On Relationships among Avalanche, Nonlinearity and Correlation Immunity

Yuliang Zheng[1] and Xian-Mo Zhang[2]

[1] Monash University, Frankston, Melbourne, VIC 3199, Australia
yuliang.zheng@monash.edu.au, http://www.netcomp.monash.edu.au/links/
[2] The University of Wollongong, Wollongong, NSW 2522, Australia
xianmo@cs.uow.edu.au

Abstract. We establish, for the first time, an explicit and simple lower bound on the nonlinearity N_f of a Boolean function f of n variables satisfying the avalanche criterion of degree p, namely, $N_f \geq 2^{n-1} - 2^{n-1-\frac{1}{2}p}$. We also show that the lower bound is tight, and identify all the functions whose nonlinearity attains the lower bound. As a further contribution of this paper, we prove that except for very few cases, the sum of the degree of avalanche and the order of correlation immunity of a Boolean function of n variables is at most $n-2$. These new results further highlight the significance of the fact that while avalanche property is in harmony with nonlinearity, it goes against correlation immunity.

Key Words:

Avalanche Criterion, Boolean Functions, Correlation Immunity, Nonlinearity, Propagation Criterion.

1 Introduction

Confusion and diffusion, introduced by Shannon [16], are two important principles used in the design of secret key cryptographic systems. These principles can be enforced by using some of the nonlinear properties of Boolean functions involved in a cryptographic transformation. More specifically, a high nonlinearity generally has a positive impact on confusion, whereas a high degree of avalanche enhances the effect of diffusion. Nevertheless, it is also important to note that some nonlinear properties contradict others. These motivate researchers to investigate into relationships among various nonlinear properties of Boolean functions.

One can consider three different relationships among nonlinearity, avalanche and correlation immunity, namely, nonlinearity and avalanche, nonlinearity and correlation immunity, and avalanche and correlation immunity. Zhang and Zheng [20] studied how avalanche property influences nonlinearity by establishing a number of upper and lower bounds on nonlinearity. Carlet [3] showed that one may determine a number of different nonlinear properties of a Boolean function, if the function satisfies the avalanche criterion of a high degree. Zheng and Zhang [26] proved that Boolean functions satisfying the avalanche criterion in a hyper-space coincide with certain bent functions. They also established close relationships among plateaued functions with a maximum order, bent functions and the first order correlation immune functions [24]. Seberry, Zhang and Zheng were the first to research into relationships between nonlinearity and correlation immunity [14]. Very recently Zheng and Zhang have succeeded in deriving a new tight upper bound on the nonlinearity of high order correlation immune functions [25]. In the same paper they have also shown that correlation immune functions whose nonlinearity meets the tight upper bound coincide with plateaued functions introduced in [24, 23]. All these results help further understand how nonlinearity and correlation immunity are at odds with each other.

The aim of this work is to widen our understanding of other connections among nonlinearity properties of Boolean functions, with a specific focus on relationships between nonlinearity and avalanche, and between avalanche and correlation immunity. We prove that if a function f of n variables satisfies the avalanche criterion of degree p, then its nonlinearity N_f must satisfy the condition of $N_f \geq 2^{n-1} - 2^{n-1-\frac{1}{2}p}$. We also identify the cases when the equality holds, and characterize those functions that have the minimum nonlinearity. This result tells us that a high degree of avalanche guarantees a high nonlinearity.

In the second part of this paper, we look into the question of how avalanche and correlation immunity hold back each other. We prove that with very few exceptions, the sum of the degree of avalanche property and the order of correlation immunity of a Boolean function with n variables is less than or equal to $n-2$. This result clearly tells us that we cannot expect a function to achieve both a high degree of avalanche and a high order of correlation immunity.

2 Boolean Functions

We consider functions from V_n to $GF(2)$ (or simply functions on V_n), where V_n is the vector space of n tuples of elements from $GF(2)$. The *truth table* of a function f on V_n is a $(0,1)$-sequence defined by $(f(\alpha_0),\ f(\alpha_1), \ldots,\ f(\alpha_{2^n-1}))$, and the *sequence* of f is a $(1,-1)$-sequence defined by $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$, where $\alpha_0 = (0,\ldots,0,0)$, $\alpha_1 = (0,\ldots,0,1)$, $\ldots$, $\alpha_{2^n-1} = (1,\ldots,1,1)$. A function is said to be *balanced* if its truth table contains 2^{n-1} zeros and an equal number of ones. Otherwise it called unbalanced.

The *matrix* of f is a $(1,-1)$-matrix of order 2^n defined by $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$ where $\oplus$ denotes the addition in V_n.

