Arithmetic Correlations and Walsh Transforms

Andrew Klapper *Senior Member, IEEE,* Mark Goresky *Member, IEEE,*

***Abstract*—In this paper the authors continue a program to find arithmetic, or "with-carry," analogs of polynomial based phenomena that appear in the design and analysis of cryptosystems and other branches of digital computation and communications. They construct arithmetic analogs of the Walsh-Hadamard transform and correlation functions of Boolean functions. These play central roles in the cryptographic analysis of block ciphers and stream ciphers. After making basic definitions and constructing various algebraic tools they: (1) show how to realize arithmetic correlations as cardinalities of intersections of hypersurfaces; (2) show that the arithmetic Walsh spectrum characterizes a Boolean function; (3) study the average behavior of arithmetic Walsh transforms; (4) find the arithmetic Walsh transforms of linear and affine functions.**

***Index Terms*—Walsh-Hadamard transform, correlation functions, p-adic numbers.**

I. Introduction

Over the last 15 years the authors have carried out a program to find arithmetic, or "with-carry," analogs of polynomial based phenomena that appear in the design and analysis of cryptosystems and other branches of digital computation and communications [3], [4], [6]–[8]. In this paper we construct arithmetic analogs of the Walsh-Hadamard transform and correlation functions of Boolean functions.

A. Klapper is with the Department of Computer Science, University of Kentucky, Lexington, KY, 40506-0633, USA. http://www.cs.uky.edu/∼klapper. This material is based upon work supported by the National Science Foundation under Grants No. CCF-0514660 and CCF-0914828. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

M. Goresky is with the School of Mathematics, Institute for Advanced Study, Princeton, NJ, 08540, USA. Research partially supported by the Charles Simonyi Endowment fund at the I.A.S. and by DARPA grant no. HR00110910010.

In cryptography there are two conflicting forces: systems need complexity to resist cryptanalysis and systems need simplicity to be efficient. This seems an impossible situation, but the wiggle room comes from the fact that "simple" for purposes of cryptanalysis is not necessarily the same as "simple" for purposes of efficiency. But even systems that are close to cryptanalytically simple systems are attackable since this closeness enables a more efficient search for the secret key. Design of good cryptosystems depends on finding computationally simple constructs with large distance from cryptanalytically simple constructs.

More specifically, we have the following outline of an attack. Suppose we use a Boolean function whose Hamming distance from some linear function is at most $k \geq 0$. Any observed string of output bits together with k puts some constraints on the initial state in the form of a probability distribution. A search for the initial state guided by this distribution has smaller expected success time.

The Walsh-Hadamard transform and cross correlation measure the proximity of a Boolean function to a cryptographically simple Boolean function $f(a_1, \cdots, a_n)$ [11]. More precisely, the classical Walsh-Hadamard transform $\widehat{f}(a)$ is related to the Hamming distance d between f and the linear function $T_a =$ "inner product with a," by

$$d = (2^n - \widehat{f}(a))/2. \tag{1}$$

Consequently the Walsh-Hadamard transform provides a basis for measuring the cryptographic security of stream and block ciphers. In this paper we define and study with-carry analogs of the Walsh-Hadamard transform and of correlation functions.

The usual way to add Boolean functions f and g is to add their corresponding values: $(f +$

$g)(a_1, \cdots, a_n) = f(a_1, \cdots, a_n) + g(a_1, \cdots, a_n)$. To define addition with carry, we need some place for the carries to go. We achieve this by extending each function in n Boolean variables to a function on $\mathbb{N}^n$ by setting $f(a_1, \cdots, a_n) = f(a_1 \bmod 2, \cdots, a_n \bmod 2)$. Then the carry from adding $f(a_1, \cdots, a_n)$ and $g(a_1, \cdots, a_n)$ goes to the value of the resulting function at the point $(a_1 + 1, \cdots, a_n + 1)$.

In Section II we define these algebraic structures and obtain some basic facts about them. In Section III we use these structures to define arithmetic Walsh transforms and arithmetic correlations. In Section IV we develop some tools for computing arithmetic correlations and use them to compute the arithmetic correlations of linear and affine functions. In Section V we show that the arithmetic Walsh transform is injective, so that it is indeed a transform. In Section VI we study the expectation and second moment of the arithmetic Walsh transform. The moment calculation is essentially an analog of Parseval's identity, but the picture is somewhat more complicated in the arithmetic case — the second moment varies depending on four parameters of the function. In Sections VII and VIII we find the arithmetic Walsh transforms of linear and affine functions.

It is not clear whether there are useful applications of these ideas. One difficulty is that the arithmetic Walsh transform does not relate to a formal distance function as the Walsh-Hadamard transform does. In the arithmetic case, given the arithmetic Walsh transform $\widetilde{f}(a)$ of a Boolean function f, we can, following equation (1) define $d' = (2^n - \widetilde{f}(a))/2$, but this turns out to not be a distance function in the formal mathematical sense. In fact, d' may be zero when f is not linear. We examine this phenomenon further later in the paper.

II. Algebraic Structures

A *Boolean function* is a function

$$f : V_n = \mathbb{F}_2^n \to \mathbb{F}_2$$

for some positive integer n. Here $\mathbb{F}_2 = \{0, 1\}$ is the field with 2 elements. Addition of Boolean functions is defined termwise, $(f + g)(a) = f(a) + g(a)$. The *imbalance* $Z(f)$ of a Boolean function f is the real number

$$Z(f) = \sum_{a \in V_n} (-1)^{f(a)}.$$

If $a \in V_n$, then the *shift* of f by a is the $\mathbb{F}_2$-valued function $f_a : V_n \to \mathbb{F}$ defined by

$$f_a(b) = f(a + b).$$

The *cross-correlation* of two Boolean functions f and g is the real valued function $C_{f,g} : V_n \to \mathbb{R}$ defined by

$$C_{f,g}(b) = Z(f + g_b). \tag{2}$$

The *autocorrelation* of f is $A_f(b) = C_{f,f}(b)$. For $a, b \in V_n$ let $[a \cdot b]_2$ denote their $\mathbb{F}_2$-inner product and let $T_a(b) = [a \cdot b]_2$, so that T_a is a linear function. The *Walsh-Hadamard Transform* of f is the real valued function $\widehat{f} : V_n \to \mathbb{R}$ defined by

$$\widehat{f}(a) = Z(f + T_a). \tag{3}$$

In this paper we define arithmetic analogs of the Walsh-Hadamard transform and the cross-correlation of Boolean functions by replacing the termwise sum (which is the same as the termwise difference since we are operating modulo 2) of functions by the *with-carry* difference. This takes some work since the carries naturally take us outside the domain of the Boolean function. Let $\mathbb{N} = \{0, 1, 2, \cdots\}$ denote the natural numbers *including* 0. A Boolean function f may be extended to a mapping $\mathbf{f} : \mathbb{N}^n \to \mathbb{F}_2$ by setting

$$\mathbf{f}(a_1, \cdots, a_n) = f(a_1 \mod 2, \cdots, a_n \mod 2).$$

The set of such extensions is the set

$$P_n = \{\mathbf{f} : \mathbb{N} \to \mathbb{F}_2 : \ \mathbf{f}(a + 2b) = \mathbf{f}(a)\},$$

of 2-periodic functions, which we consider to be a subset of the set of all Boolean functions,

$$R_n = \{\mathbf{f} : \mathbb{N}^n \to \mathbb{F}_2\}.$$

In general in this paper we denote Boolean functions by lower case letters and elements of R_n by boldface lowercase letters. The extension of a Boolean function to R_n is denoted by the boldface version of the letter denoting the Boolean function. Vectors in $\mathbb{N}^n$ are denoted by lowercase letters from the beginning

of the English alphabet. We denote the inner product of two integer vectors a and b by $a \cdot b$. We denote the reduction of an integer x modulo 2 by $[x]_2$. Thus the $\mathbb{F}_2$-inner product of two binary vectors a and b is $[a \cdot b]_2$

We now define an algebraic structure on the set R_n. It is helpful to first recall the definition of the 2-adic integers (in fact R_1 is exactly the 2-adic integers). A 2-adic integer is a formal expression

$$\mathbf{f} = \sum_{i=0}^{\infty} f_i 2^i,$$

where $f_i \in \mathbb{F}_2$. The set of 2-adic integers is denoted by $\mathbb{Z}_2$. There is a well defined algebraic structure on the set of 2-adic integers that makes it a ring. It is based on performing addition and multiplication with carry. Specifically, we say that

$$\sum_{i=0}^{\infty} f_i 2^i + \sum_{i=0}^{\infty} g_i 2^i = \sum_{i=0}^{\infty} h_i 2^i$$

if there are "carry" integers $d_0, d_1, d_2, \cdots$ so that $d_0 = 0$ and for all $i \geq 0$ we have $f_i + g_i + d_i = h_i + 2d_{i+1}$. Similarly, we say that

$$\sum_{i=0}^{\infty} f_i 2^i \cdot \sum_{i=0}^{\infty} g_i 2^i = \sum_{i=0}^{\infty} h_i 2^i$$

if there are carry integers $d_0, d_1, d_2, \cdots$ so that $d_0 = 0$ and for all $i \geq 1$ we have $f_i g_0 + f_{i-1} g_1 + \cdots + h_0 g_i + d_i = h_i + 2d_{i+1}$. The algebra of 2-adic integers has been studied for more than 100 years [5], [9] and recently the authors and others have used this algebra in the study of fast generation of pseudorandom sequences [3], [6].

It is natural to identify a function $\mathbf{f} \in R_1$ with the 2-adic integer

$$\sum_{a=0}^{\infty} f(a) 2^a.$$

We wish to find a similar identification for functions $\mathbf{f} \in R_n$ of several variables. For this, we need a multiple term analog of the 2-adic integers in much the same way that we generalize power series in one variable to power series in several variables. The new structure can be thought of as having several "2s". To distinguish them from the ordinary integer 2, we denote them by $t_1, \cdots, t_n$. Then a multi-2-adic integer is a formal expression

$$\sum_{a=(a_1,\cdots,a_n)\in\mathbb{N}^n} f_a t_1^{a_1} \cdots t_n^{a_n},$$

with $f_a \in \mathbb{F}_2$. We can identify an element $\mathbf{f} \in R_n$ with a multi-2-adic integer by setting $f_{(a_1,\cdots,a_n)} = \mathbf{f}(a_1, \cdots, a_n)$. To think about this geometrically, each lattice point $(a_1, a_2, \cdots, a_n) \in \mathbb{N}^n$ corresponds to a monomial $t_1^{a_1} t_2^{a_2} \cdots t_n^{a_n}$ and the multi-2-adic number $\sum_{a\in\mathbb{N}^n} f_a t^a$ can be identified with the collection of lattice points $a \in \mathbb{N}^n$ such that $f_a = 1$ as in Figure 1 for $n = 2$.

