Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions

Palash Sarkar[*]
Centre for Applied Cryptographic Research
Department of Combinatorics and Optimization
University of Waterloo
200 University Avenue West
Waterloo, Ontario
Canada N2L 3G1
e-mail: psarkar@cacr.math.uwaterloo.ca

Abstract

In this paper we prove a general result on the Walsh Transform of an arbitrary Boolean function. As a consequence, we obtain several divisibility results on the Walsh Transform of correlation immune and resilient Boolean functions. This allows us to improve upper bounds on the nonlinearity of correlation immune and resilient Boolean functions. Also we provide new necessary conditions on the algebraic normal form of correlation immune/resilient functions attaining the maximum possible nonlinearity.

1 Introduction

Boolean functions are extensively used in stream cipher systems. Some of the important properties for a Boolean function to be used in stream cipher systems are balancedness, correlation immunity (CI), algebraic degree and nonlinearity. Construction of Boolean functions possessing a good combination of these properties have been proposed in [4, 10, 11, 13]. However, it is important to study the exact nature of the relationship between the above mentioned properties. This topic has received a lot of attention in recent times as evidenced by the papers [1, 10, 13, 15]. The most recent paper to consider these relationships is by Carlet [1], where use is made of the numerical normal form [2] to obtain certain divisibilty results which improve upon the divisibility results obtained in [10].

[*] On leave from the Indian Statistical Institute, Calcutta, INDIA. e-mail: palash@isical.ac.in

The Walsh Transform is an important tool for the analysis of Boolean functions. The Walsh Transform can be seen as a map from the n-dimensional hypercube to the integers. Here we obtain a general result relating the Walsh Transform at a point ω to the Walsh Transfrom values at the points in the subcube subtended by ω. As a consequence, we obtain some new and important divisibility results. Our technique clearly brings out the role played by McEliece's theorem in this setting. Moreover, the general result on Walsh Transform of Boolean functions that we obtain here is important in its own right.

We use the divisibility results to obtain new upper bounds on the nonlinearities of CI and resilient functions. The upper bound for resilient functions is a refinement on the one obtained by Carlet [1]. Also we obtain new necessary conditions on the algebraic normal form of n-variable, m-CI (resp. m-resilient) functions having maximum nonlinearity $2^{n-1} - 2^m$ (resp. $2^{n-1} - 2^{m+1}$). We show that for n-variable, m-CI functions to achieve nonlinearity of $2^{n-1} - 2^m$, its algebraic normal form (ANF) must have all terms of degree $n - m$. For resilient functions, this statement becomes a bit weaker but is still stronger than the result obtained by Tarannikov [13] and Carlet [1]. See Theorem 4.3 for the exact statement on resilient functions.

2 Preliminaries

In this section we introduce a few basic concepts. We denote the addition operator over $GF(2)$ by $\oplus$. Let s, s_1, s_2 be two binary strings of same length p.

1. The Hamming distance between s_1, s_2 is denoted by $d(s_1, s_2)$ and is the number of places s_1 and s_2 are unequal.

2. The Walsh Distance $wd(s_1, s_2)$, between s_1 and s_2, is denoted by $wd(s_1, s_2)$ and is the number of places s_1 and s_2 are equal minus the number of places s_1 and s_2 are unequal. The relation between the Hamming and Walsh distances is the following: $wd(s_1, s_2) = p - d(s_1, s_2)$.

3. the Hamming weight or simply the weight of s is the number of ones in s and is denoted by $wt(s)$.

Given a binary string s, its ith bit will be denoted by s_i. An n-variable Boolean function f can be considered to be represented by a binary string of length 2^n, with respect to a fixed truth table. The weight of the function f is denoted by $wt(f)$ and is the number of ones in its binary representation. A function is balanced if $wt(f) = 2^{n-1}$.

An n-variable Boolean function $f(X_n, \ldots, X_1)$ can be uniquely represented by a multivariate polynomial over $GF(2)$.

Definition 2.1 *Let $f(X_n, \ldots, X_1)$ be an n-variable function. We can write*

$$f(X_n, \ldots, X_1) = a_0 \oplus (\bigoplus_{i=1}^{i=n} a_i X_i) \oplus (\bigoplus_{1 \leq i < j \leq n} a_{ij} X_i X_j) \oplus \ldots \oplus a_{12\ldots n} X_1 X_2 \ldots X_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \{0,1\}$. *This representation of* f *is called the algebraic normal form (ANF) of* f. *The number of variables in the highest order product term with nonzero coefficient is called the algebraic degree, or simply degree of* f.

Functions of degree at most one are called affine functions. An affine function with constant term equal to zero is called a linear function. The set of all n-variable affine (resp. linear) functions is denoted by $A(n)$ (resp. $L(n)$).

Definition 2.2 *The nonlinearity* $nl(f)$ *of an* n*-variable function* f *is defined as*

$$nl(f) = \min_{g \in A(n)} (d(f,g)),$$

i.e. $nl(f)$ *is the distance of* f *from the set of all* n*-variable affine functions. The maximum possible nonlinearity for* n*-variable functions is denoted by* $nlmax(n)$.

An important tool for the analysis of Boolean function is its Walsh transform, which we define next [3].