Given two sequences $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$, their *component-wise product* is defined by $\tilde{a} * \tilde{b} = (a_1 b_1, \cdots, a_m b_m)$. In particular, if $m = 2^n$ and $\tilde{a}$, $\tilde{b}$ are the sequences of functions f and g on V_n respectively, then $\tilde{a} * \tilde{b}$ is the sequence of $f \oplus g$ where $\oplus$ denotes the addition in $GF(2)$.

Let $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$ be two sequences or vectors, the *scalar product* of $\tilde{a}$ and $\tilde{b}$, denoted by $\langle \tilde{a}, \tilde{b} \rangle$, is defined as the sum of the component-wise multiplications. In particular, when $\tilde{a}$ and $\tilde{b}$ are from V_m, $\langle \tilde{a}, \tilde{b} \rangle = a_1 b_1 \oplus \cdots \oplus a_m b_m$, where the addition and multiplication are over $GF(2)$, and when $\tilde{a}$ and $\tilde{b}$ are $(1, -1)$-sequences, $\langle \tilde{a}, \tilde{b} \rangle = \sum_{i=1}^{m} a_i b_i$, where the addition and multiplication are over the reals.

An *affine* function f on V_n is a function that takes the form of $f(x_1, \ldots, x_n) = a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$.

A $(1, -1)$-matrix N of order n is called a *Hadamard* matrix if $NN^T = nI_n$, where N^T is the transpose of N and I_n is the identity matrix of order n. A Sylvester-Hadamard matrix of order 2^n, denoted by H_n, is generated by the following recursive relation

$$H_0 = 1,\ H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix},\ n = 1,\, 2, \ldots .$$

Let ℓ_i, $0 \le i \le 2^n - 1$, be the i row of H_n. It is known that ℓ_i is the sequence of a linear function $\varphi_i(x)$ on V_n, defined by the scalar product $\varphi_i(x) = \langle \alpha_i, x \rangle$, where α_i is the binary representation of an integer i.

The *Hamming weight* of a $(0, 1)$-sequence ξ, denoted by $HW(\xi)$, is the number of ones in the sequence. Given two functions f and g on V_n, the *Hamming distance* $d(f, g)$ between them is defined as the Hamming weight of the truth table of $f(x) \oplus g(x)$, where $x = (x_1, \ldots, x_n)$.

3 Cryptographic Criteria of Boolean Functions

The following criteria for cryptographic Boolean functions are often considered: (1) **balance**, (2) **nonlinearity**, (3) **avalanche**, (4) **correlation immunity**, (5) **algebraic degree**, (6) absence of non-zero **linear structures**. In this paper we focus on avalanche, nonlinearity and correlation immunity.

Parseval's equation (Page 416 [8]) is a useful tool in this research: Let f be a function on V_n and ξ denote the sequence of f. Then $\sum_{i=0}^{2^n-1} \langle \xi, \ell_i \rangle^2 = 2^{2n}$ where ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$.

The *nonlinearity* of a function f on V_n, denoted by N_f, is the minimal Hamming distance between f and all affine functions on V_n, i.e.,

$$N_f = \min_{i=1,2,\ldots,2^{n+1}} d(f, \psi_i)$$

where ψ_1, ψ_2, …, $\psi_{2^{n+1}}$ are all the affine functions on V_n. High nonlinearity can be used to resist a linear attack [9]. The following characterization of nonlinearity will be useful (for a proof see for instance [10]).

Lemma 1. *The nonlinearity of f on V_n can be expressed by*

$$N_f = 2^{n-1} - \frac{1}{2} \max\{|\langle \xi, \ell_i \rangle|, 0 \le i \le 2^n - 1\}$$

where ξ is the sequence of f and ℓ_0, …, ℓ_{2^n-1} are the rows of H_n, namely, the sequences of linear functions on V_n.

From Lemma 1 and Parseval's equation, it is easy to verify that $N_f \leq 2^{n-1} - 2^{\frac{1}{2}n-1}$ for any function f on V_n. A function f on V_n is called a *bent function* if $\langle \xi, \ell_i \rangle^2 = 2^n$ for every i, $0 \leq i \leq 2^n - 1$ [13]. Hence f is a bent function on V_n if and only $N_f = 2^{n-1} - 2^{\frac{1}{2}n-1}$. It is known that a bent function on V_n exists only when n is even.

Let f be a function on V_n. We say that f satisfies the *avalanche criterion with respect to* α if $f(x) \oplus f(x \oplus \alpha)$ is a balanced function, where $x = (x_1, \ldots, x_n)$ and α is a vector in V_n. Furthermore f is said to satisfy the *avalanche criterion of degree* k if it satisfies the avalanche criterion with respect to every non-zero vector α whose Hamming weight is not larger than k. [1] From [13], a function f on V_n is bent if and only if f satisfies the avalanche criterion of degree n. Note that the *strict avalanche criterion (SAC)* [18] is the same as the avalanche criterion of degree one.

