Upper bounds on the numbers of resilient functions and of bent functions

Claude Carlet* Andrew Klapper †

Abstract

Bent and resilient functions play significant roles in cryptography, coding theory, and combinatorics. However, the numbers of bent and resilient functions on a given number of variables are not known. Even a reasonable bound on the number of bent functions is not known and the best known bound on the number of resilient functions seems weak for functions of high orders. In this paper we present new bounds which significantly improve upon those which can be directly deduced from the restrictions on the degrees of these functions. In the case of bent functions, it is the first one of this type. In the case of m-resilient functions, it improves upon the known bounds for m large.

Keywords: Boolean function, nonlinearity, bent, resilient, correlation-immune.

1 Introduction

Since the introduction of the notion of bent function in the mid-70's, the problem of efficiently upper bounding their number has remained open. The case of resilient functions is different: an upper bound obtained by M. Schneider seems efficient, at least for resilient functions of low orders. In both cases (bent and resilient functions), simple upper bounds can be directly derived from the upper bounds on their algebraic degrees. But these derived bounds are weak. This can be checked by trying (unsuccessfully) to

*INRIA, Domaine de Voluceau, Rocquencourt, BP 105 - 78153, Le Chesnay Cedex, FRANCE. E-mail: claude.carlet@inria.fr; also member of GREYC-Caen and of University of Paris 8.

†Dept. of Computer Science, 779A Anderson Hall, University of Kentucky, Lexington, KY, 40506-0046. E-mail: klapper@cs.uky.edu. Project sponsored by the National Science Foundation under grant #9980429.

obtain an m-resilient function (respectively, a bent function) in n variables by picking at random a Boolean function of algebraic degree upper bounded by $n-m-1$ (respectively, $n/2$). In this paper, we use characterizations of these functions by means of their Numerical Normal Forms to derive upper bounds on the numbers of m-resilient functions and of bent functions, which show that these numbers are exponentially (with respect to n) smaller than the numbers of Boolean functions of algebraic degrees smaller than or equal to $n-m-1$ and $n/2$ respectively. We improve upon Schneider's bound for high orders resilient functions.

We denote by $\oplus$ (respectively, $+$) addition in F_2 (respectively, in $\mathbf{Z}$) and by $\bigoplus_{i\in\ldots}$ (respectively, $\sum_{i\in\ldots}$) the corresponding multiple sum. Let n be any positive integer. Any Boolean function f in n variables (i.e., any $\{0,1\}$-valued function defined on the set ${F_2}^n$ of all binary words of length n) admits (cf. [18]) a unique algebraic normal form (or ANF):

$$f(x_1,\cdots,x_n)=\bigoplus_{I\subseteq\{1,\cdots,n\}} a_I\prod_{i\in I}x_i=\bigoplus_{I\subseteq\{1,\cdots,n\}} a_I\,x^I,$$

where the a_I's are in F_2 and $x^I=\prod_{i\in I}x_i$. We call the degree of the algebraic normal form of a Boolean function its *algebraic degree*. Any function f also admits (cf. [7]) a unique numerical normal form (or NNF):

$$f(x_1,\cdots,x_n)=\sum_{I\subseteq\{1,\cdots,n\}}\lambda_I\,x^I,$$

where the λ_I's are in $\mathbf{Z}$. We call the degree of the numerical normal form of a Boolean function its *numerical degree*. The ANF of f being equal to its NNF mod 2, the algebraic degree of f is always smaller than or equal to its numerical degree.

The *Hamming weight*, $w_H(f)$, of a Boolean function f in n variables is the size of its support, $\{x\in F_2^n;\ f(x)=1\}$. The *Hamming distance*, $d_H(f,g)$, between two Boolean functions f and g is the Hamming weight of their difference (i.e. of their sum modulo 2) $f\oplus g$. The *nonlinearity* of f is its minimum distance to all affine functions. Functions used in stream or block ciphers must have high nonlinearities to resist certain attacks on these ciphers (correlation and linear attacks). A Boolean function is called *bent* if its nonlinearity equals $2^{n-1}-2^{n/2-1}$ (which is the maximum possible value), where n is even. The distance from a bent function to every affine function equals $2^{n-1}\pm 2^{n/2-1}$. This property can also be stated in terms of the Walsh (i.e., Hadamard) transform of f, defined as

$$\widehat{f}(s)=\sum_{x\in {F_2}^n} f(x)\,(-1)^{x\cdot s},$$

where $x\cdot s$ denotes the usual inner product $x\cdot s=\bigoplus_{i=1}^n x_i\,s_i$. But it is more easily stated in terms of the Walsh transform of the "sign" function $\chi_f(x) = (-1)^{f(x)}$, equal to

$$\widehat{\chi_f}(s) = \sum_{x \in F_2{}^n} (-1)^{f(x) \oplus x \cdot s}.$$

The function f is bent if and only if $\widehat{\chi_f}(s)$ has constant magnitude $2^{n/2}$ (cf. [10, 18, 27]). Indeed, the distance $d_H(f, l)$ between f and the affine function $l(x) = s \cdot x \oplus \epsilon$ ($s \in F_2^n$; $\epsilon \in F_2$) and the number $\widehat{\chi_f}(s)$ are related by:

$$\widehat{\chi_f}(s) = (-1)^{\epsilon}(2^n - 2d_H(f, l)). \tag{1}$$

Notice that

$$\widehat{\chi_f}(s) = 2^n - 2\widehat{f}(s) \text{ if } s = 0 \text{ and } \widehat{\chi_f}(s) = -2\widehat{f}(s) \text{ otherwise.} \tag{2}$$

The notion of bent function is invariant under linear equivalence and it is independent of the choice of the inner product in $F_2{}^n$ (since any other inner product has the form $\langle x, s \rangle = x \cdot L(s)$, where L is a self-adjoint linear isomorphism). Any function f is bent if and only if its support is a *difference set* in the elementary Abelian 2-group F_2^n (cf. [10]). The notion of difference sets in Abelian groups had been known for several decades when bent functions were introduced in cryptography, but it was not well studied in the framework of elementary 2-groups.