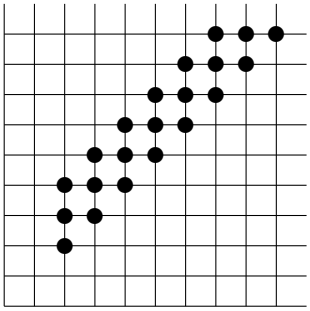

Fig. 1. $t_1^2 t_2^2 (1 + t_2 + t_2^2) \sum_{n=0}^{\infty} (t_1 t_2)^n$

For convenience, if $a \in \mathbb{N}^n$, let t^a denote $t_1^{a_1} \cdots t_n^{a_n}$. Also, let $1^n = (1, 1, \cdots, 1) \in \mathbb{N}^n$ and $0^n = (0, 0, \cdots, 0) \in \mathbb{N}^n$. In each arithmetic computation, we want a coefficient equal to 2 to induce a carry to "the next place in each variable", that is, to the monomial with the exponent of each t_i increased by one. Accordingly, define an addition operation by saying that

$$\sum_{a\in\mathbb{N}^n} f_a t^a + \sum_{a\in\mathbb{N}^n} g_a t^a = \sum_{a\in\mathbb{N}^n} h_a t^a$$

if

1) there exist integers $\{d_a : a \in \mathbb{N}^n\}$ so that $d_a = 0$ if any component of a is zero, and
2) for all $a \in \mathbb{N}^n$, we have: $f_a + g_a + d_a = h_a + 2d_{a+1^n}$.

In other words, addition is just 2-adic addition along the diagonals

$$D_a = \{a + c(1, 1, \cdots, 1) : c \in \mathbb{N}\}. \tag{4}$$

(Since each diagonal ends on a coordinate hyperplane the set of distinct diagonals is parametrized by elements $a = (a_1, \cdots, a_n) \in \mathbb{N}^n$ such that at least one of the coordinates a_i vanishes.) Similarly, define a multiplication operation by saying that

$$\sum_{a\in\mathbb{N}^n} f_a t^a \cdot \sum_{a\in\mathbb{N}^n} g_a t^a = \sum_{a\in\mathbb{N}^n} h_a t^a$$

if

1) there exist integers $\{d_a : a \in \mathbb{N}^n\}$ so that $d_a = 0$ if any component of a is zero, and
2) for all $a \in \mathbb{N}^n$ we have: $\sum_{b+c=a} f_b g_c + d_a = h_a + 2d_{a+1^n}$.

This is not simply multiplication along the diagonals. In contrast, let

$$\mathbb{Z}[[t_1, \cdots, t_n]] = \left\{ \sum_{\substack{a=(a_1,\cdots,a_n),\\ a_j\in\mathbb{N}}} c_a t_1^{a_1} \cdots t_n^{a_n} : c_a \in \mathbb{Z} \right\},$$

be the power series ring in n variables over the integers. In this ring the t_i are treated as variables and are added and multiplied as for polynomials (with no carry).

Theorem 1: The ring R_n is isomorphic to the quotient ring

$$S_n = \mathbb{Z}[[t_1, \cdots, t_n]]/(t_1 t_2 \cdots t_n - 2). \tag{5}$$

Proof: In the ring $S_n = \mathbb{Z}[[t_1, \cdots, t_n]]/(t_1 t_2 \cdots t_n - 2)$ we may write $2 = t_1 t_2 \cdots t_n$ and hence $-1 = \sum_{i=0}^{\infty} (t_1 \cdots t_n)^i$. Therefore any element $f \in S_n$ can be written uniquely as a formal power series

$$f = \sum_{a=(a_1,\cdots,a_n)} f_a t_1^{a_1} \cdots t_n^{a_n} \tag{6}$$

where $a \in \mathbb{N}^n$ and where each coefficient $f_a \in \{0, 1\}$. Such an element f may, in turn, be identified with a Boolean function $\mathbf{f} : V_n \to \{0, 1\}$ by $\mathbf{f}(a_1, \cdots, a_n) = f_{(a_1,\cdots,a_n)}$. In this way we have established a one to one correspondence $S_n \leftrightarrow R_n$. We claim that this correspondence is a homomorphism of rings (and hence is an isomorphism). In fact, if we add two elements $\mathbf{f}, \mathbf{g} \in R_n$ as elements in R_n and compare this to the sum $f+g$ as elements in $\mathbb{Z}[[t_1, \cdots, t_n]]$ we find that these differ by a multiple of $(2 - t_1 \cdots t_n)$, which is to say that the one to one correspondence is an additive homomorphism. The same argument proves that it is also a multiplicative homomorphism. □

Corollary 1: The addition and multiplication operations defined above make R_n into a commutative ring. The zero (additive identity) is the element $z \in R_n$ with $z_a = 0$ for all a, and the one (multiplicative identity) is the element $e \in R_n$ with $e_{0,0,\cdots,0} = 1$ and $e_a = 0$ if $a \neq 0^n$.

Another way to organize the sum (6) is to group the terms that occur along each diagonal D_a of equation (4). For fixed $a \in \mathbb{N}^n$ lying on one of the coordinate hyperplanes, in the ring S_n, the sum of terms in the diagonal D_a defines a 2-adic integer

$$\begin{aligned} \overline{f}(a) &= \sum_{i=0}^{\infty} \mathbf{f}(a + i(1, 1, \cdots, 1))(t_1 \cdots t_n)^i \\ &= \sum_{i=0}^{\infty} \mathbf{f}(a + i(1, 1, \cdots, 1))2^i. \end{aligned} \tag{7}$$

In this way we have constructed a one to one correspondence between Boolean functions $\mathbf{f} \in R_n$ and functions $\overline{f} : \mathcal{H} \to \mathbb{Z}_2$ where

$$\mathcal{H} = \{(a_1, \cdots, a_n) \in \mathbb{N}^n : \quad \text{some } a_i = 0.\}$$

denotes the union of the coordinate hyperplanes. We refer to $\bar{f}(a)$ as the *restriction* of f to the diagonal D_a. The same notation and terminology will be used even if a does not have a zero component.

It is important to note that the set P_n of elements of R_n that have period 2 in all directions is not a subring of R_n. In fact the sum and difference of elements of P_n may not be in P_n. However, since addition is just 2-adic addition on each diagonal, and the sum of two periodic 2-adic integers is eventually periodic (i.e., periodic beyond some point), the sum and difference of two elements of P_n are ultimately periodic along each diagonal. Moreover, the set of restrictions to diagonals are periodic (that is, the restriction of an element $\mathbf{f} \in P_n$ to a diagonal D_a is the same as the restriction of $\mathbf{f}$ to D_{a+2b} for any $b \in V_n$). Thus if $\mathbf{f}, \mathbf{g} \in P_n$, then $\mathbf{f} + \mathbf{g}$ and $\mathbf{f} - \mathbf{g}$ (where the sum and difference of $\mathbf{f}$ and $\mathbf{g}$ are in the ring R_n) are eventually 2-periodic in the following sense.

Definition 1: The element $\mathbf{f} \in R_n$ is eventually p-periodic if there is an integer k so that if $a = (a_1, \cdots, a_n) \in \mathbb{N}^n$, and $a_i \geq k$ for $i = 1, \cdots, n$, then for every $b \in \mathbb{N}^n$, $\mathbf{f}(a + pb) = \mathbf{f}(a)$. If $a = (a_1, \cdots, a_n) \in \mathbb{N}^n$, and $a_i \geq k$ for $i = 1, \cdots, n$, then the restriction of $\mathbf{f}$ to the set $\{a + b : b = (b_1, \cdots, b_n), 0 \leq b_i < p, i = 1, \cdots, n\}$ is called a *complete period* of $\mathbf{f}$.

If $p = 2$, then it is possible to take $k = 2$ in the above Definition 1. For, if $\mathbf{f} = \sum_{i=0}^{\infty} f_i 2^i$ and $\mathbf{g} = \sum_{i=0}^{\infty} g_i 2^i$ is a pair of 2-adic integers whose coefficient sequences have period 2, then the coefficient sequences of $-\mathbf{f}$, $\mathbf{f} + \mathbf{g}$, and $\mathbf{f} - \mathbf{g}$ are periodic from the coefficients with index 2 on. Tables I, II, and III show the first four coefficients of the negation of $\mathbf{f}$ and the sum and difference $\mathbf{f} + \mathbf{g}$ and $\mathbf{f} - \mathbf{g}$ for all possible combinations of periodic 2-adic integers with period 2.

$\mathbf{f}$	$-\mathbf{f}$
00	0000
01	0110
10	1101
11	1000

TABLE I
NEGATION OF A 2-PERIODIC 2-ADIC INTEGER.

$\mathbf{f}+\mathbf{g}$	00	01	10	11
00	0000	0101	1010	1111
01	0101	0010	1111	1001
10	1010	1111	0101	0010
11	1111	1001	0010	0111

TABLE II
SUM OF 2-PERIODIC 2-ADIC INTEGERS.

$\mathbf{f}-\mathbf{g}$	00	01	10	11
00	0000	0110	1101	1000
01	0101	0000	1010	1101
10	1010	1101	0000	0110
11	1111	1010	0101	0000

TABLE III
DIFFERENCE OF 2-PERIODIC 2-ADIC INTEGERS.

The possibilities for $\mathbf{f}$ and $\mathbf{g}$ are given by the first two coefficients of each. In the second and third tables, the various $\mathbf{f}$s are listed down the left hand side and the various $\mathbf{g}$s are listed across the top. For each table entry, the last two bits are repeated periodically.

Let us return to the case of R_n, and suppose that $\mathbf{f} : \mathbb{N} \to \{0, 1\}$ is strictly 2-periodic. Then in the representation in equation (7) we have

$$\begin{aligned} \bar{f}(a) &= \sum_{i=0}^{\infty} \mathbf{f}(a + i \cdot 1^n) 2^i \\ &= f(a) + f(a + 1^n)2 + f(a)2^2 \\ &\quad + f(a + 1^n)2^3 + \cdots \\ &= -\frac{f(a) + 2f(a + 1^n)}{3}. \end{aligned} \tag{8}$$

III. ARITHMETIC CORRELATIONS AND WALSH TRANSFORMS

Now we can define the arithmetic correlations and Walsh transforms. First note that when defining classical correlation functions (equation (2)) and Walsh-Hadamard transforms (equation(3)) of binary valued functions, we can we can replace the plus sign by a minus and the result will be unchanged. However, when these concepts are generalized to N-ary valued functions, $N > 2$, the sign matters and it becomes apparent that a minus sign is needed are needed. For example, the unshifted cross-correlation of a function with itself is 2^n is we use a minus sign, but has various values if we use a plus sign. This is the point of view we use here. First we extend the notion of imbalance to eventually 2-periodic elements.

Definition 2: Let $\mathbf{f} \in R_n$ be eventually p-periodic. Then the *imbalance* of $\mathbf{f}$ is

$$Z(\mathbf{f}) = \sum_a (-1)^{\mathbf{f}(a)},$$

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

Note that $Z(\mathbf{f})$ is independent of the choice of complete period. This definition is consistent with the definition of the imbalance of Boolean functions in the sense that the imbalance of a Boolean function equals the imbalance of its periodic extension to $\mathbb{N}^n$.

Definition 3: The *arithmetic cross-correlation* of two eventually periodic functions $\mathbf{f}$ and $\mathbf{g}$ in R_n is

the real number $C^a_{\mathbf{f},\mathbf{g}} \in \mathbb{R}$ defined by

$$C^a_{\mathbf{f},\mathbf{g}} = Z(\mathbf{f} - \mathbf{g}).$$

If f and g are two Boolean functions on V_n, then the *arithmetic cross-correlation* of f and g is the real valued function $C^a_{f,g} : \mathbb{N}^n \to \mathbb{R}$ defined by

$$C^a_{f,g}(a) = C^a_{\mathbf{f},\mathbf{g}_a}$$

where $\mathbf{f}$ is the extension of f and $\mathbf{g}_a$ is the extension of g_a. The *arithmetic autocorrelation* of f is

$$A^a_f(b) = C^a_{f,f}(b).$$

In defining $\mathbf{g}_a$ it doesn't matter whether we translate by a and then extend to $\mathbb{N}^n$ or extend to $\mathbb{N}^n$ and then translate by a. A linear function is a Boolean function T_a, $a \in V_n$, where $T_a(b) = [a \cdot b]_2$. Thus the extension $\mathbf{T}_a$ is also defined by $\mathbf{T}_a(b) = [a \cdot b]_2$ for $b \in \mathbb{N}^n$.