Let f be a function on V_n. For a vector $\alpha \in V_n$, denote by $\xi(\alpha)$ the sequence of $f(x \oplus \alpha)$. Thus $\xi(0)$ is the sequence of f itself and $\xi(0) * \xi(\alpha)$ is the sequence of $f(x) \oplus f(x \oplus \alpha)$. Set $\Delta_f(\alpha) = \langle \xi(0), \xi(\alpha) \rangle$, the scalar product of $\xi(0)$ and $\xi(\alpha)$. $\Delta(\alpha)$ is called the auto-correlation of f with a shift α. We omit the subscript of $\Delta_f(\alpha)$ if no confusion occurs. Obviously, $\Delta(\alpha) = 0$ if and only if $f(x) \oplus f(x \oplus \alpha)$ is balanced, i.e., f satisfies the avalanche criterion with respect to α. In the case that f does not satisfy the avalanche criterion with respect to a vector α, it is desirable that $f(x) \oplus f(x \oplus \alpha)$ is almost balanced. Namely we require that $|\Delta_f(\alpha)|$ take a small value.

Let f be a function on V_n. $\alpha \in V_n$ is called a *linear structure* of f if $|\Delta(\alpha)| = 2^n$ (i.e., $f(x) \oplus f(x \oplus \alpha)$ is a constant). For any function f, we have $\Delta(\alpha_0) = 2^n$, where α_0 is the zero vector on V_n. It is easy to verify that the set of all linear structures of a function f form a linear subspace of V_n, whose dimension is called the *linearity of* f. A non-zero linear structure is cryptographically undesirable. It is also well-known that if f has non-zero linear structures, then there exists a nonsingular $n \times n$ matrix B over $GF(2)$ such that $f(xB) = g(y) \oplus \psi(z)$, where $x = (y, z)$, $y \in V_p$, $z \in V_q$, g is a function on V_p that has no non-zero linear structures, and ψ is a linear function on V_q.

The following lemma is the re-statement of a relation proved in Section 2 of [4].

Lemma 2. *For every function f on V_n, we have*

$$(\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1}))H_n = (\langle \xi, \ell_0 \rangle^2, \langle \xi, \ell_1 \rangle^2, \ldots, \langle \xi, \ell_{2^n-1} \rangle^2).$$

where ξ denotes the sequence of f, ℓ_i is the ith row of H_n, and α_i is the vector in V_n that corresponds to the binary representation of i, $i = 0, 1, \ldots, 2^n - 1$.

[1] The avalanche criterion was called the propagation criterion in [12], as well as in all our earlier papers dealing with the subject. Historically, Feistel was apparently the first person who coined the term of "avalanche" and realized its importance in the design of a block cipher [6]. According to Coppersmith [5], a member of the team who designed DES, avalanche properties were employed in selecting the S-boxes used in the cipher, which contributed to the strength of the cipher against various attacks including differential [1] and linear [9] attacks.

The concept of correlation immune functions was introduced by Siegenthaler [17]. Xiao and Massey gave an equivalent definition [2, 7]: A function f on V_n is called a *kth-order correlation immune function* if $\sum_{x\in V_n} f(x)(-1)^{\langle\beta,x\rangle} = 0$ for all $\beta \in V_n$ with $1 \le HW(\beta) \le k$, where in the the sum, $f(x)$ and $\langle\beta,x\rangle$ are regarded as real-valued functions. From Section 4.2 of [2], a correlation immune function can also be equivalently restated as follows: Let f be a function on V_n and let ξ be its sequence. Then f is called a *kth-order correlation immune function* if $\langle\xi,\ell\rangle = 0$ for every ℓ, where ℓ is the sequence of a linear function $\varphi(x) = \langle\alpha,x\rangle$ on V_n constrained by $1 \le HW(\alpha) \le k$. It should be noted that $\langle\xi,\ell\rangle = 0$, if and only if $f(x)\oplus\varphi(x)$ is balanced. Hence f is a kth-order correlation immune function if and only if $f(x)\oplus\varphi(x)$ is balanced for each linear function $\varphi(x) = \langle\alpha,x\rangle$ on V_n where $1 \le HW(\alpha) \le k$. Correlation immune functions are used in the design of running-key generators in stream ciphers to resist a correlation attack. Relevant discussions on correlation immune functions, and more generally on resilient functions, can be found in [22].