Definition 2.3 *Let* $f(\overline{X})$ *be an* n*-variable Boolean function. Let* $\overline{X} = (X_n, \ldots, X_1)$ *and* $\overline{\omega} = (\omega_n, \ldots, \omega_1)$ *both belong to* $\{0,1\}^n$ *and* $<\overline{X}, \overline{\omega}> = X_n\omega_n \oplus \ldots \oplus X_1\omega_1$. *Then the Walsh transform of* $f(\overline{X})$ *is a real valued function over* $\{0,1\}^n$ *which is defined as*

$$W_f(\overline{\omega}) = \sum_{\overline{X} \in \{0,1\}^n} (-1)^{f(\overline{X}) \oplus <\overline{X}, \overline{\omega}>}.$$

The Walsh transform is sometimes called the spectral distribution or simply the spectrum of a Boolean function.

A function f of $2k$ variables is called bent if $W_f(\overline{\omega}) = \pm 2^k$ for all $\overline{\omega} \in \{0,1\}^{2k}$. These functions are important in both cryptography and coding theory since they achieve the maximum possible nonlinearity among all $2k$-variable functions.

Correlation immune functions were introduced by Siegenthaler [12], to withstand a class of "divide-and-conquer" attacks on certain models of stream ciphers. Xiao and Massey [5] provided a spectral characterization of correlation immune functions. Here we state this characterization as the definition of correlation immunity.

Definition 2.4 *A function* $f(X_n, \ldots, X_1)$ *is* m*-th order correlation immune (CI) iff its Walsh transform* W_f *satisfies*

$$W_f(\overline{\omega}) = 0, \textit{ for } 1 \leq wt(\overline{\omega}) \leq m.$$

Further, if f *is balanced then* $W_f(\overline{0}) = 0$. *Balanced* m*-th order correlation immune functions are called* m*-resilient functions.*

Thus, a function $f(X_n, \ldots, X_1)$ is m-resilient iff its Walsh transform W_f satisfies

$$W_f(\overline{\omega}) = 0, \text{ for } 0 \leq wt(\overline{\omega}) \leq m.$$

The relationship between Walsh transform and Walsh distance is [7] $W_f(\overline{\omega}) = wd(f, \bigoplus_{i=1}^{i=n} \omega_i X_i)$. Siegenthaler [12] showed that an n-variable, mth order CI function can have maximum degree $n-m$ and if the function is balanced then the maximum degree possible is $n-m-1$ (see also [5, 9]).

We next present a few notations for future convenience.

1. By H_r, we denote the Hadamard matrix of order 2^r defined recursively as.

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ and for } r > 1, \quad H_r = H_{r-1} \otimes H_1.$$

2. The inner product between two n-bit vectors x, y is denoted by $< x, y >$.

3. By an m-CI (resp. m-resilient) function we denote a function which is correlation immune (resp. resilient) of order m.

4. By an (n, m, d, x)-CI (resp. (n, m, d, x)-resilient) function we mean an n-variable, m-CI (resp. m-resilient) function having degree d and nonlinearity x. Note that an (n, m, d, x)-resilient function is certainly (n, m, d, x)-CI but the opposite does not necessarily hold. In the above notation, we may replace some component by $-$ if we do not want to specify it.

We will also use the following consequence of McEliece's theorem on cyclic codes (see [6]). If f is an n-variable, degree d function then $wt(f) \equiv 0 \bmod 2^{\lfloor \frac{n-1}{d} \rfloor}$.

3 Walsh Transform

In this section we prove an important result on the Walsh Transform of an arbitrary Boolean function. The Walsh Transform can be interpreted as a function from the n-dimensional hypercube to the set of integers. Let $x, y \in \{0,1\}^n$, i.e., they are points on the n-dimensional hypercube. We say $x \leq y$ if $x_i \leq y_i$ for all $1 \leq i \leq n$. Further $x < y$ if $x \leq y$ and $x \neq y$. Let ω be a point on the n-dimensional hypercube. Then the subcube subtended by ω is given by the set of all points θ such that $\theta \leq \omega$. We now present a result which relates the value of the Walsh transform at ω to the values of the Walsh transform at all the points in the subcube subtended by ω. This is a crucial result as it allows us to prove some general divisibility results as its consequences. We begin with the following result.

Proposition 3.1 *Let $g(X_n, \ldots, X_1)$ be an n-variable Boolean function and r be an integer in the range $1 \leq r \leq n$. For $0 \leq i \leq 2^r - 1$, let $g_i(X_{n-r}, \ldots, X_1)$ be defined as follows*

$$g_i(X_{n-r}, \ldots, X_1) = g(X_n = i_r, \ldots, X_{n-r+1} = i_1, X_{n-r}, \ldots, X_1),$$

where $i_r \dots i_1$ is the r-bit binary expansion of i. Let $w_i = wt(g_i)$. Then

$$H_r[w_0, \dots, w_{2^r-1}]^T = [a_0, \dots, a_{2^r-1}]^T,$$

where H_r is the Hadamard matrix of order 2^r and

$$a_0 = \frac{2^n - W_g(0)}{2}, \quad a_i = -\frac{W_g(\theta_i)}{2} \textit{ for } i > 0.$$

Here θ_i is the n-bit vector formed by appending $(n-r)$ zeros to the end of $i_r \dots i_1$.