Definition 4: The *arithmetic Walsh transform* of an eventually periodic $\mathbf{f} \in R_n$ is the real valued function $\widetilde{\mathbf{f}} : V_n \to \mathbb{R}$ defined by

$$\widetilde{\mathbf{f}}(a) = Z(\mathbf{f} - \mathbf{T}_a).$$

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, $\widetilde{f}(a) = \widetilde{\mathbf{f}}(a)$. The list of values $\langle \cdots, \widetilde{f}(b), \cdots \rangle$, $b \in V_n$, is the *arithmetic Walsh spectrum of* f. Each $\widetilde{f}(b)$ is an *arithmetic Walsh coefficient*.

We want to use the representation in equations (7) and (8) to compute correlations. Let

$$U_n = \{a = (a_1, \cdots, a_n) : a_i \in \{0, 1\} \text{ and } a_1 = 0\}.$$

The restriction of an eventually periodic function $\mathbf{f} \in R_n$ to a diagonal D_a with $a \in U_n$ is eventually periodic. If we select one full period from each of these diagonals, altogether we will have one complete period of $\mathbf{f}$. It follows that the imbalance of $\mathbf{f}$ is the sum of the imbalances of the restrictions of $\mathbf{f}$ to the diagonals. The imbalance of the restriction of $\mathbf{f}$ to diagonal D_a in turn is the imbalance of the 2-adic integer $\bar{f}(a)$ (defined in equation (7)). This then is the imbalance of the 2-adic representation of the rational number in equation (8). Thus

$$Z(f) = \sum_{a \in U_n} Z(\bar{f}(a)). \tag{9}$$

Theorem 2: Let $f : V_n \to \mathbb{F}_2$ be a Boolean function. If $[b \cdot 1^n]_2 = 0$, then

$$\begin{aligned}
\widetilde{f}(b) &= \sum_{a \in U_n} 2(1 - f(a) - f(a + 1^n) \\
&\quad +2f(a)f(a + 1^n)[a \cdot b]_2) \\
&= 2^n - 2 \sum_{a \in V_n} f(a) \\
&\quad +4 \sum_{a \in U_n} f(a)f(a + 1^n)[a \cdot b]_2 \qquad (10) \\
&= 2^n - 2 \sum_{a \in V_n} f(a) \\
&\quad +2 \sum_{a \in V_n} f(a)f(a + 1^n)[a \cdot b]_2 \qquad (11)
\end{aligned}$$

If $[b \cdot 1^n]_2 = 1$, then

$$\begin{aligned}
\widetilde{f}(b) &= 2 \sum_{a \in U_n} (f(a + 1^n) - f(a)f(a + 1^n) \\
&\quad +(f(a) - f(a + 1^n))[a \cdot b]_2) \qquad (12) \\
&= \sum_{a \in V_n} (f(a + 1^n) - f(a)f(a + 1^n) \\
&\quad +(f(a) - f(a + 1^n))[a \cdot b]_2). \qquad (13)
\end{aligned}$$

Proof: If $[b \cdot 1^n]_2 = 0$, then $[(a + 1^n) \cdot b]_2 = [a \cdot b]_2$, while if $[b \cdot 1^n]_2 = 1$, then $[(a + 1^n) \cdot b]_2 = [a \cdot b]_2 + 1 \mod 2 = 1 - [a \cdot b]_2$. Let $\omega = f(a) + 2f(a + 1^n) - [a \cdot b]_2 - 2[(a + 1^n) \cdot b]_2$. It then follows from the discussion above that

$$\widetilde{f}(b) = \sum_{a \in U_n} Z((\bar{f} - \bar{T}_b)(a)) = \sum_{a \in U_n} Z\left(\frac{-\omega}{3}\right)$$

Thus

$$\widetilde{f}(b) = \sum_{a \in U_n} Z\left(-\frac{f(a) + 2f(a + 1^n)}{3} + [a \cdot b]_2\right)$$

if $[b \cdot 1^n]_2 = 0$, while

$$\widetilde{f}(b) = \sum_{a \in U_n} Z\left(-\frac{f(a) + 2f(a + 1^n) + [a \cdot b]_2 - 2}{3}\right)$$

if $[b \cdot 1^n]_2 = 1$.

If u is an integer, then the 2-adic expansion of $u/3$ is eventually periodic with period dividing 2. If u is not a multiple of 3, the each period equals 10 or 01. In this case the imbalance of $u/3$ is 0. If u is a multiple

of 3, then the eventual period is 1 and each period is either 1 (if u is negative) or 0 (if u is nonnegative). The imbalance of $u/3$ is thus -2 if u is negative and is 2 if u is nonnegative. Let $Z_a = Z((\bar{f} - \bar{T}_b)(a))$.

For $[b \cdot 1^n]_2 = 0$, we have the following table of values:

$f(a)$	$f(a+1^n)$	$[a \cdot b]_2$	Z_a
0	0	0	2
1	0	0	0
0	1	0	0
1	1	0	-2
0	0	1	2
1	0	1	0
0	1	1	0
1	1	1	2

Using Lagrange interpolation we find that

$$Z_a = 2(1 - f(a) - f(a+1^n) + 2f(a)f(a+1^n)[a \cdot b]_2).$$

For $[b \cdot 1^n]_2 = 1$, we have the following table of values:

$f(a)$	$f(a+1^n)$	$[a \cdot b]_2$	Z_a
0	0	0	0
1	0	0	0
0	1	0	2
1	1	0	0
0	0	1	0
1	0	1	2
0	1	1	0
1	1	1	0

Using Lagrange interpolation we find that

$$\begin{aligned} Z_a &= 2(f(a+1^n) - f(a)f(a+1^n) \\ &\quad +(f(a) - f(a+1^n))[a \cdot b]_2). \end{aligned}$$

This definition makes sense for $a \notin U_n$ as well. It can be checked that $Z_a = Z_{a+1^n}$. Thus the last equality holds. This proves the theorem. □

Corollary 2: If f is a Boolean function on V_n, and $[b \cdot 1^n]_2 = 0$, then $\widetilde{f}(b)$ is even.

Corollary 3: Let $L : V_n \to V_n$ be a nonsingular $\mathbb{F}_2$-linear transformation such that $L(1^n) = 1^n$. Let f be a Boolean function on V_n. Then the set of arithmetic Walsh coefficients of f is invariant under composition with L. That is,

$$\{\widetilde{f}(b) : b \in V_n\} = \{\widetilde{(f \circ L)}(b) : b \in V_n\}.$$

Proof: Note that if $a \in V_n$, then $L(a+1^n) = L(a) + L(1^n) = L(a) + 1^n$. Let M denote the representation of L as a matrix using the standard basis of V_n. Thus $L(a) = aM$. For any matrix N let N^t denote the transpose of N. Then for any $a, b \in V_n$, we have $[a \cdot b]_2 = ab^t$. We claim that for any $b \in V_n$, $\widetilde{(f \circ L)}(b) = \widetilde{f}(b(M^{-1})^t)$.

Suppose that $[b \cdot 1^n]_2 = 0$. Then by equation (11),

$$\begin{aligned} &\widetilde{(f \circ L)}(b) \\ &= 2^n - 2 \sum_{a \in V_n} f(L(a)) \\ &\quad +2 \sum_{a \in V_n} f(L(a)) f(L(a+1^n))[a \cdot b]_2 \\ &= 2^n - 2 \sum_{a \in V_n} f(L(a)) \\ &\quad +2 \sum_{a \in V_n} f(L(a)) f(L(a)+1^n)[ab^t]_2 \\ &= 2^n - 2 \sum_{a \in V_n} f(L(a)) \\ &\quad +2 \sum_{a \in V_n} f(L(a)) f(L(a)+1^n)[aMM^{-1}b^t]_2 \\ &= 2^n - 2 \sum_{a \in V_n} f(L(a)) \\ &\quad +2 \sum_{a \in V_n} f(L(a)) f(L(a)+1^n)[L(a) \cdot b(M^{-1})^t]_2 \\ &= 2^n - 2 \sum_{a \in V_n} f(a) \\ &\quad +2 \sum_{a \in V_n} f(a) f(a+1^n)[a \cdot b(M^{-1})^t]_2 \\ &= \widetilde{f}(b(M^{-1})^t), \end{aligned}$$

where the penultimate line holds because L is a permutation. Moreover,

$$\begin{aligned} b(M^{-1})^t \cdot 1^n &= b(M^{-1})^t (1^n)^t = b(1^n M)^t \\ &= b(1^n)^t = [b \cdot 1^n]_2, \end{aligned}$$

so this is the correct expression for $\widetilde{f}(b(M^{-1})^t)$. This proves the claim in this case. A similar argument works when $[b \cdot 1^n]_2 = 1$. □

A. Relation to Metrics

Let us return for a moment to the classical case of Boolean functions and Walsh-Hadamard transforms. If f and g are Boolean functions, then the distance between f and g is

$$\delta(f,g) = |\{a \in V_n : f(a) \neq g(a)\}|.$$

This is a true distance measure. It is well-known that $Z(f-g) = 2^n - 2\delta(f,g)$, or equivalently

$$\delta(f,g) = \frac{2^n - Z(f-g)}{2}. \tag{14}$$

In particular, $Z(f-g) = 2^n$ if and only if $\delta(f,g) = 0$ if and only if $f = g$. Also, $Z(f-g) = -2^n$ if and only if f is the complement of g. Thus f has a Walsh-Hadamard coefficient equal to 2^n if and only if f is linear, and has a Walsh-Hadamard coefficient equal to -2^n if and only if f is affine and nonlinear.

Now we return to the arithmetic case. Let f and g be Boolean functions and let $\mathbf{f}$ and $\mathbf{g}$ be their extensions. Let us see how we can have $Z(\mathbf{f}-\mathbf{g}) = 2^n$. From equation (9) this is equivalent to having $Z(\bar{f}(a) - \bar{g}(a)) = 2$ for every $a \in U_n$. That is,

$$Z\left(\frac{g(a) - f(a) + 2(g(a+1^n) - f(a+1^n))}{3}\right) = 2.$$

This holds if and only if either (1) $f(a) = g(a)$ and $f(a+1^n) = g(a+1^n)$ or (2) $g(a) = g(a+1^n) = 1$ and $f(a) = f(a+1^n) = 0$. Thus $Z(\mathbf{f}-\mathbf{g}) = 2^n$ if and only if g is obtained from f by choosing some elements $X \subseteq U_n$ so that f is 0 on the diagonal determined by each $a \in X$ and changing the value on these diagonals to 1. Alternatively, if and only if f is obtained from g by choosing some elements $Y \subseteq U_n$ so that g is 1 on the diagonal determined by each $a \in Y$ and changing the value on these diagonals to 0.

Now suppose g is a linear function, say $g(a) = [a \cdot b]_2$, $b \neq 0^n$. The function g is constant on some diagonal if and only if $g(1^n) = 0$. In this case g is 1 on exactly 2^{n-2} diagonals, so there are $2^{2^{n-2}} - 1$ nonlinear functions f that arise from g as in the previous paragraph so that $\widetilde{f}(b) = 2^n$.

Recall the definition of a *metric* or *distance function*.

