Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions

Claude Carlet

GREYC and University Paris 8; and INRIA, Project CODES, BP 105-78153, Le Chesnay Cedex, France
E-mail: claude.carlet@inria.fr

and

Palash Sarkar[1]

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

Communicated by Peter Jau-Shyong Shiue

Received January 30, 2001; published online July 11, 2001

We use a general property of Fourier transform to obtain direct proofs of recent divisibility results on the Walsh transform of correlation immune and resilient functions. Improved upper bounds on the nonlinearity of these functions are obtained from the divisibility results. We deduce further information on correlation immune and resilient functions. In particular, we obtain a necessary condition on the algebraic normal form of correlation immune functions attaining the maximum possible nonlinearity.

Key Words: Boolean function; correlation immunity; resiliency; nonlinearity; algebraic degree; stream ciphers.

1. INTRODUCTION

Boolean functions are extensively used in stream cipher systems. Important necessary properties of Boolean functions used in these systems are balancedness, high order correlation immunity (CI), high algebraic

degree, and high nonlinearity. Constructions of Boolean functions possessing a good combination of these properties have been proposed in [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 [2, 10, 13, 14].

Siegenthaler [12] has shown that any m-CI function ($0 \leq m < n$) in n variables has algebraic degree smaller than or equal to $n - m$ and that any m-resilient function ($0 \leq m < n$) in n variables has algebraic degree smaller than or equal to $n - m - 1$ if $m < n - 1$ and equal to 1 if $m = n - 1$.

Sarkar and Maitra showed in [10] that the Walsh transform values of an n-variable, m-resilient (resp. m-CI) function are divisible by 2^{m+2} (resp. 2^{m+1}). This provided nontrivial upper bounds on the nonlinearity of resilient and CI functions, independently obtained by Tarannikov [13] and by Zheng and Zhang [14]. The maximum possible nonlinearity of any n-variable, m-resilient (resp. m-CI) function is $2^{n-1} - 2^{m+1}$ (resp. $2^{n-1} - 2^m$). Tarannikov [13] showed that resilient functions achieving the maximum possible nonlinearity must have degree equal to $n - m - 1$. Also Zheng and Zhang [14] showed that the upper bound on nonlinearity of CI functions of high order is same as the upper bound on nonlinearity of resilient functions of same order. In a more recent work, Carlet [2] showed that the Walsh transform values of n-variable, m-resilient, degree d functions are divisible by $2^{m+2+\lfloor (n-m-2)/d \rfloor}$. The approach in [2] is to use the numerical normal form [3] to obtain results on the Walsh transform.

In this article, we continue the study discussed above. In contrast to [2], we obtain our results directly from properties of Fourier and Walsh transforms (which are presented in Section 3). The divisibility results on CI functions are presented in Section 4 and their nonlinearity is studied in Section 5, in which we also give a necessary condition on the algebraic normal form of any CI function attaining the maximum possible nonlinearity.

2. PRELIMINARIES

In this section we introduce a few basic concepts and results. By F_2 we denote the finite field $GF(2)$ and the addition operator over F_2 (and more generally over F_2^n) is denoted by $\oplus$. The (Hamming) distance between two strings s_1, s_2 of same length is denoted by $d(s_1, s_2)$ and is the number of places where s_1 and s_2 are unequal. The (Hamming) weight of s is the number of ones in s and is denoted by $wt(s)$. The inner product between two n-bit vectors x, y is denoted by $\langle x, y \rangle$. By H_r, we denote the Hadamard matrix of order 2^r defined recursively as

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

where $\otimes$ is the Kronecker product. An n-variable Boolean function $f(x_1, \ldots, x_n)$ (i.e., a function from F_2^n to F_2) is *balanced* if $wt(f) = 2^{n-1}$ (the weight $wt(f)$ of f is the weight of its associated string of values; it is the size of its support $\{x \in F_2^n; f(x) = 1\}$). The function f can be represented uniquely by a multivariate polynomial over F_2 called its algebraic normal form. The degree of this polynomial is called the *algebraic degree* or simply *degree* of f. We will use the following consequence of McEliece's theorem on cyclic codes (see [6, p. 447]): if f is an n-variable, degree d function then $wt(f) \equiv 0 \bmod 2^{\lfloor (n-1)/d \rfloor}$.