The class of bent functions, whose complete determination is still an open problem, is relevant to several topics of information theory:

- cryptography, cf. [22] (bent functions have a drawback from cryptographic viewpoint: they are not balanced; but as soon as n is large enough (say $n = 20$), the difference $2^{n/2-1}$ between their weights and the weight 2^{n-1} of balanced functions is negligible and cannot be used in attacks);

- algebraic coding theory: for example, Kerdock codes are constructed from quadratic bent functions and are the best known codes for their parameters, cf. [18];

- sequences (cf. [24]);

- design theory (any difference set can be used to construct a symmetric design, cf. [1], pages 274-278).

More information on bent functions can be found in the survey paper [5].

A characterization of bent functions by means of their NNFs is given in [7] and is our main tool in deriving a bound on their number: a Boolean function f is bent if and only if for every I such that $\frac{n}{2} < |I| < n$ (where $|I|$ denotes the size of I), the coefficient λ_I is divisible by $2^{|I|-\frac{n}{2}}$, and if $\lambda_{\{1,\ldots,n\}} \equiv 2^{\frac{n}{2}-1} \bmod 2^{\frac{n}{2}}$.

Another class of Boolean functions which is important for cryptography is that of resilient functions. These functions play a central role in stream ciphers: in a common type of these ciphers (cf. [30]), the outputs of n linear feedback shift registers are the inputs to a Boolean function. The output of the function produces the keystream, which is then bitwise XOR-ed with the message to produce the cipher. Several divide-and-conquer attacks exist on this method of encryption (cf. [3, 15, 16, 31]) and lead to criteria the combining function must satisfy. Two main criteria are the following: the combining function must be *balanced* (i.e. uniformly distributed) and the probability distribution of its output must be unaltered when any m of its inputs are fixed [31], with m as large as possible. This property, called *m-th order correlation-immunity* [30], is characterized by the set of zero values in the Walsh spectrum [33]: f is m-th order correlation-immune if and only if $\widehat{\chi}_f(u) = 0$, or, equivalently, $\widehat{f}(u) = 0$ for all $u \in F_2^n$ such that $1 \le w_H(u) \le m$, where $w_H(u)$ denotes the Hamming weight of the n-bit vector u (the number of its nonzero components). Balanced m-th order correlation-immune functions are called *m-resilient* functions and are characterized by the fact that $\widehat{\chi}_f(u) = 0$ for all $u \in F_2^n$ such that $w_H(u) \le m$.

The notions of correlation-immune and resilient functions are not invariant under linear equivalence.

Characterizations of resilient functions and of correlation-immune functions by means of NNF are given in [8] and in [6] and are also our main tool in deriving bounds on their numbers: a Boolean function f is m-resilient if and only if for every I such that $|I| \ge n-m$, the coefficient λ_I of x^I in the NNF of the function $g(x) = f(x) \oplus x_1 \oplus \ldots \oplus x_n$ is null (i.e. if and only if the numerical degree of g is smaller than $n-m$). And f is m-th order correlation-immune if and only if, for every I such that $|I| \ge n-m$, we have: $\lambda_I = (-2)^{|I|-n} \lambda_{\{1,\cdots,n\}} = (-1)^n \, (-2)^{|I|-n} w_H(f)$.

2 Upper Bounds on Degrees of Functions

Rothaus' inequality states that any bent function has algebraic degree at most $n/2$ [27]. Thus, the number of bent functions is at most

$$2^{1+n+\ldots+\binom{n}{n/2}} = 2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}.$$

We refer to this as *the naive bound on (the number of) bent functions*. However, we know that for $n = 6$ (the highest number of variables for which the number of bent functions is known), the number of bent functions is approximately equal to 2^{32} (cf. [26]), which is much less than $2^{2^5+\frac{1}{2}\binom{6}{3}} = 2^{42}$. Also it has been checked experimentally that there is no hope of obtaining a bent function in 8 variables by picking a Boolean function of algebraic degree upper bounded by 4 at random. So a better upper bound is desirable.

Siegenthaler's inequality [30] states that any m-th order correlation-immune function in n variables has algebraic degree at most $n - m$, that any m-resilient function ($0 \leq m < n-1$) has algebraic degree smaller than or equal to $n-m-1$, and that any $(n-1)$-resilient function has algebraic degree 1. This implies that the number of m-resilient functions is at most $2^{1+n+\ldots+\binom{n}{n-m-1}}$ if $m < n-1$. This is also a weak bound that we refer to as *the naive bound on (the number of) m-resilient functions.*

A bound on the number of first order correlation-immune functions was found by Yang and Guo [32] and improved to $\sum_{j=0}^{2^{n-2}} \binom{2^{n-2}}{j}^4$ by Park, Lee, Sung and Kim [25]. The method of Park, Lee, Sung and Kim can be applied to bound the number of 1-resilient functions. This gives a slightly smaller (but more complex) bound. Maitra and Sarkar [19] have also derived an upper bound for the number of first order correlation-immune functions and Jian-Zhou Zhang, Zhi-Sheng You and Zheng-Liang Li [34] have derived an upper bound for the number of m-th order correlation-immune functions. However, their results involve complex parameters which make them impractical for obtaining effective upper bounds.

