the PSF, consider the problem of inverting the AWT. That is, of finding f given $\{W^A(f)(a) : a \in V_n\}$. As in Section 3.3, we can apply Theorem 4 to $S = V_n$. With L as in Section 3.3, by multiplying the AWT by L (again, using fast Walsh transform techniques) we can find

$$2f(d)f(d+1^n) + f(d) - f(d+1^n) \tag{8}$$

for all $d \in V_n \setminus \{0^n, 1^n\}$, as well as

$$2^n - H_{V_n} - 2f(0^n)f(1^n) - f(0^n) + f(1^n). \tag{9}$$

Consider formula (8). Its possible values are given in Table 3. We see that formula

$f(d)$	$f(d+1^n)$	$2f(d)f(d+1^n)+$ $f(d)-f(d+1^n)$
0	0	0
1	0	1
0	1	-1
1	1	2

Table 3 Inverting $W^A(f)$ at a diagonal pair.

(8) uniquely determines $f(d)$ and $f(d+1^n)$. Thus we can find $f(d)$ for all $d \neq 0^n, 1^n$.

Next, we have $W^A(f)(0^n) = 2^n - 2H_{V_n}$, which determines H_{V_n}. Knowing quantity (9) allows us to find

$$2f(0^n)f(1^n) + f(0^n) - f(1^n). \tag{10}$$

We see from Table 3 with $d = 0^n$ that formula (10) determines $f(0^n)$ and $f(1^n)$.

4 Generalized Correlation Immunity and Resilience

In this section we consider generalizations of the notions of m-correlation immunity and m-resilience. If U is a subset of V_n, then we let

$$Z_U(f) = \sum_{a \in U} (-1)^{f(a)}$$

be the imbalance of f on U. Recall that if $1 \leq m \leq n$, then f is *m-correlation immune* if its imbalance on any translate $d + S$ of a subspace S formed by fixing the values of m coordinates x_i (to 0 in S and to d_i in $d + S$) is proportional to its imbalance on V_n. That is, if

$$Z_{d+S}(f) = \frac{|d+S|}{2^n} Z_{V_n}(f) = \frac{|S|}{2^n} Z_{V_n}(f).$$

It is *m-resilient* if it is balanced (meaning that $Z_{V_n}(f) = 0$) and m-correlation immune. It is known that m-resilience is equivalent to the vanishing of all Walsh-Hadamard coefficients $W(f)(a)$ where a has Hamming weight at most m. Let us generalize this.

Definition 5 A *statistic* μ on B_n consists of a real valued function μ_U with domain B_n for each $U \subseteq V_n$.

For example, the imbalance $Z_U(f)$ of f on U is a statistic. We define another statistic, H, by

$$H_U(f) = \sum_{a \in U} f(a),$$

the Hamming weight of f on U. For any U and f we have $Z_U(f) = 2^n - 2H_U(f)$, so Z and H are essentially equivalent.

We define a third statistic, Q, by

$$Q_U(f) = \sum_{a \in U} f(a) f(a + 1^n)$$

for $U \subseteq V_n$. Note if μ is any of the three statistics, then for all disjoint $U, W \subseteq V_n$ and all $f \in B_n$ we have $\mu_U(f) + \mu_W(f) = \mu_{U \cup W}(f)$.

The functions Z_U and H_U depend only on the restriction $f|_U$ of f to U. This is not the case for Q if $1^n + U \neq U$. This is why we take B_n to be the domain of μ_U in general in Definition 5 rather than just letting the domain be the set of Boolean functions on U.

Definition 6 Let $S \subseteq V_n$ be a linear subspace. Let $f \in B_n$. Then f is *μ-correlation immune on S* if $\mu_T(f)$ is proportional to the size of T for every translate $T = d + S$ of S. That is, if for every such T we have

$$\mu_T(f) = \frac{|T|}{2^n} \mu_{V_n}(f) = \frac{|S|}{2^n} \mu_{V_n}(f).$$

Also, f is *μ-resilient on S* if it is balanced and is μ-correlation immune on S.

For example, in the classical theory of Boolean functions we say f is m-resilient if f is Z-resilient (or equivalently, f is H-resilient) on every subspace S formed by fixing m coordinates to 0. In this case f is balanced on U if and only if $Z_U(f) = 0$ (or, equivalently, if and only if $H_U(f) = |U|/2$).