Functions of degree at most one are called affine functions. The set of all n-variable affine functions is denoted by $A(n)$. The *nonlinearity* $nl(f)$ of an n-variable function f is defined as

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

(where the distance $d(f, g)$ between the functions f and g is the distance between their associated strings of values); i.e., $nl(f)$ is the distance between f and 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 functions is the *Walsh transform*, which we define next (see for example [4]). The Walsh transform of an n-variable function $f(x_1, \ldots, x_n)$ is the real valued function over F_2^n whose value at every $u \in F_2^n$ is defined as

$$W_f(u) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus \langle x, u \rangle}.$$

For $0 \leq i \leq 2^n - 1$, set $f_i = (-1)^{f(i_1, \ldots, i_n)}$, where $i_n, \ldots, i_1$ is the binary representation of i. Then the following holds,

$$H_n[(-1)^{f_0}, \ldots, (-1)^{f_{2^n-1}}]^t = [W_f(0), \ldots, W_f(2^n - 1)]^t,$$

where "^{t}" denotes transposition. A function f of $2k$ variables is called *bent* if $W_f(u) = \pm 2^k$ for all $u \in F_2^{2k}$. 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: a function $f(x_1, \ldots, x_n)$ is mth order correlation immune (m-CI) if the distribution probability of its output is unaltered when any m of its inputs are fixed. Xiao and Massey [5] provided a spectral characterization of correlation immune functions. A function f is m-CI if and only if its Walsh transform

W_f satisfies $W_f(u) = 0$, for $1 \leq wt(u) \leq m$. Notice that the two constant Boolean functions are n-CI, but they do not present interest from a cryptographic point of view. Function f is balanced if and only if $W_f(0) = 0$. A balanced m-CI function is said to be *m-resilient*.

By an $(n, m, d, \mathcal{N})$-CI (resp. $(n, m, d, \mathcal{N})$-resilient) function we mean an n-variable, m-CI (resp. m-resilient) function having degree d and nonlinearity $\mathcal{N}$. Note that an $(n, m, d, \mathcal{N})$-resilient function is certainly $(n, m, d, \mathcal{N})$-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.

3. FOURIER AND WALSH TRANSFORMS

The Fourier transform of any real-valued function φ on F_2^n is defined as:

$$\hat{\varphi}(u) = \sum_{x \in F_2^n} \varphi(x)(-1)^{\langle x, u \rangle}.$$

The Walsh transform of any Boolean function f on F_2^n is the Fourier transform of the real-valued function $\varphi = (-1)^f$. We have:

$$W_f(0) = 2^n - 2\,wt(f). \tag{1}$$

An important property of Fourier transform is the following: let E be any vector subspace of F_2^n and $E^\perp = \{x \in F_2^n; \forall y \in E, \langle x, y \rangle = 0\}$ its orthogonal. Then

$$\sum_{u \in E} \hat{\varphi}(u) = \sum_{u \in E, x \in F_2^n} \varphi(x)(-1)^{\langle x, u \rangle} = |E| \sum_{x \in E^\perp} \varphi(x),$$

where $|E|$ denotes the size of E. This comes from the fact that the sum $\sum_{u \in E}(-1)^{\langle x, u \rangle}$ is null for every $x \notin E^\perp$. Denoting by $f_{E^\perp}$ the restriction of f to $E^\perp$ and applying this last equality to $\varphi = (-1)^f$, we obtain:

$$\sum_{u \in E} W_f(u) = |E| W_{f_{E^\perp}}(0) = |E|(|E^\perp| - 2\,wt(f_{E^\perp})) = 2^n - 2|E|\,wt(f_{E^\perp}). \tag{2}$$

Notice that relation (2) applied, for any $a \in F_2^n$, to the function $f(x) \oplus \langle a, x \rangle$ expresses the sum of the values taken by the Walsh transform of f on the flat $a + E$ by means of a value of the Walsh transform of $f_{E^\perp}$. But we shall need only relation (2) here.