Moreover, a general and efficiently computed upper bound was earlier found by Schneider [29]. In the case of m-resilient functions, the upper bound he obtained is $\prod_{j=1}^{n-m} \binom{2^j}{2^{j-1}}^{\binom{n-j-1}{m-1}}$. His bound for the number of correlation-immune functions is more complex but comparable. In both cases, the bound when $m = 1$ is better than Park, Lee, Sung and Kim's bound. It seems difficult to improve it significantly for low orders. But Schneider's bound is weak for high orders. For instance, the exact number of $(n-3)$-resilient functions has been computed [2]: it is equal to $n(n-1)(3n-2)(n+1)/3$, which is much less than $\prod_{j=1}^{3} \binom{2^j}{2^{j-1}}^{\binom{n-j-1}{n-4}}$, as we can see in Table 1.

n	Schneider/exact	n	Schneider/exact
5	3.9×10^1	9	1.1×10^9
6	8.6×10^2	10	5.7×10^{11}
7	4.4×10^4	11	5.9×10^{14}
8	4.8×10^6	12	1.3×10^{18}

Table 1: (SCHNEIDER'S BOUND/EXACT NUMBER) OF $(n-3)$-RESILIENT FUNCTIONS

In this paper we derive a new bound which significantly improves upon Schneider's bound for high order correlation-immune and resilient functions.

Remark: It has recently been shown that the distance between any m-th order correlation-immune function (respectively, any m-resilient function) and any affine function is divisible by 2^m (respectively, 2^{m+1}) [28] (this result can be improved [6, 9] when the algebraic degree of the function is more strictly upper bounded than by Siegenthaler's bound). As has been observed [4, 6], the divisibility properties of the distances between affine functions and resilient functions imply upper bounds on their algebraic degrees. The same observation can be made for bent functions. Indeed, according to relations (1) and (2), the distance between a Boolean function f and every affine function is divisible by 2^k (respectively is congruent to 2^{k-1} modulo 2^k) where $k < n$, if and only if, for every word s, the number $\widehat{f}(s)$ is divisible by 2^k (respectively is congruent to 2^{k-1} modulo 2^k). Then f has algebraic degree at most $n-k$. This is a direct consequence of the fact that the ANF of any Boolean function equals its NNF modulo 2 and of the relations obtained in [7] between the coefficients λ_u and the values of the Walsh transform:

$$\widehat{f}(s) = (-1)^{w(s)} \sum_{I \subseteq \{1,\cdots,n\} \mid supp(s) \subseteq I} 2^{n-|I|} \lambda_I, \tag{3}$$

where $supp(s)$ denotes the support $\{i;\ s_i = 1\}$ of s;

$$\lambda_I = 2^{-n} (-2)^{|I|} \sum_{x \in F_2{}^n \mid I \subseteq supp(x)} \widehat{f}(x). \tag{4}$$

These bounds on the algebraic degrees do not in turn imply the divisibility properties of their distances to affine functions. McEliece's Theorem [18, 21] applied to Reed-Muller codes gives a tight divisibility bound on the distances between affine functions and functions of algebraic degrees at most d: these distances are divisible by $2^{\lfloor (n-1)/d \rfloor}$. □

We denote by $\mathcal{B}(n)$ the set of Boolean functions in n variables, by $\mathcal{B}(k,n)$ the subset of those Boolean functions of algebraic degrees at most k, by $\mathcal{D}(k,n)$ the set of functions in $\mathcal{B}(n)$ whose distances to affine functions are all divisible by 2^k and by $\mathcal{C}(k,n)$ the set of functions in $\mathcal{B}(n)$ whose distances to affine functions are all congruent to 2^k mod 2^{k+1}. We also denote $B(n) = |\mathcal{B}(n)|$, $B(k,n) = |\mathcal{B}(k,n)|$, $D(k,n) = |\mathcal{D}(k,n)|$, and $C(k,n) = |\mathcal{C}(k,n)|$. Thus every bent function is in $\mathcal{C}(n/2-1,n)$, every m-th order correlation immune function is in $\mathcal{D}(m,n)$, and every m-resilient function is in $\mathcal{D}(m+1,n)$. According to the remark above, we have $\mathcal{D}(k,n) \subseteq \mathcal{B}(n-k,n)$ and $\mathcal{C}(k,n) \subseteq \mathcal{B}(n-k-1,n)$. Applying this fact with $k = m$ (respectively, $k = m+1$) implies Siegenthaler's upper bound. Applying it with $k = n/2 - 1$ implies Rothaus' upper bound.

It is possible to give characterizations of $\mathcal{D}(k,n)$ and of $\mathcal{C}(k,n)$ by means of NNFs.

Proposition 2.1 *Let n be any positive integer and m, k any non-negative integers smaller than n. Let f be any Boolean function on F_2^n and $\sum_{I\subseteq\{1,\cdots,n\}} \lambda_I\, x^I$ be its NNF. Then*

1. *$f \in \mathcal{D}(k,n)$ if and only if, for every multi-index I, the number λ_I is divisible by $2^{|I|+k-n}$.*

2. *$f \in \mathcal{C}(k-1,n)$ if and only if, for every multi-index $I \neq \{1,\ldots,n\}$, the number λ_I is divisible by $2^{|I|+k-n}$ and if $\lambda_{\{1,\ldots,n\}}$ is congruent to 2^{k-1} mod 2^k.*