Proof : The first row of H_r is the all one row and so

$$a_0 = \sum_{k=0}^{k=2^r-1} w_i = wt(g) = d(g, l_0),$$

where l_0 is the all zero linear function. Using the relation $W_f(0) = wd(g, l_0) = 2^n - 2d(g, l_0)$ we get the result for a_0. Now we consider the case $i > 0$. Consider

$$l_{\theta_i}(X_n, \dots, X_1) =< \theta_i, (X_n, \dots, X_1) >=< (i_r, \dots, i_1, 0, \dots, 0), (X_n, \dots, X_1) > .$$

So $W_g(\theta_i) = wd(g, l_{\theta_i})$. Define $\lambda_i(Y_r, \dots, Y_1) =< (i_r, \dots, i_1), (Y_r, \dots, Y_1) >$. Then the ith row $R_i = (R_{i,0}, \dots, R_{i,2^r-1})$ of H_r is given by $R_{i,j} = (-1)^{\lambda_i(j_r, \dots, j_1)}$, where $j_r \dots j_1$ is the r-bit binary expansion of j. Note that $a_i =< (R_{i,0}, \dots, R_{i,2^r-1}), (w_0, \dots, w_{2^r-1}) >$. For $0 \leq k \leq 2^r - 1$, define

$$l_k(X_{n-r}, \dots, X_1) = l_{\theta_i}(X_n = k_r, \dots, X_{n-r+1} = k_1, X_{n-r}, \dots, X_1),$$

where $k_r \dots k_1$ is the r-bit binary expansion of k. Clearly,

$$wd(g, l_{\theta_i}) = \sum_{k=0}^{k=2^r-1} wd(g_k, l_k) = \sum_{k=0}^{k=2^r-1} (2^{n-r} - 2d(g_k, l_k)). \tag{1}$$

The following computation shows that each l_k is a constant function.

$$\begin{aligned} l_k(X_{n-r}, \dots, X_1) &= l_{\theta_i}(X_n = k_r, \dots, X_{n-r+1} = k_1, X_{n-r}, \dots, X_1) \\ &= < (i_r, \dots, i_1, 0, \dots, 0), (X_n = k_r, \dots, X_{n-r+1} = k_1, X_{n-r}, \dots, X_1) > \\ &= < (i_r, \dots, i_1), (k_r, \dots, k_1) > \\ &= \lambda_i(k_r, \dots, k_1) \end{aligned}$$

Since l_k is constant the value of $d(g_k, l_k)$ is $wt(g_k)$ or $2^{n-r} - wt(g_k)$ according as $\lambda_i(k_r, \dots, k_1)$ is 0 or 1. This is expressed by writing

$$d(g_k, l_k) = 2^{n-r}\lambda_i(k_r, \dots, k_1) + (-1)^{\lambda_i(k_r, \dots, k_1)} wt(g_k).$$

We now continue the computation of Equation 1.

$$\begin{aligned}
wd(g, l_{\theta_i}) &= \sum_{k=0}^{k=2^r-1} (2^{n-r} - 2(2^{n-r}\lambda_i(k_r, \ldots, k_1) + (-1)^{\lambda_i(k_r,\ldots,k_1)} wt(g_k))) && (2)\\
&= 2^n - 2^{n-r+1} \sum_{k=0}^{k=2^r-1} \lambda_i(k_r, \ldots, k_1) - 2 \sum_{k=0}^{k=2^r-1} (-1)^{\lambda_i(k_r,\ldots,k_1)} wt(g_k) && (3)
\end{aligned}$$

Since $i > 0$, the function $\lambda_i(k_r, \ldots, k_1)$ is balanced and hence $\sum_{k=0}^{k=2^r-1} \lambda_i(k_r, \ldots, k_1) = 2^{r-1}$. Thus we get

$$\begin{aligned}
wd(g, l_{\theta_i}) &= -2 \sum_{k=0}^{k=2^r-1} (-1)^{\lambda_i(k_r,\ldots,k_1)} wt(g_k) && (4)\\
&= -2 \sum_{k=0}^{k=2^r-1} R_{i,k} w_k && (5)\\
&= -2 < (R_{i,0}, \ldots, R_{i,2^r-1}), (w_0, \ldots, w_{2^r-1}) > && (6)\\
&= -2a_i. && (7)
\end{aligned}$$

This gives the result. ■

Let f be an n-variable Boolean function and ω be in $\{0,1\}^n$ with $wt(\omega) = r$. By f_ω we denote the $(n-r)$-variable Boolean function defined as follows. Let $i_1, \ldots, i_r$ be such that $\omega_{i_1} = \ldots = \omega_{i_r} = 1$ and $\omega_j = 0$ for $j \notin \{i_1, \ldots, i_r\}$. Then f_ω is formed from f by setting variable X_j to 0 iff $j \in \{i_1, \ldots, i_r\}$.