Lemma 7 *Suppose that for all disjoint $U, W \subseteq V_n$ we have $\mu_U(f)+\mu_W(f) = \mu_{U\cup W}(f)$. If S is a linear subspace of V_n and $f \in B_n$ is μ-correlation immune on S, then f is μ-correlation immune on any subspace $S' \subseteq V_n$ containing S.*

Proof. Any subspace of V_n containing S is a disjoint union of translates of S. □

Certain correlation attacks lead us to consider the behavior of statistics on special subspaces. Suppose that $f \in B_n$ is used as a combiner in a stream cipher. Let $\mu_U(f)$ be a statistic defined for subsets $U \subseteq V_n$. Now suppose that $U \subseteq V_n$ is defined by fixing the values of m inputs to $b \in V_m$. If $\mu_U(f)$ depends on b, then it may be possible to mount a correlation attack to determine the value of b with high probability.

Definition 8 Let μ be a statistic. A Boolean function $f \in B_n$ is (μ, m)-*correlation immune* if it is μ-correlation immune on every subspace of $S \subseteq V_n$ formed by picking $I \subseteq \{1, \cdots, n\}$ of cardinality m and including in S all vectors whose support is disjoint from I. It is (μ, m)-*resilient* if it is μ-resilient on every such subspace.

Thus a function f is m-correlation immune in the traditional sense if and only if it is (Z, m)-correlation immune. It is m-resilient in the traditional sense if and only if it is (Z, m)-resilient.

4.1 Q-Correlation Immunity and Resilience from the PSF

The classical PSF implies the following result (see e.g. [3]):

Theorem 9 *Let $f \in B_n$ be a Boolean function and let S be a linear subspace of V_n. Then f is Z-correlation immune on $S^\perp$ if and only if for all $a \in S \setminus \{0^n\}$ we have $W^A(f)(a) = 0$. Also, f is Z-resilient on $S^\perp$ if and only if for all $a \in S$ we have $W^A(f)(a) = 0$.*

In this section we use the PSF to obtain a condition on the AWT that is equivalent to Q-correlation immunity and resilience. First we reduce without loss of generality to the case when 1^n is a parity check for the given subspace S.

Lemma 10 *Let S be a linear subspace of V_n. Let $S_0 = \{a \in S : a \cdot 1^n = 0\}$. Then f is Q-correlation immune (resp., Q-resilient) on $S^\perp$ if and only if it is Q-correlation immune (resp., Q-resilient) on $S_0^\perp$.*

Proof. If $S = S_0$ the result is trivial, so assume that $S \neq S_0$. This means that 1^n is not a parity check for S. Note that 1^n is a parity check for S_0. We have $S_0^\perp = S^\perp \cup (1^n + S^\perp)$ (this is a disjoint union). More generally, for any $d \in V_n$ we have $d+S_0^\perp = (d+S^\perp)\cup(d+1^n+S^\perp)$. Moreover, $Q_{d+S^\perp} = Q_{d+1^n+S^\perp}$, so $Q_{d+S_0^\perp} = 2Q_{d+S^\perp}$. Thus $Q_{d+S_0^\perp} = Q_{V_n}|d + S_0^\perp|/2^n$ if and only if $Q_{d+S^\perp} = Q_{V_n}|d + S^\perp|/2^n$.

It follows that f is Q-correlation immune (reps., Q-resilient) on $S^\perp$ if and only if it is Q-correlation immune (reps., Q-resilient) on $S_0^\perp$. □

Now suppose S is a subspace of V_n of dimension m and that 1^n is a parity check for S. This is equivalent to saying that S contains only vectors with even Hamming weight.

We have $W^A(f)(0^n) = Z(f) = 2^n - 2H_{V_n}$. If $d \in S^\perp$, then each $(-1)^{d\cdot a} = 1$. It follows from Theorem 2 that

$$(1-|S|)W^A(f)(0^n) + \sum_{a\in S\setminus\{0^n\}} W^A(f)(a) = |S|(Q_{V_n}(f) - Q_{S^\perp}(f)). \tag{11}$$

Theorem 11 *Let $f \in B_n$ and let S be a linear subspace of V_n. Let $S_0 = \{a \in S : a \cdot 1^n = 0\}$. Then f is Q-correlation immune on $S^\perp$ if and only if $W^A(f)(a) = W^A(f)(0^n) + Q_{V_n}$ for all $a \in S_0 \setminus \{0^n\}$.*

The reader is encouraged to compare this theorem to Theorem 9.