Definition 5: Let S be a set. A function $d : S \times S \to \mathbb{R}$ is a metric if for all $a, b, c \in S$ (1) $d(a,b) \geq 0$; (2) $d(a,b) = 0$ if and only if $a = b$; (3) $d(a,b) = d(b,a)$; and (4) $d(a,c) \leq d(a,b) + d(b,c)$

Following the classical situation, we can define a function on Boolean functions by

$$\widetilde{\delta}(f,g) = \frac{2^n - Z(\mathbf{f}-\mathbf{g})}{2}.$$

unlike the classical situation, this is not a metric: if g is linear as above then there are $2^{2^{n-2}}$ functions f with $\widetilde{\delta}(f,g) = 0$. Also, δ is not symmetric. For example, let g be the Boolean function that is 1 at all points and let f be the Boolean function that is 0 at all points. Then as above $\widetilde{\delta}(f,g) = 0$. But on each diagonal D_a, g's value is the 2-adic number -1, so $Z(\mathbf{g}-\mathbf{f}) = Z(\mathbf{g}) = -2^n$. Thus $\widetilde{\delta}(f,g) = 2^n$.

However, any function $\delta(f,g)$ can be made symmetric by adding $\widetilde{\delta}(f,g)$ and $\widetilde{\delta}(g,f)$.

Theorem 3: The function $d(f,g) = \widetilde{\delta}(f,g) + \widetilde{\delta}(g,f)$ is a metric on the set of Boolean functions on V_n.

Proof: We have

$$\begin{aligned} & 2(\widetilde{\delta}(f,g) + \widetilde{\delta}(g,f)) \\ &= 2^{n+1} - Z(\mathbf{f}-\mathbf{g}) - Z(\mathbf{f}-\mathbf{g}) \\ &= \sum_{a \in U_n} 4 - Z(\bar{f}(a) - \bar{g}(a)) \\ &\quad - Z(\bar{g}(a) - \bar{f}(a)). \end{aligned} \tag{15}$$

We now consider the contribution from each $a \in U_n$. On each diagonal D_a, we have $\bar{f}(a), \bar{g}(a) \in \{-1, -2/3, -1/3, 0\}$. Then $\bar{f}(a) - \bar{g}(a)$ is given by Table IV, where the possible values of $\bar{f}(a)$ are listed down the right hand side and the possible values of $\bar{g}(a)$ are listed across the top.

	-1	$-2/3$	$-1/3$	0
-1	0	$-1/3$	$-2/3$	-1
$-2/3$	$1/3$	0	$-1/3$	$-2/3$
$-1/3$	$2/3$	$1/3$	0	$-1/3$
0	1	$2/3$	$1/3$	0

TABLE IV
VALUES OF $\bar{f}(a) - \bar{g}(a)$.

The corresponding values of $Z(\bar{f}(a) - \bar{g}(a))$ are given in Table V. The value of $Z(\bar{f}(a) - \bar{g}(a)) +$

	-1	$-2/3$	$-1/3$	0
-1	2	0	0	-2
$-2/3$	0	2	0	0
$-1/3$	0	0	2	0
0	2	0	0	2

TABLE V
VALUES OF $Z(\bar{f}(a) - \bar{g}(a))$.

$Z(\bar{g}(a) - \bar{f}(a))$ is then one of the entries in the sum of Table V and its transpose. All these entries are 0 or 4, with 4 appearing if and only if $\bar{f}(a) = \bar{g}(a)$. Thus the contribution from diagonal D_a to equation (15) is 0 or 4, with 0 occurring if and only if $\bar{f}(a) = \bar{g}(a)$.

We can associate with a Boolean function f a vector v_f indexed by U_n whose entry indexed by $a \in U_n$ is the pair $(f(a), f(a + 1^n))$. For vectors $u, v \in \{(0,0),(0,1),(1,0),(1,1)\}$ indexed by U_n, let $d_H(u, v)$ be the usual Hamming distance on a four element alphabet. Then the above analysis shows that $d(f, g) = 2d_H(v_f, v_g)$. Since the Hamming distance is a metric, it is immediate that d is a metric. □

B. Nonlinearity

In the classical theory of Boolean functions one defines the *nonlinearity* $nl(f)$ of a Boolean function f to be the minimum Hamming distance from $f(a)$ to an affine function $g(a)+c$, with $g(a) = [b \cdot a]_2$ linear. From equation (14) we see that

$$nl(f) = \frac{2^n - \min|\hat{f}(b)|}{2}.$$

By analogy, we could define the *arithmetic nonlinearity* by

$$anl(f) = \frac{2^n - \min|\tilde{f}(b)|}{2}.$$

In Section III-A we saw that if $b \in V_n$, $[b \cdot 1^n]_2 = 0$, and $g(a) = [b \cdot 1^n]_2$, then g is constant on the diagonals. Furthermore, if we pick any set of diagonals on which g is constant one and change it to constant zero on these diagonals, then we will have a function f with $|\tilde{f}(b)| = 2^n$. Thus $anl(f) = 0$. If we do this for $n-3$ diagonals, then $d(f, g) = 2^{n-2}$. Thus we have a Boolean function with large nonlinearity but zero arithmetic nonlinearity.

IV. COMPUTING ARITHMETIC CORRELATIONS

Let f be a Boolean function. In this section we use equations (7) and (8) to compute the arithmetic correlations of f. Surprisingly, we see that all arithmetic autocorrelations are nonnegative.

As before, we let $U_n = \{a = (a_1, a_2, \cdots, a_n) \in V_n : a_1 = 0\}$.

A. Arithmetic Autocorrelations

Suppose first that $b \in U_n$. Then $a + b \in U_n$ if and only if $a \in U_n$. If $b = 0^n$, then $A_f^a(b) = 2^n$. Now assume that $b \neq 0^n$. Let $\Delta(a, b) = f(a+b) - f(a) + (f(a+b+1^n) - f(a+1^n))2$. Using arguments similar to those in Section III, the arithmetic autocorrelation of f with shift $a \in V_n$ is

$$A_f^a(b) = \sum_{a \in U_n} Z\left(\frac{\Delta(a, b)}{3}\right). \tag{16}$$

Then for any $a \in U_n$, both terms in

$$Z_a = Z\left(\frac{\Delta(a, b)}{3}\right) + Z\left(\frac{\Delta(a+b, b)}{3}\right) \tag{17}$$

appear in equation (16). The sum depends on $f(a)$, $f(a+1^n)$, $f(a+b)$, and $f(a+b+1^n)$, and no other terms in equation (16) depend on these values. We want to determine Z_a in terms of these four values.

The numerators of the two terms are negatives of each other, so one numerator is divisible by three if and only if the other is. If neither is a multiple of three, then both imbalances are zero. If either numerator is positive, then the other is negative so the imbalances are negatives of each other. Thus the only nonzero contribution to $A_f^a(b)$ is from those as for which $f(a+b) - f(a) + (f(a+b+1^n) - f(a+1^n))2 = 0$. This happens exactly when $f(a) = f(a+b)$ and $f(a+1^n) = f(a+b+1^n)$, and then the two imbalances add to 4. We account for each term once if we sum just over all $a < a + b$ (say in lexicographic order).

Thus

$$\begin{aligned} A_f^a(b) &= 4|\{a \in U_n : a < a+b, f(a) = f(a+b), \\ &\quad \text{and } f(a+1^n) = f(a+b+1^n)\}| \\ &= 2|\{a \in U_n : f(a) = f(a+b), \text{ and} \\ &\quad f(a+1^n) = f(a+b+1^n)\}| \\ &= |\{a \in V_n : f(a) = f(a+b), \text{ and} \\ &\quad f(a+1^n) = f(a+b+1^n)\}|. \end{aligned} \tag{18}$$

This expression is also correct when $b = 0^n$.

Now suppose that $b \in V_n - U_n$. If $b = 1^n$, then $a+b = a+1^n$ and $a+b+1^n = a$. Thus the contribution from the term corresponding to any $a \in U_n$ is

$$\begin{aligned} Z\left(\frac{\Delta(a,1^n)}{3}\right) &= Z\left(\frac{f(a) - f(a+1^n)}{3}\right) \\ &= \begin{cases} 2 & \text{if } f(a) = f(a+1^n) \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Thus

$$\begin{aligned} A_f^a(b) &= 2|\{a \in U_n : f(a) = f(a+1^n)\}| \\ &= |\{a \in V_n : f(a) = f(a+1^n)\}|. \end{aligned}$$

Equation (18) agrees with this value when $b = 1^n$.

Lastly, let $b \in V_n - U_n$ and $b \neq 1^n$. Then for any $a \in U_n$, both terms in

$$\begin{aligned} Z_a &= Z\left(\frac{\Delta(a,b)}{3}\right) \\ &\quad + Z\left(\frac{\Delta(a+b+1^n,b)}{3}\right) \end{aligned} \tag{19}$$

appear in equation (16). The sum depends on $f(a)$, $f(a+1^n)$, $f(a+b)$, and $f(a+b+1^n)$, and no other terms depend on these values. Let u and v denote the numerators of the two terms. Then $-2v = u + 3(f(a)-f(a+b))$. Thus v is divisible by 3 if and only if u is divisible by 3. If u and v are not divisible by 3 then both terms contribute 0 to the autocorrelation. Suppose u and v are divisible by 3. Note that $f(a) - f(a+b) \in \{-1, 0, 1\}$. We have $u = 0$ if and only if $f(a) = f(a+b)$ and $f(a+1^n) = f(a+b+1^n)$, and this holds if and only if $v = 0$. If $u > 0$ then $u \geq 3$ and so $-2v = u + 3(f(a) - f(a+1^n)) \geq 0$. Thus $v \leq 0$. But $u > 0$ implies $v \neq 0$, so $v < 0$. Conversely, if $v < 0$ then $v \leq -3$ so $6 \leq -2v = u+3(f(a)-f(a+b))$ which implies $u \geq 3 > 0$. Thus u and v have opposite signs. It follows that the two terms cancel unless $f(a) = f(a+b)$ and $f(a+1^n) = f(a+b+1^n)$. We obtain the same expression for $A_f^a(b)$. We summarize this analysis in the following theorem

Theorem 4: If f is any Boolean function on n variables and $b \in V_n$, then

$$\begin{aligned} A_f^a(b) &= |\{a \in V_n : f(a) = f(a+b), \text{ and} \\ &\quad f(a+1^n) = f(a+b+1^n)\}|. \end{aligned}$$

In particular, $A_f^a(b) \geq 0$.

One way to understand this is to define a new function f^2 with values in $\mathbb{Z}^2$ by $f^2(a) = (f(a), f(a+1^n))$. Then $A_f^a(b) = |\{a \in V_n : f^2(a) = f^2(a+b)\}|$.

B. Avalanche Criteria

In the classical theory of Boolean functions for cryptography, one important criterion for randomness is the *strict avalanche criterion*. This says that if we change a single bit of input to a Boolean function f, it should change the output half the time. This can be said more precisely by saying that the function $f(a) + f(a+b)$ is balanced if b has weight 1. More generally, we say that f has the strict avalanche condition of degree k if $f(a) + f(a+b)$ is balanced for every b with weight greater than 0 and less than or equal to k. That is, f and its translate by b are independent. It is straightforward to see that this is equivalent to saying that the autocorrelation $A_f(b)$ is zero for such b.