Theorem 3.1 *Let $f(X_n, \ldots, X_1)$ be a Boolean function and $\omega \in \{0,1\}^n$. Then*

$$W_f(\omega) = 2^n - \sum_{\theta<\omega} W_f(\theta) - 2^{wt(\omega)+1} wt(f_\omega).$$

Proof : We first note that $W_f(\omega) = wd(f, l_\omega)$. Let $wt(\omega) = r$, and

$$l_\omega(X_n, \ldots, X_1) =< \omega, (X_n, \ldots, X_1) >= X_{i_r} \oplus \ldots \oplus X_{i_1}.$$

Let π be a permutation on the variables such that

$$l(X_n, \ldots, X_1) = l_\omega(\pi(X_n, \ldots, X_1)) = X_n \oplus \ldots \oplus X_{n-r+1}.$$

Let $g(X_n, \ldots, X_1) = f(\pi(X_n, \ldots, X_1))$. Then for any $\gamma \in \{0,1\}^n$ we have

$$\begin{aligned}
W_g(\gamma) &= wd(g(X_n, \ldots, X_1), l_\gamma(X_n, \ldots, X_1))\\
&= wd(f(\pi(X_n, \ldots, X_1)), < \gamma, (X_n, \ldots, X_1) >)\\
&= wd(f(\pi^{-1}(\pi(X_n, \ldots, X_1))), < \gamma, \pi^{-1}(X_n, \ldots, X_1) >)\\
&= wd(f(X_n, \ldots, X_1), < \pi(\gamma), (X_n, \ldots, X_1) >)\\
&= W_f(\pi(\gamma))
\end{aligned}$$

As a consequence we have $W_f(\omega) = wd(f, l_\omega) = wd(g, l) = W_g(\sigma)$, where σ is the n-bit vector having the first r bits as 1. Also $wt(f_\omega) = wt(g_\sigma)$. From this it follows that it is sufficient to prove the result for $W_g(\sigma)$.

Define functions $g_0, \ldots, g_{2^r-1}$ as follows.

$$g_i(X_{n-r}, \ldots, X_1) = g(X_n = i_r, \ldots, X_{n-r+1} = i_1, X_{n-r}, \ldots, X_1),$$

where $i_r, \ldots, i_1$ is the r-bit binary expansion of i. Also for $0 \leq i \leq 2^r - 1$, let θ_i be formed by concatenating $(n-r)$ zeros to the end of $i_r \ldots i_1$. Then it is easy to see that each $\theta_i \leq \sigma$ and $\theta_{2^r-1} = \sigma$. Also the θ_i's are exactly the points on the subcube subtended by σ.

Let $w_i = wt(g_i)$. Then $w_0 = wt(g_\sigma) = wt(f_\omega)$. Using Proposition 3.1 we write

$$H_r[w_0, \ldots, w_{2^r-1}]^T = [a_0, \ldots, a_{2^r-1}]^T,$$

where H_r is the Hadamard matrix of order 2^r and

$$a_0 = \frac{2^n - W_g(0)}{2}, \quad a_i = -\frac{W_g(\theta_i)}{2} \text{ for } i > 0. \tag{8}$$

Since H_r is a Hadamard matrix, it follows that $H_r H_r = 2^r I_r$, where I_r is the identity matrix of order 2^r. Hence we get

$$2^r[w_0, \ldots, w_{2^r-1}]^T = H_r[a_0, \ldots, a_{2^r-1}]^T. \tag{9}$$

The first row of H_r is the all one row, hence equating the first component on both sides of Equation 9, we get

$$\sum_{0 \leq i \leq 2^r-1} a_i = 2^r w_0.$$

We substitute the a_i's using Equations 8 to get,

$$\frac{2^n - W_g(0)}{2} + \sum_{1 \leq i \leq 2^r-1} -\frac{W_g(\theta_i)}{2} = 2^r w_0.$$

Rearranging the terms and noting that $\sigma = \theta_{2^r-1}$ and the θ_i's are exactly the points on the subcube subtended by σ gives the required relation. ■

Remark 3.1 *Note that Equation 9 shows something stronger than the statement of Theorem 3.1. It shows that $2^{r+1}w_i = 2^n - < \zeta_i, (W_g(0), \ldots, W_g(\sigma)) >$, where $\zeta_i(j) = (-1)^{l_i(j)}$ and $l_i(x) =< i, x >$. Thus using Equation 9 we can actually determine the w_i's. This is a partial inverse Walsh Transform on a subcube and is a stronger result than Theorem 3.1. In fact, just Theorem 3.1 itself has a nice small and direct proof and has been obtained by Yuriy Tarannikov [14].*

We first use Theorem 3.1 to show that a bent function on $2k$ variables has maximum degree k, which is a well known result on bent functions [8].

Corollary 3.1 *[8] Let f be a bent function on $2k$ variables. Then the maximum possible degree of f is k.*

Proof : Suppose the degree of f is $r > k$. Without loss of generality assume that the term $X_1 \ldots X_r$ is present in the ANF of f. Choose ω to be such that $\omega_1 = \ldots = \omega_r = 0$ and $\omega_{r+1} = \ldots = \omega_{2k} = 1$. Clearly $wt(\omega) = 2k - r$. From Theorem 3.1, we have

$$\sum_{\theta \leq \omega} W_f(\theta) = 2^n - 2^{wt(\omega)+1} wt(f_\omega). \tag{10}$$