Proof. By Lemma 10, we may assume that $S = S_0$. That is, that S consists of even weight vectors.

We have $|S^\perp| = 2^n/|S|$. Let $M = |S| - 1$. Suppose that f is Q-correlation immune on $S^\perp$. This means that $Q_{d+S^\perp}(f) = Q_{V_n}|S^\perp|/2^n = Q_{V_n}/|S|$. Let a^i and d^i, $i = 0, \cdots, M$, be enumerations of S and a set of coset representatives for $S^\perp$ in V_n, respectively. Assume $a^0 = 0^n$. Thus from equation (11) and Theorem 2, respectively, we have

$$-MW^A(f)(a^0) + W^A(f)(a^1) + \cdots + W^A(f)(a^M) = MQ_{V_n} \tag{12}$$

and for each $i = 1, \cdots, M$,

$$W^A(f)(a^0) + (-1)^{a^1\cdot d^i} W^A(f)(a^1) + \cdots + (-1)^{a^M\cdot d^i} W^A(f)(a^M) = -|S|Q_{V_n}|S^\perp|/2^n$$
$$= -Q_{V_n}. \tag{13}$$

Moreover, every equation arising from Theorem 2 is among these equations. It can be checked that if $W^A(f)(0^n)$ is fixed, then $W^A(f)(a^i) = W^A(f)(0^n) + Q_{V_n}$ for $i = 1, \cdots, M$ is a solution to this system of equations. Thus it remains to see that the system of $M+1$ equations has rank M.

Let $x_{i,j} = (-1)^{a^i\cdot d^j}$, so the matrix of the system of equations in Theorem 2 is $X = [x_{i,j}]$, $0 \le i, j \le M$. This is a Hadamard matrix and thus is invertible (its inverse is $1/2^n$ times its transpose). The matrix, Y, of equations (12) and (13) is obtained from X by replacing $x_{0,0} = 1$ by $-M$. In particular, the last M rows of Y are linearly independent. Since we have already exhibited a one dimensional set of solutions, the rank of Y must be M. (In fact the first row of Y is the negative of the sum of the remaining rows.)

Conversely, suppose that $W^A(f)(a) = W^A(f)(0^n) + Q_{V_n}$ for all $a \in S_0 \setminus \{0^n\}$. Then from the first case in Theorem 2 we see that

$$|S|W^A(f)(0^n) + (|S|-1)Q_{V_n} = |S|(W^A(f)(0^n) + Q_{V_n} - Q_{S^\perp}).$$

Thus $|S|Q_{S^\perp} = Q_{V_n}$, so $Q_{S^\perp} = Q_{V_n}|S^\perp|/2^n$. Similarly, if $d \notin S^\perp$, then we see from the second case of Theorem 2 that $Q_{d+S^\perp} = Q_{V_n}|S^\perp|/2^n$. Thus f is Q-correlation immune on $S^\perp$. □

Corollary 12 *Let S be a linear subspace of V_n. Then f is Q-resilient on $S^\perp$ if and only if $W^A(f)(0^n) = 0$ and $W^A(f)(a) = Q_{V_n}$ for all $a \in S_0 \setminus \{0^n\}$.*

Proof. The function $f \in B_n$ is balanced if and only if $Z(f) = W^A(f)(0^n) = 0$. □

Corollary 13 *A Boolean function $f \in B_n$ is (Q, m)-correlation immune if and only if for all $a \in V_n \setminus \{0^n\}$ with even Hamming weight at most m we have $W^A(f)(a) = W^A(f)(0^n) + 2^{n-2}$. It is (Q, m)-resilient if and only if $W^A(f)(0^n) = 0$ and for all $a \in V_n \setminus \{0^n\}$ with even Hamming weight at most m we have $W^A(f)(a) = Q_{V_n}$.*

4.2 A Property of Q-uniformity stronger than Q-Correlation Immunity

We endow B_n with the uniform distribution. If μ is a statistic, let

$$E[\mu_U] = \frac{1}{2^{2^n}} \sum_{f \in B_n} \mu_U(f)$$

denote the expected value of μ_U, averaged over all Boolean functions.