Proof: We know that f is in $\mathcal{D}(k,n)$ (respectively, in $\mathcal{C}(k-1,n)$) if and only if, for every word s, the number $\widehat{f}(s)$ is divisible by 2^k (respectively, is congruent to 2^{k-1} mod 2^k). Thus, according to relations (3) and (4), f is in $\mathcal{D}(k,n)$ if and only if, for every multi-index I, the number λ_I is divisible by $2^{|I|+k-n}$. Similarly, f is in $\mathcal{C}(k-1,n)$ if and only if, for every multi-index $I \neq \{1,\ldots,n\}$, the number λ_I is divisible by $2^{|I|+k-n}$ and $\lambda_{\{1,\ldots,n\}}$ is congruent to 2^{k-1} mod 2^k (indeed, the set $\{x \in F_2{}^n \mid I \subseteq supp(x)\}$ has odd size if $I = \{1,\ldots,n\}$ and has even size otherwise). $\square$

3 Necessary Conditions on Functions with Walsh Spectrum Constraints

A relation between the coefficients of the NNF and the coefficients of the ANF of any Boolean function f is shown in [7]:

$$\lambda_I = \sum_{k=1}^{2^n} (-2)^{k-1} \sum_{\substack{\{I_1,\ldots,I_k\}\,|\\ I_1\cup\cdots\cup I_k = I}} a_{I_1}\cdots a_{I_k}, \tag{5}$$

where the indices $I_1,\ldots,I_k$ are all distinct and in indefinite order. Notice that this relation can be directly derived from the following observation:

$$\begin{aligned} f(x) = \bigoplus_{I\subseteq\{1,\cdots,n\}} a_I\, x^I \iff & (-1)^{f(x)} = \prod_{I\subseteq\{1,\cdots,n\}} (-1)^{a_I\, x^I} \\ \iff & 1 - 2\, f(x) = \prod_{I\subseteq\{1,\cdots,n\}} (1 - 2\, a_I\, x^I) \\ \iff & f(x) = \frac{1}{2}\left(1 - \prod_{I\subseteq\{1,\cdots,n\}} (1 - 2\, a_I\, x^I)\right). \end{aligned}$$

We deduce necessary conditions for a function to bent or resilient (see also [13, 14]).

Theorem 3.1 *Let n and m be any positive integers. Let f be any Boolean function on F_2^n. Let $f(x) = \bigoplus_{I\subseteq\{1,\cdots,n\}} a_I\, x^I$ be its ANF. Denote by $g(x)$ the function $f(x) \oplus x_1 \oplus \ldots \oplus x_n$ and let $g(x) = \bigoplus_{I\subseteq\{1,\cdots,n\}} b_I\, x^I$ its ANF (i.e. $b_I = a_I \oplus 1$ if $|I| = 1$; $b_I = a_I$ otherwise). Then*

1. *if $f \in \mathcal{D}(m,n)$ and $n > m \geq 2$, then for every multi-index I such that $|I| \geq n-m+2$, we have that $\bigoplus_{\{J,K\}\,|\,J\cup K=I} a_J\; a_K = 0$.*
2. *if $f \in \mathcal{C}(m,n)$ and $n-1 > m \geq 2$, then for every multi-index I such that $|I| \geq n-m+1$, we have that $\bigoplus_{\{J,K\}\,|\,J\cup K=I} a_J\; a_K = 0$.*
3. *if f is bent (n even) and $n \geq 6$, then for every multi-index I such that $|I| \geq \frac{n}{2}+2$, we have that $\bigoplus_{\{J,K\}\,|\,J\cup K=I} a_J\; a_K = 0$.*
4. *if f is m-th order correlation-immune with $n > m \geq 2$, then for every multi-index I such that $|I| \geq n-m+2$, we have that $\bigoplus_{\{J,K\}\,|\,J\cup K=I} a_J\; a_K = 0$.*
5. *if f is m-resilient with $n > m \geq 2$, then for every multi-index I such that $|I| \geq n-m$, we have that $\bigoplus_{\{J,K\}\,|\,J\cup K=I} b_J\; b_K = 0$.*

Proof: Let $f(x) = \sum_{I\subseteq\{1,\cdots,n\}} \lambda_I\, x^I$ be the NNF of f. If $f \in \mathcal{D}(m,n)$, then according to Proposition 2.1, for every multi-index I, the number λ_I is divisible by $2^{|I|+m-n}$. Thus, if $|I| \geq n-m+2$, then λ_I is divisible by 4. According to relation (5), this is equivalent to $a_I = 0$ (we know this already since f has algebraic degree at most $n-m$) and $\bigoplus_{\{J,K\}\,|\,J\cup K=I} a_J\; a_K = 0$.

Replacing m by $m+1$ in Proposition 2.1, we see that if $f \in \mathcal{C}(m,n)$ and if $|I| \geq n-m+1$, then λ_I is divisible by 4 (indeed, if $I \neq \{1,\ldots,n\}$, then λ_I is divisible by $2^{|I|+m+1-n}$ and thus by 4 and if $I = \{1,\ldots,n\}$, λ_I is congruent to 2^m mod 2^{m+1} and thus it is divisible by 4). This implies $\bigoplus_{\{J,K\}\,|\,J\cup K=I} a_J\; a_K = 0$.

If f is bent, then $f \in \mathcal{C}(n/2-1,n)$ and thus, if $n/2-1 \geq 2$, then for every multi-index I such that $|I| \geq \frac{n}{2}+2$, we have $\bigoplus_{\{J,K\}\,|\,J\cup K=I} a_J\; a_K = 0$.

If f is m-th order correlation-immune, then $f \in \mathcal{D}(m,n)$.