Since f is bent for any $\omega \in \{0,1\}^{2k}$, we have $W_f(\omega) = \pm 2^k$. Let the number of $\theta \leq \omega$ such that $W_f(\theta) = 2^k$ be a and then the number of $\theta \leq \omega$ such that $W_f(\theta) = -2^k$ is $2^{2k-r} - a$. Thus the left hand side of Equation 10 becomes $2^k(2a - 2^{2k-r}) = 2^{k+1}(a - 2^{2k-r-1})$. (Here we use $r < 2k$, since if $r = 2k$, then the weight of f is odd and hence none of the Walsh Transform values can be 2^k.) Thus the left hand side is congruent to 0 mod 2^{k+1}. Using the definition of f_ω, we have that f_ω is an r-variable function. From the choice of ω the term $X_1 \ldots X_r$ is in f_ω and hence the degree of f_ω is r. Thus $wt(f_\omega)$ is odd. Let S be the quantity on the right side of Equation 10. Then $S \equiv 0 \bmod 2^{2k-r+1}$ and since $wt(f_\omega)$ is odd $S \not\equiv 0 \bmod 2^{2k-r+2}$. Since $r > k$, we have $2k - r + 1 < k + 1$. Therefore $S \not\equiv 0 \bmod 2^{k+1}$. But this is a contradiction and hence the result is proved. ∎

We now turn to the application of Theorem 3.1 to correlation immune functions. The following is an important consequence of Theorem 3.1.

Corollary 3.2 *Let f be an $(n, m, d, -)$-CI nonconstant function. Then for all $\omega \in \{0,1\}^n$,*

$$W_f(\omega) \equiv 0 \bmod 2^{m+1+\lfloor \frac{n-m-1}{d} \rfloor}.$$

Proof : Choose ω in Theorem 3.1 with $wt(\omega) = m$ to get $W_f(\omega) = 2^n - \sum_{\theta<\omega} W_f(\theta) - 2^{m+1} w_0$. Since f is m-CI, $W_f(\theta) = 0$ for all $1 \leq wt(\theta) \leq m$. Thus $W_f(0) = 2^n - 2^{m+1} w_0$, where $w_0 = wt(f_\omega)$ and f_ω is an $(n-m)$-variable function with some degree $d_0 \leq d$. Note that d_0 must be greater than 0, since if $d_0 = 0$, then $w_0 = 0$ or 2^{n-m}, in which case $W_f(0) = 2^n$ or -2^n respectively and hence f is a constant function. By McEliece's theorem, $wt(f_\omega) \equiv 0 \bmod 2^{\lfloor \frac{n-m-1}{d_0} \rfloor}$. Since $d_0 \leq d$ we get $\frac{n-m-1}{d_0} > \frac{n-m-1}{d}$ and hence $wt(f_\omega) \equiv 0 \bmod 2^{\lfloor \frac{n-m-1}{d} \rfloor}$. Thus $W_f(0) \equiv 0 \bmod 2^{m+1+\lfloor \frac{n-m-1}{d} \rfloor}$. Since for $1 \leq wt(\omega) \leq m$, we have that $W_f(\omega) = 0$, this proves the result for all $0 \leq wt(\omega) \leq m$.

For $wt(\omega) > m$ we proceed by induction on the weight of ω. Let $wt(\omega) = k > m$. Then from Theorem 3.1, $W_f(\omega) = 2^n - \sum\limits_{\theta<\omega} W_f(\theta) - 2^{k+1} w_1$, where $w_1 = wt(f_\omega)$ and f_ω is an $(n-k)$-variable function with some degree $d_1 \leq d$. Again using Mceliece's theorem and the fact that $d_1 \leq d$ we get $w_1 \equiv 0 \bmod 2^{\lfloor \frac{n-k-1}{d} \rfloor}$. It is easy to check that for $k > m$, we have $k+1+\lfloor \frac{n-k-1}{d} \rfloor > m+1+\lfloor \frac{n-m-1}{d} \rfloor$. Thus $2^{k+1} w_1 \equiv 0 \bmod 2^{m+1+\lfloor \frac{n-m-1}{d} \rfloor}$. For $\theta < \omega$, we have that $wt(\theta) < wt(\omega)$ and hence by the induction hypothesis we get $W_f(\theta) \equiv 0 \bmod 2^{m+1\lfloor \frac{n-m-1}{d} \rfloor}$ for all $\theta < \omega$. This gives us

$$W_f(\omega) \equiv 0 \bmod 2^{m+1+\lfloor \frac{n-m-1}{d} \rfloor},$$

which completes the induction step and the proof. ∎

We can prove a stronger result than Corollary 3.2.

Theorem 3.2 *Let f be an $(n, m, d, -)$-CI nonconstant function and $\omega \in \{0,1\}^n$, with $wt(\omega) = m + i$, for some $i \geq 1$. Then*

$$W_f(\omega) + x_i W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor\frac{n-m-2}{d}\rfloor},$$

where $x_1 = 1$ and for $i > 1$, $x_i = 1 - \sum_{j=1}^{i-1} \binom{m+i}{m+j} x_j$.