We would like to find an arithmetic analog of the strict avalanche criterion. As a first attempt, one might ask that the arithmetic autocorrelation $A_f^a(b)$ be zero if b has weight greater than 0 and less than or equal to k. But this does not correctly capture a notion of randomness. In fact if f and its translate by b are independent, then we expect the condition $f^2(a) = f^2(a+b)$ from Section IV-A to hold one quarter of the time. By contrast, $A_f^a(b) = 0$ only if $f^2(a) \neq f^2(a+b)$ for every a. These considerations lead to the following definition.

Definition 6: A Boolean function satisfies the *arithmetic propagation criterion of degree k* (or APC(k)) if and only if $A_f^a(b) = 2^{n-2}$ for every b with Hamming

weight $1 \le \mathrm{wt}(b) \le k$. If $k = 1$, we simply say f satisfies the *arithmetic avalanche criterion* (or AAC).

This is equivalent to saying that for every b of weight 1, the function $f^2(a) + f^2(a+b)$ takes the value $(0,0)$ a quarter of the time.

Various questions can be asked relating to functions satisfying APC(k). How can we construct functions with the APC(k)? How many functions satisfy the APC(k)? Are there functions that satisfy SAC to a high order but AAC to only a low order, and vice versa? Is a Boolean function that doesn't satisfy the AAC susceptible to cryptanalysis?

n	functions	SAC only	AAC only	SAC and AAC
2	2^4	$4 = 2^2$	0	0
3	2^8	$64 = 2^6$	0	0
4	2^{16}	$\sim 2^{11.3}$	$\sim 2^{10.4}$	$\sim 2^{10.6}$
5	2^{32}	$\sim 2^{24.6}$	$\sim 2^{23.7}$	$\sim 2^{20.9}$

TABLE VI
THE NUMBERS OF SAC AND AAC FUNCTIONS FOR SMALL n.

The numbers of Boolean functions satisfying SAC and AAC for small dimensions (derived experimentally) are given in Table VI. The third column gives the number of functions satisfying SAC but not AAC, the fourth column gives the number of functions satisfying AAC but not SAC, and the fifth column gives the number of functions satisfying both SAC and AAC. It is hard to draw any conclusions from such scant data, but it appears from dimension $n = 5$ that the two criteria are largely independent. Checking all Boolean functions of dimension 6 for the SAC or ACC is beyond our computational capabilities at the moment (there are 2^{64} functions to check). Let S_n be the log base 2 of the number of Boolean functions of dimension n satisfying SAC. It is known that $S_n \ge 2^{n-1}$ [2], [13] and that the limit of $S_n/2^n$ as n tends to infinity is 1 [1]. We leave a similar analysis of the number of Boolean functions satisfying AAC as well as the above questions for further work.

C. Arithmetic Cross-Correlations

Now let g be a second Boolean function. Let $\Gamma(a,b) = g(a+b) - f(a) + 2(g(a+b+1^n) - f(a+1^n))$. By similar reasoning, the arithmetic cross-correlation of f with shift $a \in V_n$ is

$$C^a_{f,g}(b) = \sum_{a \in U_n} Z\left(\frac{\Gamma(a,b)}{3}\right).$$

Then for any $a \in U_n$, the term

$$Z_a = Z\left(\frac{\Gamma(a,b)}{3}\right) \tag{20}$$

depends on $f(a)$, $f(a+1^n)$, $g(a+b)$, and $g(a+b+1^n)$, and no other terms depend on these values. We want to determine equation (20) in terms of these four values.

The fraction in equation (20) has an eventually balanced 2-adic expansion if and only if the numerator is not a multiple of 3. If the numerator is a negative multiple of 3, then the expansion is eventually all 1s, so the imbalance is -2. If the numerator is 0 or a positive multiple of 3, then the expansion is eventually all 0s, so the imbalance is 2. This gives the following theorem.

Theorem 5: Let f and g be Boolean functions on n variables and let $b \in V_n$. Then

$$\begin{aligned} & C^a_{f,g}(b) \\ &= |\{a \in V_n : g(a+b) = f(a) \text{ and } \\ &\quad g(a+b+1^n) = f(a+1^n)\}| \\ &\quad + |\{a \in V_n : g(a+b) = g(a+b+1^n) = 1 \\ &\quad \text{ and } f(a) = f(a+1^n) = 0\}| \\ &\quad - |\{a \in V_n : g(a+b) = g(a+b+1^n) = 0 \\ &\quad \text{ and } f(a) = f(a+1^n) = 1\}|. \end{aligned} \tag{21}$$

This implies, for example, that if $f(a) = 0$ for all a and $g(a) = 1$ for all a, then $C^a_{f,g}(b) = 2^n$ for all b and that $C^a_{g,f}(b) = -2^n$ for all b.

If f is a Boolean function, let f' denote the complement of f. That is, $f'(a) = 1$ if and only if $f(a) = 0$, so $f'(a) = 1 - f(a)$ as integers.

Corollary 4: Let f and g be Boolean functions on n variables and let $b \in V_n$. Then for every $b \in V_n$

$$C^a_{f,g}(b) = C^a_{g',f'}(b).$$

D. Arithmetic Correlations of Linear and Affine Functions

In this section we use Theorems 4 and 5 to compute the arithmetic auto- and cross-correlations of linear

and affine functions. First consider autocorrelations. If f is constant (identically 0 or identically 1), then $A_f^a(b) = 2^n$ for all b. If f is nonzero and linear, then $f(a) = f(a+b)$ and $f(a+1^n) = f(a+b+1^n)$ if and only if $f(b) = 0$. Similarly, if f is affine but not linear, then $f(x) = 1 - h(x)$ with h linear, and these equations hold if and only if $h(b) = 0$. Thus in either case

$$A_f^a(b) = \begin{cases} 2^n & \text{if } f(b) = 0 \\ 0 & \text{otherwise.} \end{cases}$$

We can compare this to the classical autocorrelations, where if f is affine, then

$$A_f(b) = \begin{cases} 2^n & \text{if } f(b) = 0 \\ -2^n & \text{otherwise.} \end{cases}$$

Now let us consider the cross-correlation. Let f and g be linear or affine. Then the sets in the last two terms of equation (21) are solutions to inhomogeneous systems of degree 1 equations. In the two sets the homogeneous parts of the equations are the same. It is only the constant terms that differ. It follows that the numbers of solutions are the same for both systems, depending only on the rank of the homogeneous part, and they cancel each other. Thus for linear and affine functions $C_{f,g}^a(b)$ is the number of $a \in V_n$ such that

$$g(a+b) = f(a) \tag{22}$$

and

$$g(a+b+1^n) = f(a+1^n). \tag{23}$$

Let $f(a) = f_1(a) + c \mod 2$ and $g(a) = g_1(a) + d \mod 2$, where f_1 and g_1 are linear and $c, d \in \{0,1\}$. Then equations (22) and (23) hold if and only equation (22) and

$$g_1(1^n) = f_1(1^n) \tag{24}$$

hold. Thus if equation (24) does not hold, then $C_{f,g}^a(b) = 0$. Otherwise $C_{f,g}^a(b)$ is the number of $a \in V_n$ such that equation (22) holds.

Suppose equation (24) holds. If $f_1 \neq g_1$, then equation (22) is a rank one affine equation, so it holds for 2^{n-1} values of a. If f and g are equal and constant (i.e., $f_1 = g_1 = 0$ and $c = d$), then $C_{f,g}^a(b) = 2^n$. If f and g are unequal and constant, then $C_{f,g}^a(b) = 0$. If $f_1 = g_1 \neq 0$, then equation (22) holds if and only if $g(b) = f(0^n)$. That is, if and only if $g_1(b) = c - d \mod 2$. This occurs for 2^{n-1} values of b.

Theorem 6: Let $f(a) = f_1(a) + c \mod 2$ and $g(a) = g_1(a) + d \mod 2$, where f_1 and g_1 are linear and $c, d \in \{0,1\}$. If $g_1(1^n) \neq f_1(1^n)$ then $C_{f,g}^a(b) = 0$ for all b.

1) If $f_1 = g_1 = 0$ and $c = d$, then $C_{f,g}^a(b) = 2^n$ for all b.
2) If $f_1 = g_1 = 0$ and $c \neq d$, then $C_{f,g}^a(b) = 0$ for all b.
3) If $f_1 = g_1 \neq 0$, then $C_{f,g}^a(b) = 2^n$ for 2^{n-1} values of b and is 0 for 2^{n-1} values of b.
4) If $f_1 \neq g_1$ and $f_1(1^n) = g_1(1^n)$, then $C_{f,g}^a(b) = 2^{n-1}$ for all b.

By contrast, the classical cross-correlation is 0 for all b if $f_1 \neq g_1$. If $f_1 = g_1 = 0$, then it is 2^n for all b or -2^n for all b. If $f_1 = g_1 \neq 0$, then it is 2^n for 2^{n-1} values of b and is -2^n for 2^{n-1} values of b.

V. Uniqueness of Arithmetic Walsh Spectra

The arithmetic Walsh spectrum of a Boolean function is the set of its arithmetic Walsh coefficients. In this section we show that the mapping from Boolean functions to their arithmetic Walsh spectra is one to one. That is, we show that a Boolean function is uniquely determined by its arithmetic Walsh spectrum. We do not, however, know a simple expression for the inverse arithmetic Walsh transform, or even an efficient way to compute it. Nor do we know how to characterize those functions $V_n \to \mathbb{Z}$ that are the arithmetic Walsh transforms of Boolean functions.

It follows from equation (10) that if $b \neq 0^n$ and $\mathrm{wt}(b)$ is even, then

$$\sum_{a \in U_n} f(a) f(a+1^n)[a \cdot b]_2 = \frac{\widetilde{f}(b) - \widetilde{f}(0^n)}{4}. \tag{25}$$

Let M_n be the $(2^{n-1}-1) \times (2^{n-1}-1)$ rational matrix indexed by $U_n - \{0^n\}$ and $W_n = \{b \in V_n : \mathrm{wt}(b) \text{ even}, b \neq 0^n\}$ whose entry with index (a,b) is $[a \cdot b]_2$ treated as a rational number. Similarly, let N_n be the $(2^{n-1}-1) \times (2^{n-1}-1)$ rational matrix indexed by $U_n - \{0^n\}$ and $T_n = \{b \in V_n : \mathrm{wt}(b) \text{ odd}, b \neq 10^{n-1}\}$ whose entry with index (a,b) is $[a \cdot b]_2$ treated as a rational number.

Let $v(a) = f(a)f(a+1^n)$ and let v be the vector indexed by $U_n - \{0^n\}$ whose entries are the $v(a)$.

Let $z(b) = (\widetilde{f}(b) - \widetilde{f}(0^n))/4$ and let z be the vector indexed by W_n whose entries are the $z(b)$. Then equation (25) implies that $vM_n = z$. Thus if M_n is invertible, then the $v(a)$ with $a \neq 0^n$ or 1^n can be determined uniquely from the $\widetilde{f}(b)$.

Similarly, it follows from equation (12) that if $b \neq 10^{n-1}$ and $\mathrm{wt}(b)$ is odd, then

$$\sum_{a \in U_n} (f(a) - f(a + 1^n))[a \cdot b]_2 = \frac{\widetilde{f}(b) - \widetilde{f}(10^{n-1})}{2}. \tag{26}$$

Let $u(a) = f(a) - f(a + 1^n)$ and let u be the vector indexed by $U_n - \{0^n\}$ whose entries are the $u(a)$. Let $w(b) = (\widetilde{f}(b) - \widetilde{f}(10^{n-1}))/2$ and let w be the vector indexed by T_n whose entries are the $w(b)$. Then equation (26) implies that $uN_n = w$. Thus if N_n is invertible, then the $u(a)$ with $a \neq 10^{n-1}$ can be determined uniquely from the $\widetilde{f}(b)$.