If f is m-resilient, then for every multi-index I whose size is greater than or equal to $n-m$, the coefficient of x^I in the NNF of g is zero, since g has numerical degree at most $n-m-1$. Thus $\bigoplus_{\{J,K\}\,|\,J\cup K=I} b_J\; b_K = 0.$ □

Notice that if f is m-resilient and if $|I| > n-m$, then the condition $J \cup K = I$ and the fact that f has algebraic degree at most $n-m-1$ imply that J and K must have at least size 2; thus $\bigoplus_{\{J,K\}\,|\,J\cup K=I} b_J\; b_K = \bigoplus_{\{J,K\}\,|\,J\cup K=I} a_J\; a_K.$

Remark Divisibility by 8 (instead of 4) gives one more equality satisfied by the b_I's: according to relation (5), the coefficient of x^I in the NNF of g is congruent modulo 8 to

$$b_I - 2 \bigoplus_{\{J,K\}\,|\,J\cup K=I} b_J\; b_K + 4\left(\bigoplus_{\{J,K,L\}\,|\,J\cup K\cup L=I} b_J\; b_K\; b_L + \bigoplus_{\substack{\{\{J,K\},\{L,M\}\}\,|\\ J\cup K=I;\,L\cup M=I}} b_J\; b_K\; b_L\; b_M \right)$$

(indeed any sum of bits $\sum_{j\in J} u_j$ is congruent to $\bigoplus_{j\in J} u_j + 2\bigoplus_{\{j,k\}\subseteq J} u_j u_k$ modulo 4, and this can be applied to the sum $\sum_{\{J,K\}\,|\,J\cup K=I} b_J\; b_K$). We deduce that, additionally,

$$\bigoplus_{\{J,K,L\}\,|\,J\cup K\cup L=I} b_J\; b_K\; b_L = \bigoplus_{\substack{\{\{J,K\},\{L,M\}\}\,|\\ J\cup K=I;\,L\cup M=I}} b_J\; b_K\; b_L\; b_M$$

if $f \in \mathcal{D}(m,n)$, $m \geq 3$ and $|I| \geq n-m+3$; or if $f \in \mathcal{C}(m,n)$, $m \geq 2$ and $|I| \geq n-m+2$; or if f is bent, $n \geq 8$ and $|I| \geq \frac{n}{2}+3$; or if f is m-th order correlation-immune and $|I| \geq n-m+3$; or if f is m-resilient and $|I| \geq n-m$. It is not clear to us, however, how to use this equation to obtain further constraints on the numbers of various types of functions.

4 Dependence and Bounds

In this section we use Theorem 3.1 to obtain bounds on the numbers of bent, resilient, and correlation-immune functions and on the sizes of the sets $\mathcal{D}(m,n)$ and $\mathcal{C}(m,n)$. Our strategy is to show that certain coefficients depend on other coefficients.

In the cases of bent and correlation immune functions and in the cases of the sets $\mathcal{D}(m,n)$ and $\mathcal{C}(m,n)$, we are trying to bound the size of a set $\mathcal{E}(d,n)$ of functions $f(x) = \sum_{I\subseteq\{1,2,\cdots,n\}} a_I x^I \in \mathcal{B}(d,n)$ such that for all I with $|I| \geq d+2$, we have

$$\bigoplus_{\{J,K\}:J\cup K=I} a_J a_K = 0. \qquad (6)$$

In the case of resilient functions, we are trying to bound a similar set where the I are only constrained to have size at least $d+1$.

We obtain bounds by counting within certain subsets of $\mathcal{B}(d,n)$. Specifically, if $\mathcal{A}(d,n)$ is the set of homogeneous polynomials of degree d in $x_1,\cdots,x_n$, then we have $\mathcal{B}(d,n) = \mathcal{B}(d-1,n) \cup (\cup_{h\in\mathcal{A}(d,n)} h + \mathcal{B}(d-1,n))$. Fix $h(x) = \sum_{|I|=d} a_I x^I \in \mathcal{A}(d,n)$. An element of $\mathcal{E}(d,n) \cap (h + \mathcal{B}(d-1,n))$ is determined by a choice of a_I for each I of size less than or equal to $d-1$ satisfying equation (6).

Lemma 4.1 *Let n, d and l be positive integers such that $d \leq n$ and $l \leq \min(d-1, n-d)$. Denote by $\mathcal{E}_l(d,n)$ the set of functions $f(x) = \sum_{I\subseteq\{1,2,\cdots,n\}} a_I x^I \in \mathcal{B}(d,n)$ such that for all I with $|I| \geq d+l$, we have $\bigoplus_{\{J,K\}:J\cup K=I} a_J a_K = 0$. Let $f \in \mathcal{E}_l(d,n)$ have degree d and let J be a multi-index of cardinality d such that the coefficient a_J of x^J in the ANF of f equals 1. The coefficients a_K with $K \cap J = \emptyset$ and $l \leq |K| \leq d-1$ in the ANF of f are then completely determined by the coefficients a_L with $L \cap J \neq \emptyset$.*

Proof: Let I be any multi-index containing J and let $K = I - J$. In the equation (6) corresponding to I, the coefficient a_K appears only in the term $a_J a_K$ since if $a_L a_K$ appears, then $L \cup K = I$, so $J \subseteq L$, which is only possible if $J = L$ if $a_L = 1$. Furthermore, suppose I' is any other multi-index containing J. If a_K appeared in a term $a_L a_K$ in the equation corresponding to I', then we would have $L \cup K = I'$. Thus $J \subseteq L$ from which it follows that $I' = I$ (if $a_L = 1$). Thus a_K appears in only one equation corresponding to an I containing J, and that equation is of the form $a_K +$ (terms involving only a_Ls with $J \cap L \neq \emptyset$). The lemma follows. $\square$

It follows that

$$|\mathcal{E}_l(d,n) \cap (h + \mathcal{B}(d-1,n))| \leq \frac{B(d-1,n)}{2^{\sum_{i=l}^{\min(d-1,n-d)} \binom{n-d}{i}}}.$$