Proof : The proof is by induction on $wt(\omega)$ for $wt(\omega) \geq m + 1$.
Base: $wt(\omega) = m + 1$. Using Theorem 3.1 and the fact that $W_f(\theta) = 0$ for all $1 \leq wt(\theta) \leq m$, we get $W_f(\omega) + W_f(0) = 2^n - 2^{m+2} w_0$, where $w_0 = wt(f_\omega)$ and f_ω is an $(n - m - 1)$-variable function. As in Corollary 3.2, we can show that $w_0 \equiv 0 \bmod 2^{\lfloor\frac{n-m-2}{d}\rfloor}$. Thus we get

$$W_f(\omega) + x_1 W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor\frac{n-m-2}{d}\rfloor}.$$

Induction hypothesis: Assume the result is true for all ω with $m + 1 \leq wt(\omega) \leq m + i - 1$.
Inductive step: Let ω be such that $wt(\omega) = m + i$. Again using Theorem 3.1, we have

$$W_f(\omega) = 2^n - \sum_{\theta<\omega} W_f(\theta) - 2^{m+i+1} w_1,$$

where $w_1 = wt(f_\omega)$, and f_ω is an $(n - m - i)$-variable function with some degree $d_1 \leq d$. Again using McEliece's theorem and an argument similar to that of Corollary 3.2, we get

$$W_f(\omega) + \sum_{\theta<\omega} W_f(\theta) \equiv 0 \bmod 2^{m+2+\lfloor\frac{n-m-2}{d}\rfloor}. \tag{11}$$

Among the $W_f(\theta)$'s such that $\theta < \omega$, there are exactly $\binom{m+i}{m+j}$ many θ's having $wt(\theta) = m + j$ (for $1 \leq j \leq i - 1$). By the induction hypothesis, we have that for any such θ,

$$W_f(\theta) + x_j W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor\frac{n-m-2}{d}\rfloor}. \tag{12}$$

Substituing Equation 12 in Equation 11, we get,

$$W_f(\omega) + W_f(0)(1 - \binom{m+i}{m+i-1} x_{i-1} - \ldots - \binom{m+i}{m+1} x_1) \equiv 0 \bmod 2^{m+2+\lfloor\frac{n-m-2}{d}\rfloor}.$$

Using the definition of x_i, we get,

$$W_f(\omega) + x_i W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor\frac{n-m-2}{d}\rfloor},$$

which is what we required to prove. ■

Some important consequences can be drawn from Theorem 3.2. A weaker version of the first corollary has been obtained by Zheng and Zhang [15].

Corollary 3.3 *Let f be an $(n, m, d, -)$-CI nonconstant function.*

1. *Let $\omega \in \{0,1\}^n$ with $wt(\omega) = m + 1$. Then $W_f(\omega) \equiv 0 \bmod 2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor}$ iff $W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor}$.*

2. *If $W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor}$, then $W_f(\omega) \equiv 0 \bmod 2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor}$ for all $\omega \in \{0,1\}^n$.*

For resilient functions $W_f(0) = 0$ and hence the result becomes stronger.

Corollary 3.4 *[1] Let f be an $(n, m, d, -)$-resilient function. Then*

$$W_f(\omega) \equiv 0 \bmod 2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor} \textit{ for all } \omega \in \{0,1\}^n.$$

This result has recently been obtained by Carlet [1] using the numerical normal form of a Boolean function [2]. The next result improves upon the one obtained by Zheng and Zhang [15]. It shows that in certain situations resilient and CI functions have the same sort of divisibility results.

Corollary 3.5 *Let f be an $(n, m, d, -)$-CI nonconstant function and $\binom{n}{m+1} > 2^{2n-2m-2-2\lfloor \frac{n-m-1}{d} \rfloor}$. Then for all $\omega \in \{0,1\}^n$, we have,*

$$W_f(\omega) \equiv 0 \bmod 2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor}.$$

Proof : The proof uses a counting argument similar to the one employed by Zheng and Zhang [15]. Since f is m-CI for all $\omega \in \{0,1\}^n$, we have by Corollary 3.2,

$$W_f(\omega) \equiv 0 \bmod 2^{m+1+\lfloor \frac{n-m-1}{d} \rfloor}.$$

Thus if $W_f(\omega) \neq 0$, then $W_f(\omega) \geq 2^{m+1+\lfloor \frac{n-m-1}{d} \rfloor}$. Let y be the number of ω such that $W_f(\omega) \neq 0$. Then by Parseval's theorem we have that $y \leq 2^{2n-2m-2-2\lfloor \frac{n-m-1}{d} \rfloor}$. The number of ω such that $wt(\omega) = m + 1$ is exactly $\binom{n}{m+1}$. Thus by the given condition we get that there is at least one ω of weight $m + 1$ such that $W_f(\omega) = 0$. Using Corollary 3.3, the result then easily follows. ■

In fact, it is possible for CI and resilient functions to have the same sort of divisibility results in other situations also.

Corollary 3.6 *Let f be an $(n, m, d, -)$-CI nonconstant function and $\omega \in \{0,1\}^n$, with $wt(\omega) = m + i$, $W_f(\omega) \equiv 0 \bmod 2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor}$ and x_i is odd. Then for all $\theta \in \{0,1\}^n$,*

$$W_f(\theta) \equiv 0 \bmod 2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor}.$$

Proof : By Theorem 3.2, we have

$$W_f(\omega) + x_i W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor}.$$

Since $W_f(\omega) \equiv 0 \bmod 2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor}$ and x_i is odd, it follows that
$W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor}$. Hence using Corollary 3.3, the result follows. ■

Corollary 3.7 *1. Let f be an $(n, m, -, -)$-CI function and $\omega \in \{0,1\}^n$ be such that $wt(\omega) = m$. Then f is balanced iff f_ω is balanced.*

2. Let f be an $(n, m, -, -)$-resilient function and $\omega \in \{0,1\}^n$ with $wt(\omega) = m + 1$. Then $W_f(\omega) = 0$ iff f_ω is balanced.