4 A Tight Lower Bound on Nonlinearity of Boolean Functions Satisfying Avalanche Criterion of Degree p

Let $(a_0, a_1, \dots, a_{2^n-1})$ and $(b_0, b_1, \dots, b_{2^n-1})$ be two real-valued sequences of length 2^n, satisfying

$$(a_0, a_1, \dots, a_{2^n-1})H_n = (b_0, b_1, \dots, b_{2^n-1}) \tag{1}$$

Let p be an integer with $1 \le p \le n-1$. Rewrite (1) as

$$(a_0, a_1, \dots, a_{2^n-1})(H_{n-p} \times H_p) = (b_0, b_1, \dots, b_{2^n-1}) \tag{2}$$

where $\times$ denotes the *Kronecker product* [19]. Let e_j denote the ith row of H_p, $j = 0, 1, \dots, 2^p-1$. For any fixed j with $0 \le j \le 2^p-1$, comparing the jth, $(j+2^p)$th, …, $(j+(2^{n-p}-1)2^p)$th terms in both sides of (2), we have

$$(a_0, a_1, \dots, a_{2^n-1})(H_{n-p} \times e_j^T) = (b_j, b_{j+2^p}, b_{j+2\cdot 2^p}, \dots, b_{j+(2^{n-p}-1)2^p})$$

Write $(a_0, a_1, \dots, a_{2^n-1}) = (\chi_0, \chi_1, \dots, \chi_{2^{n-p}-1})$ where each χ_i is of length 2^p. Then we have
$(\langle\chi_0, e_j\rangle, \langle\chi_1, e_j\rangle, \dots, \langle\chi_{2^{n-p}-1}, e_j\rangle)H_{n-p} = (b_j, b_{j+2^p}, b_{j+2\cdot 2^p}, \dots, b_{j+(2^{n-p}-1)2^p})$
or equivalently,

$$\begin{aligned}&2^{n-p}(\langle\chi_0, e_j\rangle, \langle\chi_1, e_j\rangle, \dots, \langle\chi_{2^{n-p}-1}, e_j\rangle)\\ &= (b_j, b_{j+2^p}, b_{j+2\cdot 2^p}, \dots, b_{j+(2^{n-p}-1)2^p})H_{n-p}\end{aligned} \tag{3}$$

Let ℓ_i denote the i row of H_{n-p}, where $j = 0, 1, \dots, 2^{n-p}-1$. In addition, write $(b_j, b_{j+2^p}, b_{j+2\cdot 2^p}, \dots, b_{j+(2^{n-p}-1)2^p}) = \lambda_j$, where $j = 0, 1, \dots, 2^p-1$. Comparing the ith terms in both sides of (3), we have $2^{n-p}\langle\chi_i, e_j\rangle = \langle\lambda_j, \ell_i\rangle$ where $\chi_i = (a_{i\cdot 2^p}, a_{1+i\cdot 2^p}, \dots, a_{2^p-1+i\cdot 2^p})$. These discussions lead to the following lemma.

Lemma 3. *Let $(a_0, a_1, \ldots, a_{2^n-1})$ and $(b_0, b_1, \ldots, b_{2^n-1})$ be two real-valued sequences of length 2^n, satisfying*

$$(a_0, a_1, \ldots, a_{2^n-1})H_n = (b_0, b_1, \ldots, b_{2^n-1})$$

Let p be an integer with $1 \le p \le n-1$. For any fixed i with $0 \le i \le 2^{n-p}-1$ and any fixed j with $0 \le j \le 2^p - 1$, let $\chi_i = (a_{i\cdot 2^p}, a_{1+i\cdot 2^p}, \ldots, a_{2^p-1+i\cdot 2^p})$ and $\lambda_j = (b_j, b_{j+2^p}, b_{j+2\cdot 2^p}, \ldots, b_{j+(2^{n-p}-1)2^p})$. Then we have

$$2^{n-p}\langle \chi_i, e_j\rangle = \langle \lambda_j, \ell_i\rangle,\ i = 0, 1, \ldots, 2^{n-p}-1,\ j = 0, 1, \ldots, 2^p - 1 \qquad (4)$$

where ℓ_i denotes the ith row of H_{n-p} and e_j denotes the jth row of H_p.

Lemma 3 can be viewed as a refined version of the Hadamard transformation (1), and it will be a useful mathematical tool in proving the following two lemmas. These two lemmas will then play a significant role in proving the main results of this paper.