Summing over h we immediately obtain that

$$|\mathcal{E}_l(d,n)| \leq \frac{B(d,n) - B(d-1,n)}{2^{\sum_{i=l}^{\min(d-1,n-d)} \binom{n-d}{i}}} + B(d-1,n).$$

We can improve this bound when $d \leq n-d$ (or, equivalently, $d \leq n/2$) by considering the coefficients a_K with $|K| = d$. From here on let

$$\epsilon = \frac{1}{2^{\binom{n-1}{d-1} - \binom{n-1-d}{d-1} - 1}}.$$

Lemma 4.2 *Let $d \leq n/2$. The number of homogeneous degree d functions h in n variables such that equation (6) holds for every multi-index I of size $2d$ is at most $2^{\binom{n}{d}-\binom{n-d}{d}}(1+\epsilon)$.*

Proof: Let $T(d,n)$ denote the number of homogeneous degree d functions h in n variables such that equation (6) holds for every multi-index I of size $2d$. Let $\mathcal{J} = \{J : n \in J, |J| = d\}$ and let $J_1, J_2, \cdots, J_t$, with $t = \binom{n-1}{d-1}$ be an arbitrary enumeration of $\mathcal{J}$. Let S_i be the set of homogeneous degree d functions $h(x) = \sum_{K:|K|=d} a_K x^K$ with $a_{J_\ell} = 0$ for $\ell < i$ and $a_{J_i} = 1$. Then

$$T(d,n) = T(d,n-1) + \sum_{i=1}^{t} |S_i|. \tag{7}$$

To bound $|S_i|$, we consider equation (6) with $a_{J_\ell} = 0$ for $\ell < i$ and $a_{J_i} = 1$. There are $\binom{n-d}{d}$ equations for multi-indices I of size $2d$ with with $J_i \subseteq I$. Each such equation determines a_{I-J_i} as a sum of terms of the form $a_K a_L$ with $K \cup L = I$. Neither K nor L can be of the form $I' - J_i$ for a multi-index I' of size $2d$ since each of K and L must contain some element of J_i. Also, $I - J_i$ cannot equal J_ℓ for $\ell < i$ since any such J_ℓ contains n and $I - J_i$ does not. Thus S_i is contained in a linear subspace of dimension at most $\binom{n}{d} - i - \binom{n-d}{d}$. It follows from equation (7) that

$$\begin{aligned}
T(d,n) &\leq T(d,n-1) + \sum_{i=1}^{t} 2^{\binom{n}{d}-i-\binom{n-d}{d}} \\
&\leq T(d,n-1) + 2^{\binom{n}{d}-\binom{n-d}{d}} \\
&= T(d,2d-1) + \sum_{k=2d}^{n} 2^{\binom{k}{d}-\binom{k-d}{d}} \\
&= 2^{\binom{2d-1}{d}} + \sum_{k=2d}^{n} 2^{\binom{k}{d}-\binom{k-d}{d}}.
\end{aligned}$$

The first term is less than the term with $k = 2d$, and for every k, the term indexed by k is at most one half the term indexed by $k+1$, since $\binom{k+1}{d} - \binom{k+1-d}{d} - \binom{k}{d} + \binom{k-d}{d} = \binom{k}{d-1} - \binom{k-d}{d-1} \geq 1$. Thus

$$\begin{aligned}
T(d,n) &\leq 2^{\binom{n}{d}-\binom{n-d}{d}} + 2^{\binom{n-1}{d}-\binom{n-1-d}{d}+1} \\
&= 2^{\binom{n}{d}-\binom{n-d}{d}}\left(1 + \frac{1}{2^{\binom{n-1}{d-1}-\binom{n-1-d}{d-1}-1}}\right)
\end{aligned}$$

$$= \quad 2^{\binom{n}{d}-\binom{n-d}{d}}(1+\epsilon).$$

□

Thus we have the following.

Theorem 4.3 *Let l be a positive integer smaller than* $\min(d-1, n-d)$. *If $d \leq n/2$, then*

$$|\mathcal{E}_l(d,n)| \leq \frac{B(d,n)(1+\epsilon)}{2^{\sum_{i=l}^{d}\binom{n-d}{i}}} + B(d-1,n),$$

where $\epsilon = 1/2^{\Omega((2^n/n)^{1/2})}$. If $d > n/2$, then

$$|\mathcal{E}_l(d,n)| \leq \frac{B(d,n) - B(d-1,n)}{2^{2^{n-d}-\sum_{i=0}^{l-1}\binom{n-d}{i}}} + B(d-1,n).$$

Combining this with Theorem 3.1, we have the following bounds on the numbers of bent, correlation immune, and resilient functions and on the sizes of the sets $\mathcal{D}(mm,n)$ and $\mathcal{C}(m-1,n)$.

Corollary 4.4 *For $n \geq 6$ even, the number of bent functions in n variables is at most*

$$\frac{B(n/2,n)(1+\epsilon)}{2^{2^{n/2}-n/2-1}} + B(n/2-1,n) = 2^{2^{n-1}+\binom{n}{n/2}/2-2^{n/2}+n/2+1}(1+\epsilon) + 2^{2^{n-1}-\binom{n}{n/2}/2}.$$