The next result shows that an $(n-2)$-CI function must be balanced.

Proposition 3.2 *For $n \geq 4$, let f be an $(n, n-2, -, -)$-CI function. Then f must be balanced.*

Proof : Write f as a concatenation of the form $f_0 \ldots f_{2^{n-2}-1}$, where each f_i is a 2-variable function and hence given by a 4-bit string. Since f is $(n-2)$-CI, using Theorem 3.1 of [9], we have,

$$wt(f_0) = \ldots = wt(f_{2^{n-2}-1}).$$

Let this common weight be w. If $w = 0, 4$, then f is a constant function. If $w = 2$, then f is clearly balanced. Thus we have to only rule out the possibilities $w = 1, 3$. It is sufficient to consider $w = 1$, since the case $w = 3$ can be tackled by considering the complement of f and thus reducing to the case $w = 1$.

Since $w = 1$, the function f_0 must be one of the form $1000, 0100, 0010, 0001$. We consider only the form 1000, the other cases being similar. The function $f_0 f_1$ is 1-CI and hence f_1 must be of the form 0001. Again $f_0 f_2$ must also be 1-CI and hence f_2 must also be of the form 0001. Also $f_1 f_3$ must be 1-CI and this forces f_3 to be of the form 1000. Thus the string $f_0 f_1 f_2 f_3$ is of the form 1000000100011000. Now the function $f_0 f_1 f_2 f_3$ must be 2-CI, but it is not since

$$wd(0110011001100110, 1000000100011000) = 4 - 12 = -8 \neq 0,$$

and the string 0110011001100110 represents a linear function which is nondegenerate on two variables.

Hence we get a contradiction which proves the result. ■

4 Nonlinearity and Algebraic Degree

In this section we work out the consequences on the nonlinearity and algebraic degree of the divisibility results of the previous section.

Theorem 4.1 *Let f be an (n, m, d, x)-CI nonconstant unbalanced function, $K_1 = m + \lfloor \frac{n-m-1}{d_c^{\min}} \rfloor$ and $K_2 = m + \lfloor \frac{n-m-1}{d_c^{\max}} \rfloor$, where $D = \{deg(f_\omega) : \omega \in \{0,1\}^n, \ wt(\omega) = m\}$, $d_c^{\min} = \min(D)$ and $d_c^{\max} = \max(D)$. Then*

1. *If n is even and $K_1 > \frac{n}{2} - 1$, then $x \leq 2^{n-1} - 2^{K_1}$.*
2. *If n is even and $K_1 \leq \frac{n}{2} - 1$, then $x \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{K_2}$.*

3. *If n is odd and $2^{n-1} - 2^{K_1} \leq nlmax(n)$, then $x \leq 2^{n-1} - 2^{K_1}$.*

4. *If n is odd and $2^{n-1} - 2^{K_1} > nlmax(n)$, then x is less than or equal to the highest multiple of 2^{K_2} which is not greater than $nlmax(n)$.*

Proof : Let $d_c^{\min} = deg(f_\sigma)$. Using Theorem 3.1, we can write $W_f(\sigma) = 2^n - \sum_{\theta<\sigma} W_f(\theta) - 2^{m+1}wt(f_\sigma)$. Since f is m-CI, we have $W_f(\theta) = 0$ for all $1 \leq wt(\theta) \leq m$. Also by McEliece's theorem, we have $wt(f_\sigma) \equiv 0 \bmod 2^{\lfloor \frac{n-m-1}{d_c^{\min}} \rfloor}$. Since $wt(\sigma) = m$, we get $W_f(0) \equiv 0 \bmod 2^{K_1+1}$ and hence $d(f, l_0) \equiv 0 \bmod 2^{K_1}$. Further since f is unbalanced $d(f, l_0) \neq 2^{n-1}$.

From this we clearly have that $x \leq 2^{n-1} - 2^{K_1}$. However, if n is even and $K_1 \leq \frac{n}{2} - 1$, then we can improve upon the upper bound on the nonlinearity. A function whose all Walsh Transform values are $\pm 2^{\frac{n}{2}}$ is bent and a CI function cannot be bent. It can be shown in a way similar to Corollary 3.2 that for any $\omega \in \{0,1\}^n$, we have $W_f(\omega) \equiv 0 \bmod 2^{m+1+\lfloor \frac{n-m-1}{d_c^{\max}} \rfloor}$. Hence the nonlinearity must be at least 2^{K_2} less than the bent nonlinearity. Similar considerations hold for odd n. ■

Theorem 4.2 *Let f be an (n, m, d, x)-resilient nonconstant function, $L_1 = m + 1 + \lfloor \frac{n-m-2}{d_r^{\min}} \rfloor$ and $L_2 = m + 1 + \lfloor \frac{n-m-2}{d_r^{\max}} \rfloor$, where $D = \{deg(f_\omega) : W_f(\omega) \neq 0, \omega \in \{0,1\}^n,\ wt(\omega) = m+1\}$, $d_r^{\min} = \min(D)$ and $d_r^{\max} = \max(D)$. Then*

1. *If n is even and $L_1 > \frac{n}{2} - 1$, then $x \leq 2^{n-1} - 2^{L_1}$.*

2. *If n is even and $L_1 \leq \frac{n}{2} - 1$, then $x \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{L_2}$.*