Lemma 4. *Let f be a non-bent function on V_n, satisfying the avalanche criterion of degree p. Denote the sequence of f by ξ. If there exists a row L^* of H_n such that $|\langle \xi, L^*\rangle| = 2^{n-\frac{1}{2}p}$, then $\alpha_{2^{t+p}+2^p-1}$ is a non-zero linear structure of f, where $\alpha_{2^{t+p}+2^p-1}$ is the vector in V_n corresponding to the integer $2^{t+p}+2^p-1$, $t = 0, 1, \ldots, n-p-1$.*

Proof. First we note that $p > 0$. Since f is not bent, $p \le n-1$. Let us first rewrite the equality in Lemma 2 as follows

$$(\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1}))H_n = (\langle \xi, L_0\rangle^2, \langle \xi, L_1\rangle^2, \ldots, \langle \xi, L_{2^n-1}\rangle^2) \quad (5)$$

where α_i is the vector in V_n corresponding to the integer i, and L_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$. Set $i = 0$ in (4). Then we have $2^{n-p}\langle \chi_0, e_j\rangle = \langle \lambda_j, \ell_0\rangle$. Since f satisfies the avalanche criterion of degree p and $HW(\alpha_j) \le p$, $j = 1, \ldots 2^p - 1$, we have

$$\Delta(\alpha_0) = 2^n,\ \Delta(\alpha_1) = \cdots = \Delta(\alpha_{2^p-1}) = 0 \qquad (6)$$

Applying $2^{n-p}\langle \chi_0, e_j\rangle = \langle \lambda_j, \ell_0\rangle$ to (5), we obtain

$$2^{n-p}\Delta(\alpha_0) = \sum_{u=0}^{2^{n-p}-1} \langle \xi, L_{j+u\cdot 2^p}\rangle^2$$

or equivalently

$$\sum_{u=0}^{2^{n-p}-1} \langle \xi, L_{j+u\cdot 2^p}\rangle^2 = 2^{2n-p} \qquad (7)$$

Since L^* is a row of H_n, it can be expressed as $L^* = L_{j_0+u_0\cdot 2^p}$, where $0 \le j_0 \le 2^p - 1$ and $0 \le u_0 \le 2^{n-p}-1$. Set $j = j_0$ in (7), we have $\sum_{u=0}^{2^{n-p}-1}\langle \xi, L_{j_0+u\cdot 2^p}\rangle^2 = 2^{2n-p}$. From

$$\langle \xi, L_{j_0+u_0\cdot 2^p}\rangle^2 = \langle \xi, L^*\rangle^2 = 2^{2n-p} \qquad (8)$$

we have

$$\langle \xi, L_{j_0+u\cdot 2^p}\rangle = 0, \text{ for all } u,\ 0 \le u \le 2^{n-p}-1,\ u \ne u_0 \tag{9}$$

Set $i = 2^t$ and $j = j_0$ in Lemma 3, where $0 \le t \le n-p-1$, we have

$$2^{n-p}\langle \chi_{2^t}, e_{j_0}\rangle = \langle \lambda_{j_0}, \ell_{2^t}\rangle \tag{10}$$

where ℓ_{2^t} is the 2^tth row of H_{n-p} and e_{j_0} is the j_0th row of H_p, $j = 0, 1, \ldots, 2^p-1$. As f satisfies the avalanche criterion of degree p and $HW(\alpha_j) \le p$, $j = 2^{t+p}, 1+2^{t+p}, \ldots, 2^p-2+2^{t+p}$, we have

$$\varDelta(\alpha_{2^{t+p}}) = \varDelta(\alpha_{1+2^{t+p}}) = \cdots = \varDelta(\alpha_{2^p-2+2^{t+p}}) = 0 \tag{11}$$

Applying (10) to (5), and considering (8), (9) and (11), we have

$$2^{n-p}\varDelta(\alpha_{2^p-1+2^{p+t}}) = \pm 2^{2n-p}$$

and thus

$$\varDelta(\alpha_{2^p-1+2^{p+t}}) = \pm 2^n$$

This proves that $\alpha_{2^p-1+2^{p+t}}$ is indeed a non-zero linear structure of f, where $t = 0, 1, \ldots, n-p-1$. □

Lemma 5. *Let f be a non-bent function on V_n, satisfying the avalanche criterion of degree p. Denote the sequence of f by ξ. If there exists a row L^* of H_n, such that $|\langle \xi, L^*\rangle| = 2^{n-\frac{1}{2}p}$, then $p = n-1$ and n is odd.*