A particular case of relation (2) is when E equals the vector subspace of F_2^n of all words covered by a given word v. We write $x \preceq v$ if $x_i \leq v_i$ for all i such that $1 \leq i \leq n$, and we consider the vector subspace $E_v = \{x \in F_2^n; x \preceq v\}$. The orthogonal of E_v is the vector subspace E_v of all words covered by

$\bar{v} = v \oplus (1, \ldots, 1)$ and relation (2) becomes

$$\sum_{u \in E_v} W_f(u) = 2^{wt(v)} W_{f_{\bar{v}}}(0) = 2^n - 2^{wt(v)+1} wt(f_{\bar{v}}), \tag{3}$$

where $f_{\bar{v}}$ denotes the restriction of f to $E_{\bar{v}}$. This function will be viewed in the following as a Boolean function in $n - wt(v)$ variables, since $x \in E_{\bar{v}}$ is equivalent to $\forall i \in \{1, \ldots, n\}, (v_i = 1) \Rightarrow (x_i = 0)$.

Remark

1. Relation (3) can also be applied to the function $g^a(x) = f(x \oplus a)$, where a is any word of F_2^n. If f is m-CI, then $W_f(u) = 0 = W_{g^a}(u)$ if $1 \leq wt(u) \leq m$ and thus for every word v such that $wt(v) \leq m$, $W_f(0) = 2^{wt(v)} W_{g^a}(0)$. It can be easily shown that this necessary condition is also sufficient. It is in fact equivalent to the original definition of CI functions by Siegenthaler recalled in the introduction.

2. Let f be an $(n, m, -, -)$-CI function. According to relation (3) applied to any $v \in F_2^n$ of weight m, $W_f(0)$ is divisible by 2^{m+1}. This gives an argument of the fact that f has degree smaller than or equal to $n - m$: suppose that f has degree $d \geq n - m + 1$ and consider a term $x^b = x_1^{b_1}, \ldots, x_n^{b_n}$ of degree d (i.e., such that $wt(b) = d$) in its algebraic normal form. Then the Boolean function f_b having degree d which is the maximum possible degree for a function defined on a d-dimensional vector space has odd weight and according to relation (3) applied with $v = \bar{b}$, $W_f(0)$ is not divisible by 2^{m+1}, a contradiction.

3. Let f be an $(n, m, -, -)$-CI function and $v \in F_2^n$ be such that $1 \leq wt(v) \leq m$. Then, according to relation (3), f is balanced iff $f_{\bar{v}}$ is balanced. This shows by a similar argument as above that f has degree smaller than or equal to $n - m - 1$. Moreover, if f is balanced and if v is any word of weight $m + 1$, then according to relation (3), $W_f(v)$ is null if and only if $f_{\bar{v}}$ is balanced.

4. Relation (3) also permits us to prove that any bent function on F_2^n, n even, and $n \geq 4$ has degree smaller than or equal to $n/2$: suppose that a bent function has degree $d > n/2$ and consider a term x^b of degree d in its algebraic normal form. Then the Boolean function f_b has odd weight. Thus, $2^{n-d+1} wt(f_b)$ is not divisible by 2^{n-d+2} and it is therefore not divisible by $2^{n/2+1}$. According to relation (3) applied with $v = \bar{b}$, this is a contradiction with the fact that $W_f(u)$ equals $\pm 2^{n/2}$ for every u and that $E_{\bar{b}}$ has even size ($\bar{b}$ cannot be null, since f has even weight). This simplifies the presentation of the proof by Rothaus in [8].

4. CORRELATION IMMUNE FUNCTIONS

In this section we apply relation (3) to correlation immune functions.

THEOREM 4.1. *Let f be an $(n, m, d, -)$-CI nonconstant function (resp. an $(n, m, d, -)$-resilient function). Then for all $v \in F_2^n$*

$$W_f(v) \equiv 0 \bmod 2^{m+1+\lfloor (n-m-1)/d \rfloor} \text{ (resp. } W_f(v) \equiv 0 \bmod 2^{m+2+\lfloor (n-m-2)/d \rfloor}\text{).}$$

Proof. Let f be an $(n, m, d, -)$-CI nonconstant function. Choose v in relation (3) with $wt(v) = m$. Since f is m-CI, $W_f(u) = 0$ if $1 \le wt(u) \le m$. Thus, $W_f(0) = 2^n - 2^{m+1} wt(f_v)$. The function f_v is an $(n-m)$-variable function with some degree $d_0 \le d$. Note that d_0 must be greater than 0, since if $d_0 = 0$, then $wt(f_v)$ equals 0 or 2^{n-m} and thus $W_f(0) = \pm 2^n$; i.e., f is a constant function. By McEliece's theorem, we have $wt(f_v) \equiv 0 \bmod 2^{\lfloor (n-m-1)/d_0 \rfloor}$. Since $d_0 \le d$ we get $(n-m-1)/d_0 \ge (n-m-1)/d$ and hence $wt(f_v) \equiv 0 \bmod 2^{\lfloor (n-m-1)/d \rfloor}$. Thus, according to relation (3), $W_f(0) \equiv 0 \bmod 2^{m+1+\lfloor (n-m-1)/d \rfloor}$. Since for $1 \le wt(v) \le m$, we have $W_f(v) = 0$, this proves the result if $0 \le wt(v) \le m$.