A natural property of μ-uniformity to consider is, for a subspace S, that $\mu_T(f) = E[\mu_T(f)]$ for every translate T of S.

For any subset $U \subseteq V_n$, the expected value of $Q_U(f)$ over all $f \in B_n$ is $E[Q_U(f)] = |U|/4$, since the two events $f(a) = 1$ and $f(a + 1^n) = 1$ are independent and both have probability $1/2$.

Proposition 14 *Let S be a subspace of V_n. Let $f \in B_n$ be balanced. We have that, for every translate T of $S^\perp$, $Q_T(f) = |T|/4 = |S^\perp|/4$ if and only if $W^A(f)(0^n) = 0$, $W^A(f)(a) = 2^{n-2}$, for all $a \in S_0 \setminus \{0^n\}$, and $Q_{V_n} = 2^{n-2}$.*

Proof. By the same observation as in the proof of Lemma 10, we have $Q_T(f) = |S^\perp|/4$ for every translate T of $S^\perp$ if and only if $Q_{T_0}(f) = |S_0^\perp|/4$ for every translate T_0 of $S_0^\perp$, so we may assume $S = S_0$.

Suppose that $Q_T(f) = |S^\perp|/4$ for every translate T of $S^\perp$. Then for all d we have $Q_{d+S^\perp} = |S^\perp|/4 = 2^{n-2}/|S|$. By linearity we have $Q_{V_n} = 2^{n-2}$. By Theorem 2, for every $d \notin S^\perp$, $\Gamma_{S,d}(f) = -2^{n-2}$. Moreover, since f balanced implies $2^n - 2H_{V_n} = W^A(f)(0^n) = 0$, we have $\Gamma_{S,0^n}(f) = |S|(Q_{V_n} - Q_{S^\perp}) = (|S| - 1)2^{n-2}$. This gives us a nonsingular system of equations in the $W^A(f)(a)$, $a \in S$, and it is straightforward to check that $W^A(f)(0) = 0$, $W^A(f)(a) = 2^{n-2}$ for all $a \in S_0 \setminus \{0^n\}$ is a solution. Hence it is the unique solution.

Suppose $W^A(f)(0^n) = 0$, $W^A(f)(a) = 2^{n-2}$ for all $a \in S_0 \setminus \{0^n\}$, and $Q_{V_n} = 2^{n-2}$. Then by Theorem 2 for $d \notin S^\perp$ we have $-2^{n-2} = -|S|Q_{d+S^\perp}$ so $Q_{d+S^\perp} = |S^\perp|/4$. It then follows from additivity and $Q_{V_n} = 2^{n-2}$ that $Q_{S^\perp} = |S^\perp|/4$ as well. □

5 The AWT and Cubic Boolean Functions

In this section we show that, under some conditions, the arithmetic Walsh coefficient can be realized as the 2-adic imbalance of a Boolean function of degree at most three, but possibly in more variables. We begin with a generalization to the 2-adic imbalance of a well-known result on the standard imbalance.

Lemma 15 *Let $f \in B_n$ be a Boolean function and let $f'(a,b,c) = f(a) + bc \in B_{n+2}$, where a is a Boolean vector and b and c are additional Boolean variables. Then $Z(f') = 2Z(f)$.*

Proof. Considering the cases $(b,c) = (0,0),(0,1),(1,0)$ and $(1,1)$, we have that

$$\begin{aligned} Z(f') &= \sum_{a\in U_n} \sum_{b,c\in\{0,1\}} (-1)^{f(a)+bc} + (-1)^{f(a+1^n)+(b+1)(c+1)} \\ &= \sum_{a\in U_n} [(-1)^{f(a)} - (-1)^{f(a+1^n)} + (-1)^{f(a)} + (-1)^{f(a+1^n)} + (-1)^{f(a)} \\ &\quad +(-1)^{f(a+1^n)} - (-1)^{f(a)} + (-1)^{f(a+1^n)}] = 2Z(f). \end{aligned}$$