Proof. Since $|\langle \xi, L^*\rangle| = 2^{n-\frac{1}{2}p}$, p must be even. Due to $p > 0$, we must have $p \ge 2$. We now prove the lemma by contradiction. Assume that $p \ne n-1$. Since $p < n$, we have $p \le n-2$. As $|\langle \xi, L^*\rangle| = 2^{n-\frac{1}{2}p}$, from Lemma 4, $\alpha_{2^{t+p}+2^p-1}$ is a non-zero linear structure of f, where $t = 0, 1, \ldots, n-p-1$. Notice that $n-p-1 \ge 1$. Set $t = 0, 1$. Thus both $\alpha_{2^p+2^p-1}$ and $\alpha_{2^{p+1}+2^p-1}$ are non-zero linear structures of f. Since all the linear structures of a function form a linear subspace, $\alpha_{2^p+2^p-1} \oplus \alpha_{2^{p+1}+2^p-1}$ is also a linear structure of f. Hence

$$\varDelta(\alpha_{2^p+2^p-1} \oplus \alpha_{2^{p+1}+2^p-1}) = \pm 2^n \tag{12}$$

On the other hand, since f satisfies the avalanche criterion of degree p and $HW(\alpha_{2^p+2^p-1} \oplus \alpha_{2^{p+1}+2^p-1}) = 2 \le p$, we conclude that
$\varDelta(\alpha_{2^p+2^p-1} \oplus \alpha_{2^{p+1}+2^p-1}) = 0$. This contradicts (12). Thus we have $p > n-2$. The only possible value for p is $p = n-1$. Since p is even, n must be odd. □

Theorem 1. *Let f be a function on V_n, satisfying the avalanche criterion of degree p. Then*

(i) the nonlinearity N_f of f satisfies $N_f \ge 2^{n-1} - 2^{n-1-\frac{1}{2}p}$,
(ii) the equality in (i) holds if and only if one of the following two conditions holds:

(a) $p = n-1$, *n is odd and* $f(x) = g(x_1 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus h(x_1, \ldots, x_n)$, *where* $x = (x_1, \ldots, x_n)$, *g is a bent function on* V_{n-1}, *and h is an affine function on* V_n.

(b) $p = n$, *f is bent and n is even.*

Proof. Due to (7), i.e., $\sum_{u=0}^{2^{n-p}-1} \langle \xi, L_{j+u\cdot 2^p} \rangle^2 = 2^{2n-p}$, we have $\langle \xi, L_{j+u\cdot 2^p} \rangle^2 \leq 2^{2n-p}$. Since u and j are arbitrary, by using Lemma 1, we have $N_f \geq 2^{n-1} - 2^{n-1-\frac{1}{2}p}$. Now assume that

$$N_f = 2^{n-1} - 2^{n-1-\frac{1}{2}p} \tag{13}$$

From Lemma 1, there exists a row L^* of H_n such that $|\langle \xi, L^* \rangle| = 2^{n-\frac{1}{2}p}$. Two cases need to be considered: f is non-bent and f is bent. When f is non-bent, thanks to Lemma 5, we have $p = n-1$ and n is odd. Considering Proposition 1 of [3], we conclude that f must takes the form mentioned in (a). On the other hand, if f is bent, then $p = n$ and n is even. Hence (b) holds.

Conversely, assume that f takes the form in (a). Applying a nonsingular linear transformation on the variables, and considering Proposition 3 of [11], we have $N_f = 2N_g$. Since g is bent, we have $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$. Hence (13) holds, where $p = n-1$. On the other hand, it is obvious that (13) holds whenever (b) does. □

5 Relationships between Avalanche and Correlation Immunity

To prove the main theorems, we introduce two more results. The following lemma is part of Lemma 12 in [15].

Lemma 6. *Let* f_1 *be a function on* V_s *and* f_2 *be a function on* V_t. *Then* $f_1(x_1, \ldots, x_s) \oplus f_2(y_1, \ldots, y_t)$ *is a balanced function on* V_{s+t} *if* f_1 *or* f_2 *is balanced.*

Next we look at the structure of a function on V_n that satisfies the avalanche criterion of degree $n-1$.

Lemma 7. *Let f be a function on* V_n. *Then*

(i) f is non-bent and satisfies the avalanche criterion of degree $n-1$, *if and only if n is odd and* $f(x) = g(x_1 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus c_1x_1 \oplus \cdots \oplus c_nx_n \oplus c$, *where* $x = (x_1, \ldots, x_n)$, *g is a bent function on* V_{n-1}, *and* $c_1, \ldots, c_n$ *and c are all constants in* $GF(2)$,

(ii) f is balanced and satisfies the avalanche criterion of degree $n-1$, *if and only if n is odd and* $f(x) = g(x_1 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus c_1x_1 \oplus \cdots \oplus c_nx_n \oplus c$, *where g is a bent function on* V_{n-1}, *and* $c_1, \ldots, c_n$ *and c are all constant in* $GF(2)$, *satisfying* $\bigoplus_{j=1}^{n} c_j = 1$.

Proof. (i) holds due to Proposition 1 of [3].