For $wt(v) > m$ we proceed by induction on the weight of v. Let $wt(v) = k > m$. Then from relation (3), $W_f(v) = 2^n - 2^{k+1} wt(f_v) - \sum_{u \prec v} W_f(u)$, where $u \prec v$ means $u \preceq v$ and $u \ne v$ and where f_v is an $(n-k)$-variable function with some degree $d_1 \le d$. Again using McEliece's theorem and the fact that $d_1 \le d$ we get $wt(f_v) \equiv 0 \bmod 2^{\lfloor (n-k-1)/d \rfloor}$. It is easy to check that for $k > m$, we have $k + 1 + \lfloor (n-k-1)/d \rfloor \ge m + 1 + \lfloor (n-m-1)/d \rfloor$. Thus $2^{k+1} wt(f_v) \equiv 0 \bmod 2^{m+1+\lfloor (n-m-1)/d \rfloor}$. For $u \prec v$, we have $wt(u) < wt(v)$ and hence by the induction hypothesis we get $W_f(u) \equiv 0 \bmod 2^{m+1+\lfloor (n-m-1)/d \rfloor}$ for all $u \prec v$. This gives us

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

which completes the induction step and the proof.

In the case of resilient functions, the proof is similar, but we choose at the first step a word v of weight $m+1$ instead of m. Notice that the result can also be deduced from Theorem 4.2 below. ■

Thus, all Walsh coefficients of f are (at least) divisible by this same power of 2. We give below a result which permits us to say more, depending on the weight of v.

THEOREM 4.2. *Let f be an $(n, m, d, -)$-CI nonconstant function and $v \in F_2^n$, with $wt(v) = m + i$, for some $i \ge 1$. Then*

$$W_f(v) + \lambda_i W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor (n-m-2)/d \rfloor},$$

where $\lambda_1 = 1$ and for $i > 1$, $\lambda_i = 1 - \sum_{j=1}^{i-1} \binom{m+i}{m+j} \lambda_j$.

Proof. The proof is by induction on $wt(v)$ for $wt(v) \ge m + 1$.

Case. $wt(v) = m + 1$. Using relation (3) and the fact that $W_f(u) = 0$ if $1 \leq wt(u) \leq m$, we get $W_f(v) + W_f(0) = 2^n - 2^{m+2} wt(f_{\bar{v}})$, where $f_{\bar{v}}$ is an $(n - m - 1)$-variable function. As in Theorem 4.1, we can show that $wt(f_{\bar{v}}) \equiv 0 \bmod 2^{\lfloor (n-m-2)/d \rfloor}$. Thus we get

$$W_f(v) + \lambda_1 W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor (n-m-2)/d \rfloor}.$$

Induction hypothesis. Assume the result is true for all v with $m + 1 \leq wt(v) \leq m + i - 1$.

Inductive step. Let v be such that $wt(v) = m + i$. Again using relation (3), we have

$$W_f(v) + \sum_{u \prec v} W_f(u) = 2^n - 2^{m+i+1} wt(f_{\bar{v}}),$$

where $f_{\bar{v}}$ 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 Theorem 4.1, we get

$$W_f(v) + \sum_{u \prec v} W_f(u) \equiv 0 \bmod 2^{m+2+\lfloor (n-m-2)/d \rfloor}. \tag{4}$$

Among the $W_f(u)$'s such that $u \prec v$, there are exactly $\binom{m+i}{m+j}$ of them having weight $m + j$ (for $1 \leq j \leq i - 1$). By the induction hypothesis, we have that for any such u,

$$W_f(u) + \lambda_j W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor (n-m-2)/d \rfloor}. \tag{5}$$

Substituting Eq. (5) in Eq. (4), we get

$$W_f(v) + W_f(0)\left(1 - \binom{m+i}{m+i-1}\lambda_{i-1} - \cdots - \binom{m+i}{m+1}\lambda_1\right) \equiv 0 \bmod 2^{m+2+\lfloor (n-m-2)/d \rfloor}.$$