□

Assume now that $f(a) = f_1(a)f_2(a)+g(a)$ and apply a translation $b \mapsto b+f_2(a)$ and $c \mapsto c+f_1(a)$. We get

$$\begin{aligned} Z(f') &= \frac{1}{2} \sum_{b,c\in\mathbb{F}_2} \sum_{a\in\{0,1\}^n} z(\bar{f}'(a,b,c)) \\ &= \frac{1}{2} \sum_{b,c\in\mathbb{F}_2} \sum_{a\in\{0,1\}^n} z(\bar{f}'(a,b+f_2(a),c+f_1(a))) \\ &= \frac{1}{2} \sum_{a\in\{0,1\}^n} \sum_{b,c\in\mathbb{F}_2} A_{a,b,c} \end{aligned} \tag{14}$$

with

$$\begin{aligned} A_{a,b,c} = z\Bigg(&-\frac{[f(a)+(b+f_2(a))(c+f_1(a))]_2}{3} \\ &-\frac{2[f(a+1^n)+(b+f_2(a)+1)(c+f_1(a)+1)]_2}{3}\Bigg). \end{aligned}$$

This expression is the 2-adic imbalance of a Boolean function when $f_i(a+1^n) = f_i(a)$ for all a and for $i = 1,2$.

Definition 16 We say that $f \in B_n$ is *diagonal* if it has 1^n as a linear structure. That is, if for all $a \in \{0,1\}^n$ we have $f(a+1^n) = f(a)$. Similarly, $\mathbf{f} \in R_n$ is *diagonal* if for all $a \in \mathbb{N}^n$ we have $\mathbf{f}(a+1^n) = \mathbf{f}(a)$. We say $\mathbf{f} \in R_n$ is *eventually diagonal* if there is a natural number z so that $\mathbf{f}(a+1^n) = \mathbf{f}(a)$ for all $a = (a_1,\cdots,a_n) \in \mathbb{N}^n$ with each $a_i \geq z$.

For any function f, function $\Delta f(a) = f(a)+f(a+1^n)$ is diagonal. Every degree k diagonal function g is Δf for some degree $k+1$ function f, and $\Delta f = 0$ if and only if f is diagonal.

Lemma 17 *Suppose f is a diagonal Boolean function with degree k. Then there are an integer p and diagonal Boolean functions $f_{i,j}$, $i = 1,2$, $j = 1,\cdots,p$, such that*

$$f = \sum_{j=1}^{p} f_{1,j} f_{2,j}$$

and $\deg(f_{i,j}) \leq \lceil k/2 \rceil$.

Proof. It suffices to show this for Δ of a monomial, $f(c) = \Delta(c_1 \cdots c_{k+1})$, where the indeterminate $c = (c_1, \cdots, c_n)$. We prove this by induction on k. If $k = 0$, then $f = 1$ so $f_{1,1} = f_{2,1} = 1$.

Suppose the result is true for $\Delta(c_1 \cdots c_{m+1})$, $m < k$. We claim that

$$\Delta(c_1 \cdots c_{k+1}) = \Delta(c_1 \cdots c_k) + \prod_{i=1}^{k}(c_i + c_{k+1}).$$

Indeed, the left hand side includes all monomials in $c_1, \cdots, c_{k+1}$ of degrees at most k. The first term on the right hand side includes all monomials in $c_1, \cdots, c_k$ of degrees less than k, and the second term on the right hand side includes all monomials in $c_1, \cdots, c_{k+1}$ that are multiples of c_{k+1} and have degrees at most k, as well as the monomial $c_1 \cdots c_k$.

By induction there are an integer p and diagonal Boolean functions $f_{i,j}$, $i = 1, 2$, $j = 1, \cdots, p$, such that

$$\Delta(c_1 \cdots c_k) = \sum_{j=1}^{p} f_{1,j} f_{2,j}$$

and $\deg(f_{i,j}) \le \lceil (k-1)/2 \rceil$. We can write

$$f_{1,p+1} = \prod_{i=1}^{\lceil k/2 \rceil} (c_i + c_{k+1}) \quad \text{and} \quad f_{2,p+1} = \prod_{i=\lceil k/2 \rceil + 1}^{k} (c_i + c_{k+1}).$$

Then

$$\Delta(c_1 \cdots c_{k+1}) = \sum_{j=1}^{p+1} f_{1,j} f_{2,j},$$

proving the theorem. □

Theorem 18 *Let $\mathbf{g} \in R_n$ be eventually 2-periodic and eventually diagonal. Then there are an integer $p \ge 1$ and a diagonal Boolean function $h \in B_{n+2p}$ such that $Z(h) = 2^p Z(\mathbf{g})$ and $\deg(h) \le 3$.*

Proof. Since $\mathbf{g} \in R_n$ is eventually 2-periodic, there is a unique Boolean function f with extension $\mathbf{f} \in R_n$ to $\mathbb{N}^n$ so that $\mathbf{f}(a) = \mathbf{g}(a)$ for all $a \in V_n$ that are in the periodic part of $\mathbf{g}$. Moreover f is diagonal and $Z(f) = Z(\mathbf{g})$.