Assume that f is balanced and satisfies the avalanche criterion of degree $n-1$. Since f is balanced, it is non-bent. From (i) of the lemma, $f(x) = g(x_1 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus c_1x_1 \oplus \cdots \oplus c_nx_n \oplus c$, where $x = (x_1, \ldots, x_n)$, g is a bent function on V_{n-1}, and $c_1, \ldots, c_n$ and c are all constant in $GF(2)$. Set $u_j = x_j \oplus x_n$, $j = 1, \ldots, n-1$. We have $f(u_1, \ldots, u_{n-1}, x_n) = g(u_1, \ldots, u_{n-1}) \oplus c_1u_1 \oplus \cdots \oplus c_{n-1}u_{n-1} \oplus (c_1 \oplus \cdots \oplus c_n)x_n \oplus c$. Since $g(u_1, \ldots, u_{n-1}) \oplus c_1x_1 \oplus \cdots \oplus c_{n-1}u_{n-1}$ is a bent function on V_{n-1}, it is unbalanced. On the other hand, since f is balanced, we conclude that $\bigoplus_{j=1}^{n} c_j \neq 0$, namely, $\bigoplus_{j=1}^{n} c_j = 1$. This proves the necessity for (ii). Using the same reasoning as in the proof of (i), and taking into account Lemma 6, we can prove the sufficiency for (ii). □

5.1 The Case of Balanced Functions

Theorem 2. *Let f be a balanced qth-order correlation immune function on V_n, satisfying the avalanche criterion of degree p. Then we have $p + q \leq n - 2$.*

Proof. First we note that $q > 0$ and $p > 0$. Since f is balanced, it cannot be bent. We prove the theorem in two steps. The first step deals with $p+q \leq n-2$, and the second step with $p + q \leq n - 1$.

We start with proving that $p + q \leq n - 1$ by contradiction. Assume that $p + q \geq n$. Set $i = 0$ and $j = 0$ in (4), we have $2^{n-p}\langle \chi_0, e_0\rangle = \langle \lambda_0, \ell_0\rangle$. Since f satisfies the avalanche criterion of degree p and $HW(\alpha_j) \leq p$, $j = 1, \ldots 2^p - 1$, we know that (6) holds. Note that $HW(\alpha_{u \cdot 2^p}) \leq n-p \leq q$ for all u, $0 \leq u \leq 2^{n-p}-1$. Since f is a balanced qth-order correlation immune function, we have

$$\langle \xi, L_0\rangle = \langle \xi, L_{2^p}\rangle = \langle \xi, L_{2 \cdot 2^p}\rangle = \cdots = \langle \xi, L_{(2^{n-p}-1)\cdot 2^p}\rangle = 0 \tag{14}$$

Applying $2^{n-p}\langle \chi_0, e_0\rangle = \langle \lambda_0, \ell_0\rangle$ to (5), and noticing (6) and (14), we would have $2^{n-p}\Delta(\alpha_0) = 0$, i.e., $2^{2n-p} = 0$. This cannot be true. Hence we have proved that $p + q \leq n - 1$.

Next we complete the proof by showing that $p + q \leq n - 2$. Assume for contradiction that the theorem is not true, i.e., $p + q \geq n - 1$. Since we have already proved that $p + q \leq n - 1$, by assumption we should have $p + q = n - 1$. Note that $HW(\alpha_{u \cdot 2^p}) \leq n - p - 1 = q$ for all u with $0 \leq u \leq 2^{n-p} - 2$, and f is a balanced qth-order correlation immune function, where $q = n - p - 1$. Hence (14) still holds, with the exception that the actual value of $\langle \xi, L_{(2^{n-p}-1)\cdot 2^p}\rangle$ is not clear yet. Applying $2^{n-p}\langle \chi_0, e_0\rangle = \langle \lambda_0, \ell_0\rangle$ to (5), and noticing (6) and (14), we have $2^{n-p}\Delta(\alpha_0) = \langle \xi, L_{(2^{n-p}-1)\cdot 2^p}\rangle^2$. Thus we have $\langle \xi, L_{(2^{n-p}-1)\cdot 2^p}\rangle^2 = 2^{2n-p}$. Due to Lemma 5, we have $p = n - 1$. Since $q \geq 1$, we obtain $p + q \geq n$. This contradicts the inequality $p + q \leq n - 1$, that we have already proved. Hence $p + q \leq n - 2$ holds. □

5.2 The Case of Unbalanced Functions

We turn our attention to unbalanced functions. A direct proof of the following Lemma can be found in [21].