If $2 \leq n/2 \leq m < n$, then the number of m-th order correlation immune functions in n variables and the sizes of the sets $\mathcal{D}(m,n)$ and $\mathcal{C}(m-1,n)$ (with $m > 2$ in this case) are at most

$$\frac{2^{m+1}B(n-m,n)(1+\epsilon)}{B(n-m,m)} + B(n-m-1,n),$$

where $\epsilon = 1/2^{\Omega((2^n/n)^{1/2})}$. If $2 \leq m < n/2$, then the number of m-th order correlation immune functions in n variables and the sizes of the sets $\mathcal{D}(m,n)$ and $\mathcal{C}(m-1,n)$ (with $m > 2$) are at most

$$\frac{B(n-m,n) - B(n-m-1,n)}{2^{2^m-m-1}} + B(n-m-1,n).$$

If $n/2 \leq m < n$, then the number of $(m-1)$-resilient functions in n variables is at most

$$\frac{2B(n-m,n)(1+\epsilon)}{B(n-m,m)} + B(n-m-1,n),$$

where $\epsilon = 1/2^{\Omega((2^n/n)^{1/2})}$. If $2 \leq m < n/2$, then the number of $(m-1)$-resilient functions in n variables is at most

$$\frac{B(n-m,n) - B(n-m-1,n)}{2^{2^m-1}} + B(n-m-1,n).$$

5 Conclusions and Possible Improvements

We have seen that the numbers of bent, correlation immune, and resilient functions can be bounded by counting independent equations that arise from divisibility properties of the Walsh coefficients of functions. These bounds are better than previously known bounds when $n-m$ is small and at least 3, as illustrated in Tables 2 and 3 (see appendix). In fact our bound is of the form $2^{p(n)}$ where $p(n)$ is a polynomial of degree d (with coefficients depending on d), and Schneider's bound is of the form $2^{p(n)}$ where $p(n)$ is a polynomial of degree $d+1$ (with coefficients depending on d). Thus if we fix $n-m$ (and thus fix d), then for n sufficiently large our bound is smaller than Schneider's.

In fact, the bounds we have obtained are not sharp. We can see this, for instance, in the case of bent functions in six variables. It is known that there are approximately 2^{32} such functions. The naive bound is 2^{42}, and our bound is about 2^{38}. We might obtain some small improvement by strengthening the results in Lemma 4.2, but this will only reduce ϵ. We can obtain much greater improvements if we count more equations in Lemma 4.1. In choosing a general homogeneous function h of degree d in Section 4, we assumed only that it had at least one nonzero term. This is the case only for few functions h. In fact if h can be written in the form h_1h_2 where h_1 and h_2 depend on disjoint sets of variables and h_1 is a quadratic function of rank greater than 1 then one can obtain a much larger set of equations. The details of counting these equations and of counting the number of such h are beyond the scope of the current paper.

Acknowledgements

The authors are grateful to Harald Niedereitter and the Institute for Mathematical Sciences at the National University of Singapore for bringing them together and for allowing them to use the facilities of the Institute during the summer of 2001.

References

[1] E.F. Assmus and J.D. Key, *Designs and their Codes*, Cambridge Univ. Press, 1992.

[2] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, On correlation-immune functions, *Advances in Cryptology: Crypto '91, Proceedings, Lecture Notes in Computer Science* 576, (1991), pp. 86-100.

[3] A. Canteaut and M. Trabbia, Improved fast correlation attacks using parity-check equations of weight 4 and 5, *Advances in Cryptology-EUROCRYPT 2000, Lecture notes in computer science* 1807, (2000), pp. 573-588.

[4] C. Carlet, Two new classes of bent functions, *EUROCRYPT' 93, Advances in Cryptology, Lecture Notes in Computer Science* 765, (1994), pp. 77-101.

[5] C. Carlet, Recent results on binary bent functions, *International Conference on Combinatorics, Information Theory and Statistics; Journal of Combinatorics, Information and System Sciences* 24, n° 3-4, (1999), pp. 275-291

[6] C. Carlet, On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions, to appear in the *Proceedings of SETA 2001 (Sequences and their Applications, Bergen, Norway, May 2001)*, published by *Discrete Mathematics and Theoretical Computer Science Series*, Springer-Verlag.

[7] C. Carlet and P. Guillot, A new representation of Boolean functions, *Proceedings of AAECC'13, Lecture Notes in Computer Science* 1719, (1999), pp. 94-103.

[8] C. Carlet and P. Guillot, Bent, resilient functions and the Numerical Normal Form, *DIMACS Series in Discrete Mathematics and Theoretical Computer Science,* 56, (2001), pp. 87-96.

[9] C. Carlet. and P. Sarkar, Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions", to appear in *Finite fields Appl.* (2001).

[10] J. F. Dillon, *Elementary Hadamard Difference sets.* Ph.D. Thesis, Univ. of Maryland (1974).

[11] J. F. Dillon, Elementary Hadamard Difference sets, *Proc. Sixth S-E Conf. Comb. Graph Theory and Comp.*, F. Hoffman et al. (Eds), Winnipeg, Utilitas Math, (1975), pp. 237-249.

[12] P. Guillot. *Completed GPS Covers All Bent Functions.* Journal of Combinatorial Theory, Series A 93, 242-260 (2001)

[13] X.D. Hou. *On the coefficients of binary bent functions*, Proceedings of the American Mathematical Society, S 0002-9939(99)05146-1. Article electronically published on August 17, 1999.

[14] X.D. Hou and and P. Langevin. *Results on bent functions*, Journal of Combinatorial Theory, Series A, 80, 232-246 (1997).

[15] T. Johansson and F. Jönsson, Improved fast correlation attack on stream ciphers via convolutional codes. *Advances in Cryptology - EUROCRYPT'99, Lecture Notes in Computer Science* 1592, (1999), pp. 347–362.

[16] T. Johansson and F. Jönsson, Fast correlation attacks based on turbo code techniques. *Advances in Cryptology - CRYPTO'99, Lecture Notes in Computer Science* 1666, (1999), pp. 181–197.

[17] R. Lidl, and H. Niederreiter, *Finite Fields* in *Encyclopedia of Mathematics Vol. 20,* Cambridge University Press: Cambridge, 1983.