Using the definition of λ_i, we get

$$W_f(v) + \lambda_i W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor (n-m-2)/d \rfloor},$$

which is what we are required to prove. ■

Thus, since $m + 2 + \lfloor (n - m - 2)/d \rfloor \geq m + 1 + \lfloor (n - m - 1)/d \rfloor$, if for some v, $\lambda_{wt(v)-m}$ is odd, then $W_f(v)$ is divisible by $2^{m+2+\lfloor (n-m-2)/d \rfloor}$ if and only if $W_f(0)$ is also divisible by this same power of 2. And if $\lambda_{wt(v)-m}$ is even, then $W_f(v)$ is divisible by $2^{m+2+\lfloor (n-m-2)/d \rfloor}$. In particular:

COROLLARY 4.1. *Let f be an $(n, m, d, -)$-CI nonconstant function.*

1. *Let $v \in F_2^n$ with $wt(v) = m + 1$. Then $W_f(v) \equiv 0 \bmod 2^{m+2+\lfloor (n-m-2)/d \rfloor}$ iff $W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor (n-m-2)/d \rfloor}$.*

2. *If $W_f(0) \equiv 0 \bmod 2^{m+2+\lfloor (n-m-2)/d \rfloor}$, then $W_f(v) \equiv 0 \bmod 2^{m+2+\lfloor (n-m-2)/d \rfloor}$ for all $v \in F_2^n$.*

3. *If $wt(v) = m + i$, $W_f(v) \equiv 0 \bmod 2^{m+2+\lfloor (n-m-2)/d \rfloor}$ and λ_i is odd, then for all $u \in F_2^n$,*

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

A weaker version of this corollary has been obtained by Zheng and Zhang [14].

The next result shows that in certain situations the divisibility results can be strengthened.

COROLLARY 4.2. *Let f be an $(n, m, d, -)$-CI nonconstant function and $\binom{n}{m+1} > 2^{2n-2m-2-2\lfloor (n-m-1)/d \rfloor}$. Then for all $v \in F_2^n$, we have*

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

Proof. The proof uses a counting argument similar to the one employed by Zheng and Zhang [14]. Since f is m-CI for all $v \in F_2^n$, we have by Theorem 4.1,

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

Thus if $W_f(v) \neq 0$, then $W_f(v) \geq 2^{m+1+\lfloor (n-m-1)/d \rfloor}$. Let μ be the number of v such that $W_f(v) \neq 0$. Then by Parseval's theorem we have that $\mu \leq 2^{2n-2m-2-2\lfloor (n-m-1)/d \rfloor}$. The number of v such that $wt(v) = m + 1$ is exactly $\binom{n}{m+1}$. Thus by the given condition we get that there is at least one v of weight $m + 1$ such that $W_f(v) = 0$. Using Corollary 4.1, the result then easily follows. ■

As noticed by Zheng and Zhang, the condition of this corollary is satisfied when $m \geq 0.6n$. Thus, CI functions with high orders have the same divisibility properties as resilient ones.

Remark. Corollary 4.2 applies in particular if $m \geq n - 2$. But non-constant CI functions with such particular orders are in fact necessarily balanced: this is clear if $m = n - 1$, if $m = n - 2$, let f be an $(n, n-2, -, -)$-CI function $(n \geq 4)$; by definition, all restrictions of f obtained by fixing $n - 2$ coordinates of the entry have the same weight. If this weight was 0 or 4, the function would be constant. If this weight was odd, i.e., if each restriction was bent, then f would satisfy $PC(2)$ of order $n - 2$ (cf. [7]). It is proved in [1] that such functions have the form $\sum_{1 \leq i < j \leq n} x_i x_j + h(x_1, \ldots, x_n)$, where h is affine. Thus,

if they are nonbalanced, they have weight $2^{n-1} \pm 2^{n/2-1}$ if n is even and $2^{n-1} \pm 2^{(n-1)/2}$ if n is odd. A contradiction.