Theorem 7: The matrices M_n and N_n have nonzero determinants.

Proof: We order the indices in both dimensions lexicographically, with most significant position on the right. For both types of matrices, we think of the rows (the as) as being divided into three segments:

1) The rows indexed by $a = 0a'0$ with $a' \neq 0^{n-2}$;
2) The row indexed by $a = 0^{n-1}1$; and
3) The rows indexed by $a = 0a'1$ with $a' \neq 0^{n-2}$.

For M_n, we think of the columns (the bs) as being divided into three segments:

1) The columns indexed by $b = b'0$ with $\mathrm{wt}(b')$ even and $b' \neq 0^{n-1}$;
2) The column indexed by $b = 10^{n-2}1$; and
3) The columns indexed by $b = b'1$ with $\mathrm{wt}(b')$ odd and $b' \neq 10^{n-2}$.

Similarly, for N_n, we think of the columns as being divided into three segments:

1) The columns indexed by $b = b'0$ with $\mathrm{wt}(b')$ odd;
2) The column indexed by $b = 0^{n-1}1$; and
3) The columns indexed by $b = b'1$ with $\mathrm{wt}(b')$ even and $b' \neq 0^{n-1}$.

Let $\langle 1 \rangle_n$ denote the $2^n \times 2^n$ matrix all of whose entries are 1. Following these decompositions of the indices, we can decompose M_n into blocks as follows.

1) If $a = 0a'0$ with $a' \neq 0^{n-2}$ and $b = b'0$ with $b' \neq 0^{n-1}$ and $\mathrm{wt}(b')$ even, then $[0a' \cdot b']_2 = [a \cdot b]_2$. Thus the upper left hand block of M_n equals M_{n-1}.
2) If $a = 0a'1$ with $a' \neq 0^{n-2}$ and $b = b'0$ with $b' \neq 0^{n-1}$ and $\mathrm{wt}(b)$ even, then $[0a' \cdot b']_2 = [a \cdot b]_2$. Thus the lower left hand block of M_n equals M_{n-1}.
3) If $a = 0a'0$ with $a' \neq 0^{n-2}$ and $b = b'1$ with $b' \neq 10^{n-2}$ and $\mathrm{wt}(b')$ odd, then $[0a' \cdot b']_2 = [a \cdot b]_2$. Thus the upper right hand block of M_n equals N_{n-1}.
4) If $a = 0a'1$ with $a' \neq 0^{n-2}$ and $b = b'1$ with $b' \neq 10^{n-2}$ and $\mathrm{wt}(b')$ odd, then $[0a' \cdot b']_2 = 1 - [a \cdot b]_2$. Thus the lower right hand block of M_n equals $\langle 1 \rangle_{n-1} - N_{n-1}$.
5) If $a = 0^{n-1}1$, then the row indexed by a is $0^{2^{n-1}-1}1^{2^{n-1}}$.
6) If $b = 10^{n-2}1$, then the column indexed by b is $0^{2^{n-1}-1}1^{2^{n-1}}$.

Denoting the determinant of a matrix K by $|K|$, we can summarize this by saying

$$M_n = \begin{vmatrix} & & & 0 & & & \\ & M_{n-1} & & \vdots & & N_{n-1} & \\ & & & 0 & & & \\ 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ & & & 1 & & & \\ & M_{n-1} & & \vdots & & \langle 1 \rangle_{n-1} - N_{n-1} & \\ & & & 1 & & & \end{vmatrix}$$

By subtracting the first block of rows from the last block of rows, then subtracting the row indexed by $a = 0^{n-1}1$ from each of the last block of rows, we

have

$$
\begin{aligned}
&|M_n| \\
&= \begin{vmatrix} & & & 0 & & \\ & M_{n-1} & & \vdots & & N_{n-1} \\ & & & 0 & & \\ 0 & \cdots & 0 & 1 & 1 \cdots & 1 \\ & & & 1 & & \\ & 0 & & \vdots & \langle 1\rangle_{n-1} - 2N_{n-1} & \\ & & & 1 & & \end{vmatrix} \\
&= \begin{vmatrix} & & & 0 & & \\ & M_{n-1} & & \vdots & N_{n-1} & \\ & & & 0 & & \\ 0 & \cdots & 0 & 1 & 1 \cdots & 1 \\ & & & 0 & & \\ & 0 & & \vdots & -2N_{n-1} & \\ & & & 0 & & \end{vmatrix} \\
&= 2^{2^{n-1}-1}|M_{n-1}||N_{n-1}|. \qquad (27)
\end{aligned}
$$

A similar argument gives

$$|N_n| = 2^{2^{n-1}-1}|M_{n-1}||N_{n-1}|. \qquad (28)$$

Finally, we see that M_2 and N_2 are 1×1 matrices whose single entries are 1, hence whose determinants are 1. It follows that the determinant of M_n and N_n are nonzero as claimed. □

In fact it follows from equations (27) and (28) that

$$|M_n| = |N_n| = 2^{(n-2)2^{n-1}+1},$$

but we shall not use this fact.

Corollary 5: ([7]) The values of $u(a)$ and $v(a)$ for $a \in U_n - \{0^n\}$ are uniquely determined by the $\widetilde{f}(b)$. This in turn uniquely determines the values of the $f(a)$ for $a \neq 0^n, 1^n$.

Having determined the $f(a)$ with $a \neq 0^n, 1^n$, we are left with two equations in the unknowns $f(0^n)$ and $f(1^n)$. From equation (11) with $b = 0^n$ we have

$$f(0^n) + f(1^n) = x$$

for some $x \in \mathbb{Z}$, and from equation (13) with $b = 10^{n-1}$ we have

$$f(1^n) - f(0^n)f(1^n) = y$$

for some $y \in \mathbb{Z}$. The values x and y are uniquely determined by the $\widetilde{f}(b)$.

We can make a table of possible values

$f(0^n)$	$f(1^n)$	x	y
0	0	0	0
1	0	1	0
0	1	1	1
1	1	2	0

It follows that $f(0^n)$ and $f(1^n)$ are uniquely determined by any valid value of x and y. We have proved the following theorem.

Theorem 8: Every Boolean function on V_n is uniquely determined by its arithmetic Walsh transform.

Embedded in this proof is a method of computing the function f from its arithmetic Walsh transform. It is, however, more complicated than the situation for Walsh-Hadamard transforms where one simply computes essentially the Walsh-Hadamard transform of the Walsh-Hadamard transform. We do not know of such an idempotency law for the arithmetic Walsh transform.

VI. Statistics of the Arithmetic Walsh Transform

Recall that for a Boolean function f, the mean of the Walsh-Hadamard coefficients of f is $(-1)^{f(0)}$ and the second moment is 2^n (independent of f). The picture is quite different in the arithmetic case.

Let

$$H(f) = \sum_{a \in V_n} f(a),$$

the Hamming weight of f, and let

$$Q(f) = \sum_{a \in U_n} f(a)f(a+1^n) = \frac{1}{2}\sum_{a \in V_n} f(a)f(a+1^n),$$

the number of diagonals on which f is a constant 1.

Lemma 1: If f is a Boolean function on n variables, then

$$\begin{aligned}
&\sum_{a \in V_n} f(a)f(a+1^n) \sum_{[b\cdot 1^n]_2 = 0} [a \cdot b]_2 \\
&= \quad 2^{n-1}Q(f) - 2^{n-1}f(0^n)f(1^n),
\end{aligned}$$

$$\sum_{a\in V_n}(f(a)-f(a+1^n)))\sum_{[b\cdot 1^n]_2=1}[a\cdot b]_2$$
$$= \quad 2^{n-1}(f(1^n)-f(0^n)),$$

$$\sum_{a,c\in V_n} f(a)f(a+1^n)f(c)f(c+1^n)$$
$$\cdot \sum_{[b\cdot 1^n]_2=0}[a\cdot b]_2[c\cdot b]_2$$
$$= \quad 2^{n-1}Q(f)^2+2^{n-1}Q(f)-2^n f(0^n)f(1^n)Q(f)$$
$$= \quad 2^{n-1}Q(f)(Q(f)+1-2f(0^n)f(1^n)).$$

and

$$\sum_{a,c\in V_n}(f(a)-f(a+1^n))(f(c)-f(c+1^n))$$
$$\cdot \sum_{[b\cdot 1^n]_2=1}[a\cdot b]_2[c\cdot b]_2$$
$$= \quad 2^{n-1}(H(f)-2Q(f)).$$

Proof: We prove the third equation. Proofs of the other three equations are similar.

Let

$$R_{a,c}=\sum_{[b\cdot 1^n]_2=0}[a\cdot b]_2[c\cdot b]_2.$$

Then $R_{a,c}=|\{b:[b\cdot 1^n]_2=0,[a\cdot b]_2=1,$ and $[c\cdot b]_2=1\}|$. There are several possibilities.

1) If a or c is 0^n or 1^n, then $R_{a,c}=0$.
2) If $a=c$ and $a,c\notin\{0^n,1^n\}$, then $R_{a,c}=2^{n-2}$.
3) If $a=c+1^n$ and $a,c\notin\{0^n,1^n\}$, then $R_{a,c}=2^{n-2}$.
4) Otherwise a, c, and 1^n are linearly independent modulo 2, so $R_{a,c}=2^{n-3}$.

Thus

$$\sum_{a,c\in V_n} f(a)f(a+1^n)f(c)f(c+1^n)$$
$$\cdot \sum_{[b\cdot 1^n]_2=0}[a\cdot b]_2[c\cdot b]_2$$
$$= \quad 2^{n-3}\sum_{a,c\in V_n} f(a)f(a+1^n)f(c)f(c+1^n)$$
$$+(2^{n-2}-2^{n-3})$$
$$\cdot \sum_{a\in V_n} f(a)f(a+1^n)f(a+1^n)f(a)$$
$$+(2^{n-2}-2^{n-3})$$
$$\cdot \sum_{a\in V_n} f(a)f(a+1^n)f(a)f(a+1^n)$$
$$+(-2^{n-3})\sum_{a\in V_n} f(0^n)f(1^n)f(c)f(c+1^n)$$
$$+(-2^{n-3})\sum_{a\in V_n} f(1^n)f(0^n)f(c)f(c+1^n)$$
$$+(-2^{n-3})\sum_{a\in V_n} f(a)f(a+1^n)f(0^n)f(1^n)$$
$$+(-2^{n-3})\sum_{a\in V_n} f(a)f(a+1^n)f(1^n)f(0^n)$$
$$= \quad 2^{n-1}Q(f)^2+2^{n-1}Q(f)$$
$$-2^n f(0^n)f(1^n)Q(f)$$
$$= \quad 2^{n-1}Q(f)(Q(f)+1-2f(0^n)f(1^n)).$$

Note that in the final two lines one would expect a term $f(0^n)f(1^n)$ with some coefficient, accounting for all the appearances of this term in the various sums. In fact for each of the four choices of $a,c\in\{0^n,1^n\}$ we have $[a\cdot b]_2[c\cdot b]_2=0$. Thus the coefficient of $f(0^n)f(1^n)$ is zero.

□

Theorem 9: Let f be a Boolean function on n variables. The mean arithmetic Walsh transform of f is

$$E[\widetilde{f}(b)] \quad = \quad 2^{n-1}-\frac{H(f)+f(0^n)-f(1^n)}{2}$$
$$-f(0^n)f(1^n).$$

The proof is omitted. The proof is similar to (and simpler than) the proof of Theorem 10, and a sketch has appeared previously [7].