[18] F. J. Mac Williams and N. J. Sloane, *The theory of error-correcting codes*, Amsterdam, North Holland, 1977.

[19] S. Maitra et P. Sarkar, Enumeration of correlation-immune Boolean functions, *ACISP*, (1999), pp. 12-25.

[20] S. Maitra et P. Sarkar, Hamming weights of correlation-immune Boolean functions, *Information Processing Letters* 71, (1999), pp. 149-153.

[21] R. J. McEliece, Weight congruences for p-ary cyclic codes, *Discrete Math.* 3, (1972), pp. 177-192.

[22] W. Meier and O. Staffelbach, Nonlinearity Criteria for Cryptographic Functions, *Advances in Cryptology, EUROCRYPT' 89, Lecture Notes in Computer Science* 434, (1990), pp. 549-562.

[23] C. J. Mitchell, Enumerating Boolean functions of cryptographic signifiance. *Journal of Cryptology* 2, (1990), pp. 155-170.

[24] J. D. Olsen, R. A. Scholtz and L. R. Welch, Bent function sequences, *IEEE Trans. on Inf. Theory*, IT- 28, n° 6, (1982).

[25] S. M. Park, S. Lee, S. H. Sung et K. Kim, Improving bounds for the number of correlation-immune Boolean functions. *Information Processing Letters* 61, (1997), pp. 209-212.

[26] B. Preneel, *Analysis and Design of Cryptographic Hash Functions*, Ph. D. Thesis, Katholieke Universiteit Leuven, K. Mercierlaan 94, 3001 Leuven, Belgium (1993).

[27] O. S. Rothaus, On bent functions, *J. Comb. Theory* 20A, (1976), pp. 300-305.

[28] P. Sarkar and S. Maitra, Nonlinearity Bounds and Constructions of Resilient Boolean Functions, *Crypto 2000, Advances in Cryptology, Lecture Notes in Computer Science* 1880, ed. Mihir Bellare, (2000), pp. 515-532.

[29] M. Schneider, A note on the construction and upper bounds of correlation-immune functions, *6th IMA Conference*, (1997), pp. 295-306.

[30] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, *IEEE Transactions on Information theory* IT-30, (1984), pp. 776-780.

[31] T. Siegenthaler, Decrypting a Class of Stream Ciphers Using Ciphertext Only, *IEEE Transactions on Computers* C-34, n° 1, (1985), pp. 81-85.

[32] Y. Yang and B. Guo, Further enumerating Boolean functions of cryptographic signifiance, *Journal of Cryptology* 8, (1995), pp. 115-122.

[33] Xiao Guo-Zhen and J. L. Massey, A Spectral Characterization of Correlation-Immune Combining Functions, *IEEE Transactions on Information Theory* 34, n° 3, (1988), pp. 569-571.

[34] Jian-Zhou Zhang, Zhi-Sheng You, and Zheng-Liang Li, Enumeration of binary orthogonal arrays of strength 1, *Discrete Mathematics*, to appear.

A Tables

n	$n-m=3$	$n-m=4$	$n-m=5$	$n-m=6$	$n-m=7$
6	6.3×10^{3}	3.5×10^{10}	1.8×10^{16}	–	–
7	2.5×10^{4}	1.1×10^{15}	5.0×10^{27}	1.7×10^{35}	–
8	9.9×10^{4}	3.0×10^{20}	3.6×10^{44}	6.6×10^{63}	2.8×10^{73}
9	3.9×10^{5}	6.2×10^{26}	1.1×10^{68}	3.0×10^{110}	1.5×10^{138}
10	1.6×10^{6}	1.0×10^{34}	2.2×10^{99}	5.3×10^{182}	5.7×10^{250}
11	6.3×10^{6}	1.4×10^{42}	4.8×10^{139}	3.9×10^{289}	1×10^{438}
12	2.5×10^{7}	1.5×10^{51}	1.8×10^{190}	4.1×10^{441}	4.2×10^{736}
13	1×10^{8}	1.3×10^{61}	1.8×10^{252}	6.7×10^{650}	1.2×10^{1195}
14	4×10^{8}	8.8×10^{71}	8.3×10^{326}	6.1×10^{930}	2.6×10^{1875}
15	1.6×10^{9}	4.9×10^{83}	2.6×10^{415}	3.4×10^{1296}	9.3×10^{2854}

Table 2: Bounds on the number of m-resilient functions, m large

n	$n-m=3$	$n-m=4$	$n-m=5$	$n-m=6$	$n-m=7$
6	1.5×10^{2}	6.3	3.6×10^{-1}	–	–
7	3.7×10^{3}	1.9×10^{2}	2.9×10^{-1}	7.2×10^{-2}	–
8	1.8×10^{5}	6.6×10^{4}	8.4×10^{-1}	2.6×10^{-3}	1×10^{-2}
9	1.7×10^{7}	5.6×10^{8}	5.4×10	1.7×10^{-5}	3.2×10^{-6}
10	3.3×10^{9}	2.3×10^{14}	9.3×10^{5}	5.6×10^{-8}	4.2×10^{-13}
11	1.3×10^{12}	9×10^{21}	1×10^{14}	1.5×10^{-9}	7.2×10^{-25}
12	9.9×10^{14}	6.8×10^{31}	3.5×10^{27}	7.2×10^{-8}	1×10^{-42}
13	1.5×10^{18}	2×10^{44}	3.4×10^{48}	2.7×10	1×10^{-64}
14	4.7×10^{21}	4.4×10^{59}	1.9×10^{79}	1.9×10^{22}	8.8×10^{-95}
15	2.9×10^{25}	1.5×10^{78}	2.3×10^{122}	5.2×10^{62}	2.8×10^{-119}

Table 3: (Schneider's bound/New bound) for m-resilient functions