3. *If n is odd and $2^{n-1} - 2^{L_1} \leq nlmax(n)$, then $x \leq 2^{n-1} - 2^{L_1}$.*

4. *If n is odd and $2^{n-1} - 2^{L_1} > nlmax(n)$, then x is less than or equal to the highest multiple of 2^{L_2} which is not greater than $nlmax(n)$.*

Proof : The proof is similar to that of Theorem 4.1. Again let $d_r^{\min} = deg(f_\sigma)$. Theorem 3.1 then provides $W_f(\sigma) = 2^n - \sum_{\theta<\sigma} W_f(\theta) - 2^{m+2}wt(f_\sigma)$, where $wt(f_\sigma) \equiv 0 \bmod 2^{\lfloor \frac{n-m-2}{d_r^{\min}} \rfloor}$. Since f is m-resilient, $W_f(\theta) = 0$ for all $0 \leq wt(\theta) \leq m$. Also $wt(\sigma) = m + 1$ and thus we get $W_f(\sigma) \equiv 0 \bmod 2^{L_1+1}$. Further from the definition of $d_r^{\min}$ we have $W_f(\sigma) \neq 0$. Thus $d(f, l_\sigma) \equiv 0 \bmod 2^{L_1}$ and $d(f, l_\sigma) \neq 2^{n-1}$. The rest of the details are similar to Theorem 4.1. ■

Theorem 4.2 refines the divisibility result obtained by Carlet [1]. We can now obtain the following result which is a stronger version of the result obtained by Tarannikov [13] and Carlet [1].

Theorem 4.3

1. *Let f be an (n, m, d, x)-CI function. If $x \not\equiv 0 \bmod 2^{m+1}$, then $d = n - m$. Further, if $x = 2^{n-1} - 2^m$, then the ANF for f has all terms of degree $n - m$.*

2. *Let f be an (n, m, d, x)-resilient function. If $x \not\equiv 0 \bmod 2^{m+2}$, then $d = n - m - 1$. Further, if $x = 2^{n-1} - 2^{m+1}$, then $d = n - m - 1$ and for any $\omega \in \{0,1\}^n$ of weight $m + 1$ we have that either $W_f(\omega) = 0$ (and hence f_ω is balanced) or $deg(f_\omega) = n - m - 1$.*

Proof : We only prove (1), the proof of (2) being similar. From the proof of Theorem 4.1, we get that $x \equiv 0 \bmod 2^{m+\lfloor\frac{n-m-1}{d_c^{\max}}\rfloor}$. Thus if $x \not\equiv 0 \bmod 2^{m+1}$, then clearly $d_c^{\max} = n - m$. Since $d_c^{\max} \leq d \leq n - m$, it follows that $d = n - m$. If $x = 2^{n-1} - 2^m$, we must have f to be unbalanced. Further in Theorem 4.1 we must have $d_c^{\min} = n - m$. But this means that any subfunction obtained from f by setting exactly m variables to 0 has degree $n - m$. Again this is possible iff the ANF for f has all terms of degree $n - m$. ■

The upper bound on nonlinearity for CI functions is more than the upper bound on nonlinearity for resilient functions. However, using Corollaries 3.5 and 3.6 it can be shown that in certain cases the upper bound for nonlinearity of CI functions is same as that of resilient functions. We do not provide the details here. Instead we will provide them in the full version of the paper.

References

[1] C. Carlet. On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions. Preprint, 2000.

[2] C. Carlet, P. Guillot. A new representation of Boolean functions. In Proceedings of AAECC'13, LNCS 1719, pages 1–14. 1999.

[3] C. Ding, G. Xiao, and W. Shan. *The Stability Theory of Stream Ciphers.* Number 561 in Lecture Notes in Computer Science. Springer-Verlag, 1991.

[4] E. Filiol, C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation immunity. In Proceedings of Eurocrypt'99, LNCS 1592 , pages 475–488. 1998.

[5] X. Guo-Zhen and J. Massey. A spectral characterization of correlation immune combining functions. *IEEE Transactions on Information Theory*, 34(3):569–571, May 1988.

[6] F. J. MacWillams and N. J. A. Sloane. *The Theory of Error Correcting Codes.* North Holland, 1977.

[7] S. Maitra and P. Sarkar. Highly nonlinear resilient functions optimizing Siegenthaler's inequality. In *Advances in Cryptology - CRYPTO'99*, number 1666 in Lecture Notes in Computer Science, pages 198–215. Springer Verlag, August 1999.

[8] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, 20:300–305, 1976.

[9] P. Sarkar. A note on the spectral characterization of correlation immune Boolean functions. Information Processing Letters, 74(5-6), pp. 191–195. 2000.

[10] P. Sarkar and S. Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. In *Advances in Cryptology - CRYPTO 2000.*

[11] P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 491–512. Springer Verlag, 2000.

[12] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, September 1984.

[13] Y. V. Tarannikov. On resilient Boolean functions with maximum possible nonlinearity. *Cryptology ePrint Archive, eprint.iacr.org, No. 2000/005*, 2000.

[14] Y. V. Tarannikov. Personal communication.

[15] Y. Zheng, X.-M. Zhang. Improved upper bound on the nonlinearity of high order correlation immune functions. In Proceedings of SAC 2000.