Parseval's identity says the the sum of the squares of the Walsh-Hadamard coefficients of a Boolean function on n variables is 2^{2n}. This important fact leads, for example, to the notion of bent functions [10], [12]. Again the picture is more complicated in the arithmetic case.

Theorem 10: Let f be a Boolean function on n variables. The second moment of the arithmeticWalsh transform of f is

$$\begin{aligned} E[\widetilde{f}(b)^2] &= 2^{2n-1} + \frac{5}{2}H(f)^2 - 6H(f)Q(f) \\ &\quad +4Q(f)^2 - (2^{n+1} - \frac{1}{2} + f(0^n) \\ &\quad -f(1^n) - 4f(0^n)f(1^n))H(f) \\ &\quad +(2^{n+1} + 1 + 2f(0^n) - 2f(1^n) \\ &\quad -4f(0^n)f(1^n))Q(f) \\ &\quad -2^{n+1}f(0^n)f(1^n). \end{aligned}$$

Proof: We have

$$\begin{aligned} &E[\widetilde{f}(b)^2] \\ &= \frac{1}{2^n}\sum_{b\in V_n}\widetilde{f}(b)^2 \\ &= \frac{1}{2^n}\left(\sum_{[b\cdot 1^n]_2=0}\widetilde{f}(b)^2 + \sum_{[b\cdot 1^n]_2=1}\widetilde{f}(b)^2\right). \end{aligned}$$

We again use equations (11) and (13) to compute these two sums separately. For the first sum we have

$$\begin{aligned} \sum_{[b\cdot 1^n]_2=0}\widetilde{f}(b)^2 &= \sum_{[b\cdot 1^n]_2=0}\left(2^n - 2\sum_{a\in V_n} f(a)\right. \\ &\quad \left. +2\sum_{a\in V_n} f(a)f(a+1^n)[a\cdot b]_2\right)^2 \\ &= \sum_{[b\cdot 1^n]_2=0}\left(2^n - 2H(f)\right. \\ &\quad \left. +2\sum_{a\in V_n} f(a)f(a+1^n)[a\cdot b]_2\right)^2 \\ &= \sum_{[b\cdot 1^n]_2=0}(2^n - 2H(f))^2 \\ &\quad +4(2^n - 2H(f))\sum_{a\in V_n} f(a)f(a+1^n)[a\cdot b]_2 \\ &\quad +4\left(\sum_{a\in V_n} f(a)f(a+1^n)[a\cdot b]_2\right)^2 \\ &= 2^{n-1}(2^n - 2H(f))^2 + 4(2^n - 2H(f)) \\ &\quad \cdot\sum_{a\in V_n} f(a)f(a+1^n)\sum_{[b\cdot 1^n]_2=0}[a\cdot b]_2 \\ &\quad +4\sum_{a,c\in V_n} f(a)f(a+1^n)f(c)f(c+1^n) \\ &\quad \cdot\sum_{[b\cdot 1^n]_2=0}[a\cdot b]_2[c\cdot b]_2 \\ &= 2^{n-1}(2^n - 2H(f))^2 \\ &\quad +4(2^n - 2H(f))(2^{n-1}Q(f) \\ &\quad -2^{n-1}f(0^n)f(1^n)) \\ &\quad +4(2^{n-1}Q(f)^2 + 2^{n-1}Q(f) \\ &\quad -2^n f(0^n)f(1^n)Q(f)) \\ &= 2^{3n-1} - 2^{2n+1}H(f) + 2^{n+1}H(f)^2 \\ &\quad -2^{n+2}H(f)Q(f) + 2^{n+2}H(f)f(0^n)f(1^n) \\ &\quad +(2^{2n+1} + 2^{n+1})Q(f) - 2^{2n+1}f(0^n)f(1^n) \\ &\quad +2^{n+1}Q(f)^2 - 2^{n+2}f(0^n)f(1^n)Q(f). \end{aligned}$$

Similarly, for the second sum we have

$$\begin{aligned} &\sum_{[b\cdot 1^n]_2=1}\widetilde{f}(b)^2 \\ &= \sum_{[b\cdot 1^n]_2=1}\left(\sum_{a\in V_n} f(a+1^n) - f(a)f(a+1^n)\right. \\ &\quad \left. +(f(a) - f(a+1^n))[a\cdot b]_2\right)^2 \\ &= \sum_{[b\cdot 1^n]_2=1}\left(H(f) - 2Q(f)\right. \\ &\quad \left. +\sum_{a\in V_n}(f(a) - f(a+1^n))[a\cdot b]_2\right)^2 \end{aligned}$$

$$
\begin{aligned}
&= 2^{n-1}(H(f)-2Q(f))^2 + 2(H(f)-2Q(f)) \\
&\quad \cdot \sum_{a\in V_n} (f(a)-f(a+1^n)) \sum_{[b\cdot 1^n]_2=1} [a\cdot b]_2 \\
&\quad + \sum_{a,c\in V_n} (f(a)-f(a+1^n)) \\
&\quad \cdot (f(c)-f(c+1^n)) \sum_{[b\cdot 1^n]_2=1} [a\cdot b]_2[c\cdot b]_2 \\
&= 2^{n-1}(H(f)-2Q(f))^2 \\
&\quad +2^n(H(f)-2Q(f))(f(1^n)-f(0^n)) \\
&\quad +2^{n-1}(H(f)-2Q(f)).
\end{aligned}
$$

It follows that

$$
\begin{aligned}
E[\widetilde{f}(b)^2] = &\\
&2^{2n-1} - 2^{n+1}H(f) + 2H(f)^2 \\
&-4H(f)Q(f) + 4H(f)f(0^n)f(1^n) \\
&+(2^{n+1}+2)Q(f) - 2^{n+1}f(0^n)f(1^n) \\
&+2Q(f)^2 - 4f(0^n)f(1^n)Q(f) \\
&+2^{-1}(H(f)-2Q(f))^2 \\
&+(H(f)-2Q(f))(f(1^n)-f(0^n)) \\
&+2^{-1}(H(f)-2Q(f)) \\
= \; &2^{2n-1} + \frac{5}{2}H(f)^2 - 6H(f)Q(f) \\
&+4Q(f)^2 - (2^{n+1} - \frac{1}{2} + f(0^n) - f(1^n) \\
&-4f(0^n)f(1^n))H(f) \\
&+(2^{n+1}+1+2f(0^n)-2f(1^n) \\
&-4f(0^n)f(1^n))Q(f) - 2^{n+1}f(0^n)f(1^n),
\end{aligned}
$$

as claimed. □

VII. Arithmetic Walsh Transforms of Linear Functions

In this section we make use of the analysis in Section III to completely describe the arithmetic correlations of linear functions. That is, of Boolean functions $f(a) = \mathbf{T}_c(a) = [a\cdot c]_2$, $a, c \in V_n$.

If $c = 0^n$, then f is identically zero. By Theorem 2,

$$
\widetilde{\mathbf{T}}_{0^n}(b) = \begin{cases} 2^n & \text{if } [b\cdot 1^n]_2 = 0 \\ 0 & \text{if } [b\cdot 1^n]_2 = 1. \end{cases}
$$

For the remainder of the section we assume that $c \neq 0^n$. By equation (11), if $[b\cdot 1^n]_2 = 0$, then

$$
\begin{aligned}
&\widetilde{\mathbf{T}}_c(b) = \\
&\quad 2^n - 2\sum_{a\in V_n} [a\cdot c]_2 \\
&\quad +2\sum_{a\in V_n} [a\cdot c]_2[(a+1^n)\cdot c]_2[a\cdot b]_2 \\
&= \; 2\sum_{a\in V_n} [a\cdot c]_2[(a+1^n)\cdot c]_2[a\cdot b]_2. \qquad (29)
\end{aligned}
$$

By equation (13), if $[b\cdot 1^n]_2 = 1$, then

$$
\begin{aligned}
&\widetilde{\mathbf{T}}_c(b) = \\
&\quad \sum_{a\in V_n} [(a+1^n)\cdot c]_2(1-[a\cdot c]_2) \\
&\quad +([a\cdot c]_2 - [(a+1^n)\cdot c]_2)[a\cdot b]_2). \qquad (30)
\end{aligned}
$$

We treat these equations separately. First suppose that $[b\cdot 1^n]_2 = 0$. If $b = 0^n$, then $\widetilde{\mathbf{T}}_c(b) = 0$. If $b \neq 0^n$ and $c\cdot 1^n = 0$, then

$$
\begin{aligned}
\widetilde{\mathbf{T}}_c(b) &= 2\sum_{a\in V_n} [a\cdot c]_2[a\cdot c]_2[a\cdot b]_2 \\
&= 2\sum_{a\in V_n} [a\cdot c]_2[a\cdot b]_2 \\
&= \begin{cases} 2\sum_{a\in V_n} [a\cdot c]_2 = 2^n & \text{if } b = c \\ 2\cdot 2^{n-2} = 2^{n-1} & \text{if } b \neq c. \end{cases}
\end{aligned}
$$

(The last line holds because $[a\cdot c]_2[a\cdot b]_2 = 1$ on the intersection of two hyperplanes and is 0 everywhere else.) The last case occurs for $2^{n-1}-2$ values of b for each such c. If $c\cdot 1^n = 1$, then

$$
\widetilde{\mathbf{T}}_c(b) = 2\sum_{a\in V_n} [a\cdot c]_2(1-[a\cdot c]_2)[a\cdot b]_2 = 0,
$$

since if $x \in \{0,1\}$, then $x(1-x) = 0$. This occurs for 2^{n-1} values of b for each such c.

Now suppose that $[b\cdot 1^n]_2 = 1$. If $c\cdot 1^n = 0$, then

$$
\begin{aligned}
\widetilde{\mathbf{T}}_c(b) &= \sum_{a\in V_n} [a\cdot c]_2(1-[a\cdot c]_2) \\
&\quad +([a\cdot c]_2 - [a\cdot c]_2)[a\cdot b]_2) \\
&= 0.
\end{aligned}
$$

This occurs for 2^{n-1} values of b for each such c. If $c \cdot 1^n = 1$, then

$$\begin{aligned}
\widetilde{\mathbf{T}}_c(b) &= \sum_{a \in V_n} (1 - [a \cdot c]_2)^2 \\
&\quad +(2[a \cdot c]_2 - 1)[a \cdot b]_2) \\
&= \sum_{a \in V_n} (1 - [a \cdot c]_2) \\
&\quad +(2[a \cdot c]_2 - 1)[a \cdot b]_2) \\
&= 2^{n-1} + \sum_{a \in V_n} (2[a \cdot c]_2 - 1)[a \cdot b]_2) \\
&= 2^{n-1} \\
&\quad + \begin{cases} \sum_{a \in V_n} 2[a \cdot c]_2^2 - [a \cdot c]_2 \\ \text{if } b = c \\ \sum_{a \in V_n} 2[a \cdot c]_2[a \cdot b]_2 - [a \cdot b]_2 \\ \text{if } b \neq c. \end{cases} \\
&= \begin{cases} 2^n & \text{if } b = c \\ 2^{n-1} & \text{if } b \neq c. \end{cases}
\end{aligned}$$

The second case occurs for $2^{n-1} - 1$ values of b for each such c. Now we fix c and describe the distribution of values of $\widetilde{\mathbf{T}}_c(b)$.