5. CONSEQUENCES ON THE NONLINEARITY AND ON THE ALGEBRAIC NORMAL FORMS OF CORRELATION IMMUNE FUNCTIONS

Relation (3) implies directly upper bounds on the nonlinearity of m-CI and of m-resilient functions of degree d. Consider first an m-CI function and assume it is not m-resilient; then applying relation (3) with $wt(v) = m$ shows that $W_f(0)$ has magnitude greater than or equal to $2^{m+1+\lfloor (n-m-1)/d_0 \rfloor}$, where $d_0 \leq d$ is the degree of f_v which shows that f has nonlinearity smaller than or equal to $2^{n-1} - 2^{m+\lfloor (n-m-1)/d_0 \rfloor}$. Notice that we can choose v, among all words of weight m, such that the degree of f_v is minimum.

Consider now an m-resilient function f and assume it is not $(m+1)$-resilient; then there exists a word v of weight $m+1$ such that $W_f(v) \neq 0$. According to relation (3), $W_f(v)$ has then magnitude greater than or equal to $2^{m+2+\lfloor (n-m-2)/d_1 \rfloor}$, where $d_1 \leq d$ is the degree of f_v, which shows that f has nonlinearity smaller than or equal to $2^{n-1} - 2^{m+1+\lfloor (n-m-2)/d_1 \rfloor}$. Here again, we can choose v, among all words of weight $m+1$ in the support of W_f, such that the degree of f_v is minimum.

But these nonlinearity upper bounds are inefficient if $2^{n-1} - 2^{m+\lfloor (n-m-1)/d_0 \rfloor}$ (resp. $2^{n-1} - 2^{m+1+\lfloor (n-m-2)/d_1 \rfloor}$) is greater than or equal to $2^{n-1} - 2^{n/2-1}$, which is known to be greater than the nonlinearity of any balanced function. In this case, the divisibility results of Section 4 permit us to give efficient bounds, because they give information on all the values of the Walsh transform of f.

THEOREM 5.1. *Let f be an $(n, m, d, \mathcal{N})$-CI nonconstant unbalanced (resp. balanced) function. Set $K_1 = m + \lfloor (n-m-1)/d_{\min} \rfloor$ and $K_2 = m + \lfloor (n-m-1)/d_{\max} \rfloor$, where $D = \{deg(f_v):\ v \in F_2^n,\ wt(v) = m\}$, $d_{\min} = \min(D)$, and $d_{\max} = \max(D)$. Set $L_1 = m+1+\lfloor (n-m-2)/d'_{\min} \rfloor$ and $L_2 = m+1+\lfloor (n-m-2)/d'_{\max} \rfloor$, where $D' = \{deg(f_v):\ W_f(v) \neq 0,\ v \in F_2^n,\ wt(v) = m+1\}$, $d'_{\min} = \min(D')$, and $d'_{\max} = \max(D')$. Here $d_{\min}, d_{\max}, d'_{\min}, d'_{\max} \leq d$. Then*

1. *If n is even and $K_1 > \frac{n}{2} - 1$ (resp. $L_1 > \frac{n}{2} - 1$), then $\mathcal{N} \leq 2^{n-1} - 2^{K_1}$ (resp. $\mathcal{N} \leq 2^{n-1} - 2^{L_1}$).*
2. *If n is even and $K_1 \leq \frac{n}{2} - 1$ (resp. $L_1 \leq \frac{n}{2} - 1$), then $\mathcal{N} \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{K_2}$ (resp. $\mathcal{N} \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{L_2}$).*
3. *If n is odd and $2^{n-1} - 2^{K_1} \leq nlmax(n)$ (resp. $2^{n-1} - 2^{L_1} \leq nlmax(n)$), then $\mathcal{N} \leq 2^{n-1} - 2^{K_1}$ (resp. $\mathcal{N} \leq 2^{n-1} - 2^{L_1}$).*
4. *If n is odd and $2^{n-1} - 2^{K_1} > nlmax(n)$ (resp. $2^{n-1} - 2^{L_1} > nlmax(n)$), then $\mathcal{N}$ is less than or equal to the highest multiple of 2^{K_2} (resp. 2^{L_2}) which is not greater than $nlmax(n)$.*

The following result provides a restriction on the algebraic normal form of a correlation immune function achieving the maximum possible degree.