Let k be the degree of f. If $k \le 3$, then we are done. Otherwise we apply Lemma 17 to obtain diagonal Boolean functions $f_{i,j}$, $i = 1, 2$, $j = 1, \cdots, p$, such that $f = \sum_{j=1}^{p} f_{1,j} f_{2,j}$ and $\deg(f_{i,j}) \le \lceil k/2 \rceil$.

Let $\langle x, y \rangle$ denote the inner product of x and y. Let $b = (b_1, \cdots, b_p)$, $c = (c_1, \cdots, c_p)$, and $f_i(b) = (f_{i,1}(b_1), \cdots, f_{i,p}(b_p))$, $i = 1, 2$. Let

$$f'(a, b, c) = [f(a) + \langle b, c \rangle]_2 \in B_{n+2p}, \text{ and } f''(a, b, c) =$$

$$[f(a) + \langle b + f_2(a), c + f_1(a) \rangle]_2 = \sum_{j=1}^{p} (b_j c_j + b_j f_{1,j}(a) + c_j f_{2,j}(a)) \mod 2.$$

By Lemma 15 we have $Z(f') = 2^p Z(f)$. As in equation (14), but with $b, c \in \{0,1\}^p$ instead of in $\{0,1\}$, we have

$$\begin{aligned} Z(f') &= \frac{1}{2} \sum_{a\in\{0,1\}^n} \sum_{b,c\in\{0,1\}^p} z(\bar{f}'(a,b,c)) \\ &= \frac{1}{2} \sum_{a\in\{0,1\}^n} \sum_{b,c\in\{0,1\}^p} z(\bar{f}'(a,b+f_2(a),c+f_1(a))) \\ &= \frac{1}{2} \sum_{a\in\{0,1\}^n} \sum_{b,c\in\{0,1\}^p} z\left(-\frac{[f(a)+\langle b+f_2(a), c+f_1(a)\rangle]_2}{3}\right. \\ &\qquad \left. -\frac{2[f(a+1^n)+\langle b+1^p+f_2(a), c+1^p+f_1(a)\rangle]_2}{3}\right). \end{aligned}$$

We have $[f(a)+\langle b+f_2(a), c+f_1(a)\rangle]_2 = f''(a,b,c)$ and

$$\begin{aligned} &[f(a+1^n)+\langle b+1^p+f_2(a), c+1^p+f_1(a)\rangle]_2 \\ &= [f(a+1^n)+\langle b+1^p+f_2(a+1^n), c+1^p+f_1(a+1^n)\rangle]_2 \\ &= f''(a+1^n, b+1^p, c+1^p). \end{aligned}$$

Thus $Z(f'') = Z(f') = 2^p Z(f)$, and $\deg(f'') \le 1 + \lceil k/2 \rceil$. We can repeat these steps, replacing f by f'', until the degree is at most 3. □

Corollary 19 *Let $f \in B_n$ be a diagonal Boolean function and let $c \in V_n$. Then there are an integer $p \ge 0$ and a Boolean function $h \in B_{n+2p}$ so that h has algebraic degree at most 3 and $Z(h) = 2^p W^A(f)(c)$.*

Proof. Apply Theorem 18 to $\mathbf{g} = \mathbf{f} - \mathbf{l}_c$. □

The second author has determined the AWT of a large class of quadratic functions [6]. It is well known that every quadratic function $f \in B_n$ can be transformed to a quadratic form of one of three standard types by a change of basis, $a \to aN$, with N an invertible $n \times n$ matrix [7]. It was shown by him that if r is the rank of f, and N can be chosen so that $1^n N = 1^n$, then

$$W^A(f)(a) \in \{0, 2^{n-1}, 2^{n-2}, 2^{n-2} \pm 2^{n-\lfloor r/2 \rfloor - 1}\},$$

or

$$W^A(f)(a) \in \{2^{n-\lfloor r/2 \rfloor}, 2^{n-1}, 2^{n-2}, 2^{n-2} \pm 2^{n-\lfloor r/2 \rfloor - 1}\}.$$

Corollary 19 shows that the AWT of cubic functions behave more like that of general functions, as it was already the case with the WHT.