Theorem 11: Let $c \in V_n$. If $c = 0^n$, then the arithmetic Walsh transform of $\mathbf{T}_c$ has values 0, which occurs 2^{n-1} times, and 2^n, which occurs 2^{n-1} times. If $c \cdot 1^n = 0$ and $c \neq 0^n$, then the arithmetic Walsh transform of $\mathbf{T}_c$ has values 0, which occurs $2^{n-1} + 1$ times, 2^{n-1}, which occurs $2^{n-1} - 2$ times, and 2^n, which occurs once. If $c \cdot 1^n = 1$, then the arithmetic Walsh transform of $\mathbf{T}_c$ has values 0, which occurs 2^{n-1} times, 2^{n-1}, which occurs $2^{n-1} - 1$ times, and 2^n, which occurs once.

VIII. Arithmetic Walsh Transforms of Affine Functions

In this section we make use of the analysis in Section III to completely describe the arithmetic correlations of affine nonlinear functions. That is, of Boolean functions $f(a) = \mathbf{S}_c(a) = 1 - [a \cdot c]_2$, $a, c \in V_n$.

If $c = 0^n$, then f is identically one. By Theorem 2,

$$\widetilde{\mathbf{S}}_{0^n}(b) = \begin{cases} -2^n & \text{if } b = 0^n \\ 0 & \text{if } b \neq 0^n. \end{cases}$$

For the remainder of the section we assume that $c \neq 0^n$. Theorem 2 implies that if $[b \cdot 1^n]_2 = 0$, then

$$\begin{aligned}
&\widetilde{\mathbf{S}}_c(b) = \\
&\quad 2^n - 2 \sum_{a \in V_n} (1 - [a \cdot c]_2) \\
&\quad +2 \sum_{a \in V_n} (1 - [a \cdot c]_2)(1 - [(a + 1^n) \cdot c]_2)[a \cdot b]_2 \\
&= 2 \sum_{a \in V_n} (1 - [a \cdot c]_2)(1 - [(a + 1^n) \cdot c]_2)[a \cdot b]_2.
\end{aligned} \tag{31}$$

If $[b \cdot 1^n]_2 = 1$, then

$$\begin{aligned}
&\widetilde{\mathbf{S}}_c(b) = \\
&\quad \sum_{a \in V_n} (1 - [(a + 1^n) \cdot c]_2)[a \cdot c]_2 \\
&\quad +([(a + 1^n) \cdot c]_2 - [a \cdot c]_2)[a \cdot b]_2.
\end{aligned} \tag{32}$$

We treat these equations separately. First suppose that $[b \cdot 1^n]_2 = 0$. If $b = 0^n$, then $\widetilde{\mathbf{S}}_c(b) = 0$. If $b \neq 0^n$ and $c \cdot 1^n = 0$, then

$$\begin{aligned}
\widetilde{\mathbf{S}}_c(b) &= 2 \sum_{a \in V_n} (1 - [a \cdot c]_2)[a \cdot b]_2 \\
&= \begin{cases} 0 & \text{if } b = c \\ 2 \cdot 2^{n-2} = 2^{n-1} & \text{if } b \neq c. \end{cases}
\end{aligned}$$

The last case occurs for $2^{n-1} - 2$ values of b for each such c. If $c \cdot 1^n = 1$, then

$$\widetilde{\mathbf{S}}_c(b) = 2 \sum_{a \in V_n} (1 - [a \cdot c]_2)[a \cdot c]_2[a \cdot b]_2 = 0.$$

This occurs for 2^{n-1} values of b for each such c.

Now suppose that $[b \cdot 1^n]_2 = 1$. If $c \cdot 1^n = 0$, then

$$\begin{aligned}
\widetilde{\mathbf{S}}_c(b) &= \sum_{a \in V_n} (1 - [a \cdot c]_2)[a \cdot c]_2 \\
&\quad +([a \cdot c]_2 - [a \cdot c]_2)[a \cdot b]_2 \\
&= 0.
\end{aligned}$$

This occurs for 2^{n-1} values of b for each such c. If

$c \cdot 1^n = 1$, then

$$\begin{aligned}
\widetilde{\mathbf{S}}_c(b) = & \\
& \sum_{a \in V_n} [a \cdot c]_2^2 + (1 - 2[a \cdot c]_2)[a \cdot b]_2 \\
= & \sum_{a \in V_n} [a \cdot c]_2 + (1 - 2[a \cdot c]_2)[a \cdot b]_2 \\
= & \ 2^{n-1} + \sum_{a \in V_n} (1 - 2[a \cdot c]_2)[a \cdot b]_2 \\
= & \begin{cases} 2^{n-1} + \sum_{a \in V_n} [a \cdot c]_2 - 2[a \cdot c]_2^2 \\ \text{if } b = c \\ 2^{n-1} + \sum_{a \in V_n} [a \cdot b]_2 - 2[a \cdot c]_2[a \cdot b]_2 \\ \text{if } b \neq c. \end{cases} \\
= & \begin{cases} 0 & \text{if } b = c \\ 2^{n-1} & \text{if } b \neq c. \end{cases}
\end{aligned}$$

The second case occurs for $2^{n-1} - 1$ values of b for each such c. Now we fix c and describe the distribution of values of $\widetilde{\mathbf{S}}_c(b)$.

Theorem 12: Let $c \in V_n$. If $c = 0^n$, then the arithmetic Walsh transform of $1 - \mathbf{S}_c$ has values 0, which occurs $2^n - 1$ times, and -2^n, which occurs once. If $c \cdot 1^n = 0$ and $c \neq 0^n$, then the arithmetic Walsh transform of $1 - \mathbf{S}_c$ has values 0, which occurs $2^{n-1}+2$ times and 2^{n-1}, which occurs $2^{n-1}-2$ times. If $c \cdot 1^n = 1$, then the arithmetic Walsh transform of $1 - \mathbf{S}_c$ has values 0, which occurs $2^{n-1}+1$ times and 2^{n-1}, which occurs $2^{n-1} - 1$ times.

IX. Future Work

A. Bentness

In cryptography we generally want to use Boolean functions that are as far from being linear as possible. Linear functions have Walsh-Hadamard spectra with one large coefficient (with value 2^n) and all remaining coefficients zero. In a sense all the "mass" is concentrated in one coefficient. These are the functions for which the maximum absolute values of the Walsh-Hadamard coefficients is as large as possible.

By contrast, a bent function has all the mass spread uniformly across all coefficients, so the absolute values of all the Walsh-Hadamard coefficients are the same (equal to $2^{n/2}$). These can also be characterized as the functions for which the maximum absolute values of the Walsh-Hadamard coefficients is as small as possible.

We would like to find an arithmetic analog of bentness, but the situation is not so clear. Linear and affine functions do not have such neat arithmetic Walsh spectra so it is not so clear what one might consider the opposite behavior. Bent functions are also the functions whose Hamming distance is the maximum allowed by Parseval's identity (the second moment equals 2^n). But, as we have seen in Section III-A, the arithmetic Walsh transform does not correspond to a metric in the way that the Walsh-Hadamard transform does. It is possible that it would be better if we built our theory of arithmetic Walsh transforms around a symmetric version of the Walsh-Hadamard transform: define

$$\widetilde{f}^S(b) = Z(\mathbf{f} - \mathbf{T}_b) + Z(\mathbf{T}_b - \mathbf{f}).$$

It remains to attempt to redo all the work in this paper on replacing $\widetilde{f}(b)$ by $\widetilde{f}^S(b)$.

B. Cryptanalysis

Ultimately, Walsh-Hadamard transforms and bentness are studied because of their implications for the cryptanalysis of symmetric key cryptosystems [11]. If the maximum absolute value of the Walsh-Hadamard coefficients is small, then system resists certain attacks that attempt to find good linear approximations to the given function. Bent functions are optimal in this sense (although they are provably suboptimal in other senses, so one typically looks for "almost bent" functions). We do not yet know of a cryptanalytic attack whose effectiveness is similarly measured by the arithmetic Walsh transform.

References

[1] D. Biss, A lower bound for the number of functions satisfying the strict avalanche criterion, *Discrete Math* **185** (1998) pp. 29–39.

[2] T. Cusick and P. Stănică, Bounds on the number of functions satisfying the strict avalanche criterion, *Inf. Proc. Lett.* **60** (1996) pp. 215–219.

[3] M. Goresky and A. Klapper, Arithmetic Cross-Correlations of FCSR Sequences, *IEEE Trans. Info. Theory* **43** (1997) pp. 1342-1346.

[4] M. Goresky and A. Klapper, Fibonacci and Galois Representations of Feedback with Carry Shift Registers, *IEEE Trans. Info. Theory* **48** (2002) pp. 2826-2836.
[5] K. Hensel, Über eine neue Begrndung der Theorie der algebraischen Zahlen, Jahresber. Deutsch. Math. Verein 6 (1897) pp. 83-88.
[6] A. Klapper and M. Goresky, Feedback Shift Registers, Combiners with Memory, and 2-Adic Span, *Journal of Cryptology* **10** (1997) pp. 111-147.
[7] A. Klapper and M. Goresky, A With-Carry Walsh Transform (Extended Abstract), in C. Carlet and A. Pott, eds., *Sequences and Their Applications – SETA 2010, Lecture Notes in Computer Science* **6338** (2010) 217-228.
[8] A. Klapper and J. Xu, Algebraic feedback shift registers, *Theoretical Computer Science* **226** (1999) pp. 61–93.
[9] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta Functions,* Springer-Verlag: New York, 1984.
[10] V. Kumar, R. Scholtz and L. Welch, Generalized bent functions and their properties, *J. Comb. Theory A* **40** (1985) pp. 90–107.
[11] W. Meier and O. Staffelbach, Nonlinearity Criteria for Cryptographic Functions, in J.-J. Quisquater and J. Vandewalle, eds., *Advances in Cryptology, EUROCRYPT' 89, Lecture Notes in Computer Science* **434** (1990) pp. 549-562.
[12] O. S. Rothaus, On "bent" functions, J. Comb. Theory A **20** (1976) pp. 300–305.
[13] A. Youssef and S. Tavares, Comment on "Bounds on the number of functions satisfying the strict avalanche criterion," Inf. Proc. Lett **60** (1996) pp. 271–275.

Andrew Klapper received the A.B. degree in mathematics from New York University in 1974, the M.S. degree in applied mathematics from SUNY at Binghamton in 1975, the M.S. degree in mathematics from Stanford University in 1976, and the Ph.D. degree in mathematics from Brown University in 1982.

He is a Professor in the Department of Computer Science at the University of Kentucky. He was awarded a University Research Professorship for 2002-03. His past research has included work on algebraic geometry over p-adic integer rings, computational geometry, modeling distributed systems, structural complexity theory, covering properties of codes, and cryptography. His current interests include statistical properties of pseudo-random sequences based on abstract algebra, with applications in cryptography and CDMA. he is also a morris dancer.

Dr. Klapper is a member of the Information Theory Society and is a Senior Member of the IEEE. He was the general chair of Crypto '98 and of SETA 2008. He was the Associate Editor for Sequences for the IEEE Transactions on Information Theory from 1999 to 2002. He is currently an Associate Editor of the journals Applied Mathematics of Communications and Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences.

Mark Goresky received his Ph.D. in Mathematics from Brown University in 1976. He has held academic positions at MIT, at the University of British Columbia, and at Northeastern University. He is currently a long term member in the School of Mathematics at the Institute for Advanced Study, Princeton NJ. He is interested in the generation and analysis of pseudorandom sequences, but he also maintains a research program in number theory and automorphic forms. Further information is available on his home page which may be found by googling "Mark Goresky".