THEOREM 5.2. *Let f be an $(n, m, d, \mathcal{N})$-CI function. If $\mathcal{N} \not\equiv 0 \bmod 2^{m+1}$, then $d = n - m$. Further, if $\mathcal{N} = 2^{n-1} - 2^m$, then ANF of f contains all possible terms of degree $n - m$.*

Proof. By the same arguments as for Theorem 5.1, we get that $\mathcal{N} \equiv 0 \bmod 2^{m+\lfloor (n-m-1)/d_{\max} \rfloor}$. Thus if $\mathcal{N} \not\equiv 0 \bmod 2^{m+1}$, then clearly $d_{\max} = n - m$. Since $d_{\max} \leq d \leq n - m$, it follows that $d = n - m$. If $\mathcal{N} = 2^{n-1} - 2^m$, we must have f to be unbalanced. Further in Theorem 5.1 we must have $d_{\min} = n - m$. This completes the proof. ■

We can state a similar (but less interesting) result for those resilient functions achieving the maximum possible nonlinearity. This result provides a small improvement on the result obtained by Tarannikov [13].

THEOREM 5.3. *Let f be an $(n, m, d, \mathcal{N})$-resilient function. If $\mathcal{N} \not\equiv 0 \bmod 2^{m+2}$, then $d = n - m - 1$. Further, if $\mathcal{N} = 2^{n-1} - 2^{m+1}$, then $d = n - m - 1$ and for any $v \in F_2^n$ of weight $m + 1$ we have that either $W_f(v) = 0$ (and hence f_v is balanced) or $deg(f_v) = n - m - 1$.*

The upper bound on nonlinearity for CI functions is more than the upper bound on nonlinearity for resilient functions. However, using Corollaries 4.1 and 4.2 it can be shown that in certain cases the upper bound for nonlinearity of CI functions is the same as that of resilient functions.

REFERENCES

1. C. Carlet, On the propagation criterion of degree ℓ and order k, *in* "Advances in Cryptology-EUROCRYPT' 98," Lecture Notes in Computer Science, Vol. 1403, pp. 462–474, Springer-Verlag, Berlin/New York, 1998.
2. C. Carlet, On the coset weight divisibility and nonlinearity of resilient functions, Preprint, 2000.
3. C. Carlet and P. Guillot, A new representation of Boolean functions, *in* "Proceedings of AAECC'13," Lecture Notes in Computer Science, Vol. 1719, pp. 94–103, Springer-Verlag, Berlin/New York, 1999.
4. C. Ding, G. Xiao, and W. Shan, "The Stability Theory of Stream Ciphers," Lecture Notes in Computer Science, Vol. 561, Springer-Verlag, Berlin/New York, 1991.
5. X. Guo-Zhen and J. Massey, A spectral characterization of correlation immune combining functions, *IEEE Trans. Inform. Theory* **34** (1988), 569–571.
6. F. J. MacWillams and N. J. A. Sloane, "The Theory of Error Correcting Codes," North-Holland, Amsterdam, 1977.
7. Preneel, Van Leekwijck, Van Linden, Govaerts, and Vandevalle, Propagation characteristics of Boolean functions, *in* "Advances in Cryptology, EUROCRYPT'90," Lecture Notes in Computer Sciences, Vol. 473, pp. 161–173, Springer-Verlag, Berlin/New York, 1991.

8. O. S. Rothaus, On bent functions, *J. Combin. Theory, Ser. A* **20** (1976), 300–305.
9. P. Sarkar, A note on the spectral characterization of correlation immune Boolean functions, *Inform. Process. Lett.* **74**(5–6), (2000), 191–195.
10. P. Sarkar and S. Maitra, Nonlinearity bounds and constructions of resilient Boolean functions, *in* "Advances in Cryptology—CRYPTO 2000," Lecture Notes in Computer Science, Vol. 1880, pp. 515–532, Springer-Verlag, Berlin/New York, 2000.
11. P. Sarkar and S. Maitra, Construction of nonlinear Boolean functions with important cryptographic properties, *in* "Advances in Cryptology—EUROCRYPT 2000," Lecture Notes in Computer Science, Vol. 1807, pp. 491–512, Springer-Verlag, Berlin/New York, 2000.
12. T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, *IEEE Trans. Inform. Theory* **30** (1984), 776–780.
13. Y. V. Tarannikov, On resilient Boolean functions with maximum possible nonlinearity, *in* "Proceedings of INDOCRYPT 2000," Lecture Notes in Computer Science, Springer-Verlag, Berlin/New York, in press.
14. Y. Zheng and X.-M. Zhang, Improved upper bound on the nonlinearity of high order correlation immune functions, *in* "Proceedings of Selected Areas in Cryptography 2000," Lecture Notes in Computer Science, Springer-Verlag, Berlin/New York, in press.