6 Conclusion

We have generalized the Poisson Summation Formula (PSF) to the Arithmetic Walsh Transform (AWT). The formula, which expresses weighted sums of arithmetic Walsh coefficients $W^A(f)(a)$, with weightings of the form $(-1)^{d \cdot a}$, summed over a linear subspace of $\{0,1\}^n$, is more complex than in the case of the Walsh Hadamard Transform: it has a different expression according to whether all the elements in the subspace have even Hamming weights or not, and in each of these two cases, the formula depends on different subcases relative to d. However it is still simple enough to hope that in the future we can generalize some important corollaries of the classical PSF to the AWT, and it has allowed us already to generalize a notion of correlation immunity/resiliency to the "with carry" context. We have also showed that, despite the higher complexity of the AWT, the property that every WHT coefficient of any Boolean function is proportional to the WHT coefficient of a Boolean function of degree at most 3 (in larger number of variables) can be generalized, as is, to the AWT (but in this paper we need to restrict ourselves to the so-called diagonal functions). We hope that this paper will promote further research on the AWT, which plays an important role when adapting the study of Boolean functions to the "with carry" framework.
Many questions remain open; for instance:
- Determine whether functions with constant squared AWT can exist. The mean and the 2nd moment of the AWT have been determined in [5, Theorems 9 and 10], but the question of the existence of constant squared AWT remains open. In this same reference (see [5, Section IX.A]) the question of how to define arithmetic bentness was raised; this related but wider question is of course still open as well.
- The main question from cryptographic viewpoint is: can a metric be used for defining a cryptographic parameter quantifying how good a given function is when used to combine or filter FCSRs? This question results in two sub-questions: (1) what is the relevant class of weak functions in the framework of FCSRs, similar to that of affine functions in the framework of LFSRs? (2) What is the relevant metric for expressing how different two functions are with respect to their use to combine or filter FCSRs? Can this metric be related to the AWT? For instance, is the metric of [5, Theorem 3] relevant? There is a notion of distance playing an important role in the framework of $\mathbb{Z}_4$-linear codes which deals with addition with carry: the Lee distance, defined as a distance between elements of $\mathbb{Z}/4\mathbb{Z}$. Can this notion be generalized to our framework?

References

1. F. Arnault, T. Berger, B. Pousse. A matrix approach for FCSR automata. *Cryptography and Communications 3(2)*, pp. 109-139, 2011.
2. C. Carlet, A Transformation on Boolean functions, its consequences on some problems related to Reed–Muller codes, in G. Cohen and P. Charpin, (eds.), *EUROCODE '90, Lecture Notes in Computer Science* **514**, pp. 42-50 (1991)
3. C. Carlet, Boolean functions for cryptography and error correcting codes, in Y. Crama, P. Hammer (eds.), *Boolean Methods and Models*, Cambridge University Press: Cambridge, 2010, pp. 257–397. Available at: http://www.math.univ-paris13.fr/~carlet/pubs.html.
4. M. Goresky and A. Klapper, *Algebraic Shift Register Sequences*, Cambridge University Press: Cambridge, 2012.
5. A. Klapper and M. Goresky, Arithmetic correlations and Walsh transforms, *IEEE Trans. Info. Theory* **58**, pp. 479-492 (2012).

6. A. Klapper, 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* **7280**, pp. 65-76 (2012).
7. R. Lidl and H. Niederreiter *Finite Fields* in *Encyclopedia of Mathematics vol. 20,* Cambridge University Press: Cambridge, 1983.
8. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland: Amsterdam, 1977.
9. D. Mandelbaum, Arithmetic codes with large distance, *IEEE Trans. Info. Theory* **IT-13**, pp. 237-242 (1967)
10. T. R. N. Rao, Error Coding For Arithmetic Processors. Academic Press, New York, 1974.
11. V. Strassen, Gaussian Elimination is not Optimal, *Numer. Math.* **13**, pp. 354-356 (1969).