Lemma 8. *Let $k \geq 2$ be a positive integer and $2^k = a^2 + b^2$, where both a and b are integers with $a \geq b \geq 0$. Then $a = 2^{\frac{1}{2}k}$ and $b = 0$ when k is even, and $a = b = 2^{\frac{1}{2}(k-1)}$ otherwise.*

Theorem 3. *Let f be an unbalanced qth-order correlation immune function on V_n, satisfying the avalanche criterion of degree p. Then*

(i) $p + q \leq n$,

(ii) *the equality in (i) holds if and only if n is odd, $p = n - 1$, $q = 1$ and $f(x) = g(x_1 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus c_1x_1 \oplus \cdots \oplus c_nx_n \oplus c$, where $x = (x_1, \ldots, x_n)$, g is a bent function on V_{n-1}, $c_1, \ldots, c_n$ and c are all constants in $GF(2)$, satisfying $\bigoplus_{j=1}^{n} c_j = 0$.*

Proof. Since f is correlation immune, it cannot be bent. Once again we now prove (i) by contradiction. Assume that $p + q > n$. Hence $n - p < q$. We keep all the notations in Section 5.1. Note that $HW(\alpha_{u \cdot 2^p}) \leq n - p < q$ for all u with $1 \leq u \leq 2^{n-p} - 1$. Since f is an unbalanced qth-order correlation immune function, we have (14) again, with the understanding that $\langle \xi, L_0 \rangle \neq 0$. Applying $2^{n-p}\langle \chi_0, e_0 \rangle = \langle \lambda_0, \ell_0 \rangle$ to (5), and noticing (6) and (14) with $\langle \xi, L_0 \rangle \neq 0$, we have $2^{n-p}\Delta(\alpha_0) = \langle \xi, L_0 \rangle^2$. Hence $\langle \xi, L_0 \rangle^2 = 2^{2n-p}$ and p must be even. Since f is not bent, noticing Lemma 5, we can conclude that $p = n - 1$ and n is odd. Using (ii) of Lemma 7, we have

$$f(x) = g(x_1 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus c_1x_1 \oplus \cdots \oplus c_nx_n \oplus c$$

where $x = (x_1, \ldots, x_n)$, g is a bent function on V_{n-1}, and $c_1, \ldots, c_n$ and c are all constants in $GF(2)$, satisfying $\bigoplus_{j=1}^{n} c_j = 0$. One can verify that while $x_j \oplus f(x)$ is balanced, $j = 1, \ldots, n$, $x_j \oplus x_i \oplus f(x)$ is not if $j \neq i$. Hence f is 1st-order, but not 2nd-order, correlation immune. Since $q > 0$, we have $q = 1$ and $p + q = n$. This contradicts the assumption that $p + q > n$. Hence we have proved that $p + q \leq n$.

We now prove (ii). Assume that $p + q = n$. Since $n - p = q$, we can apply $2^{n-p}\langle \chi_0, e_0 \rangle = \langle \lambda_0, \ell_0 \rangle$ to (5), and have (6) and (14) with $\langle \xi, L_0 \rangle \neq 0$. By using the same reasoning as in the proof of (i), we can arrive at the conclusion that (ii) holds. □

Theorem 4. *Let f be an unbalanced qth-order correlation immune function on V_n, satisfying the avalanche criterion of degree p. If $p + q = n - 1$, then f also satisfies the avalanche criterion of degree $p + 1$, n is odd and f must take the form mentioned in (ii) of Theorem 3.*

Proof. Let $p + q = n - 1$. Note that $HW(\alpha_{u \cdot 2^p}) \leq n - p - 1 = q$ for all u, $0 \leq u \leq 2^{n-p} - 2$. Since f is unbalanced and qth-order correlation immune, we have (14), although once again $\langle \xi, L_0 \rangle \neq 0$ and the value of $\langle \xi, L_{(2^{n-p}-1) \cdot 2^p} \rangle$ is not clear yet. Applying $2^{n-p}\langle \chi_0, e_0 \rangle = \langle \lambda_0, \ell_0 \rangle$ to (5), noticing (6) and (14), with the understanding that $\langle \xi, L_0 \rangle \neq 0$ and $\langle \xi, L_{(2^{n-p}-1) \cdot 2^p} \rangle$ is not decided yet, we have $2^{n-p}\Delta(\alpha_0) = \langle \xi, L_0 \rangle^2 + \langle \xi, L_{(2^{n-p}-1) \cdot 2^p} \rangle^2$. That is

$$\langle \xi, L_0 \rangle^2 + \langle \xi, L_{(2^{n-p}-1) \cdot 2^p} \rangle^2 = 2^{2n-p} \tag{15}$$

There exist two cases to be considered: p is even and p is odd.

Case 1: p is even and thus $p \geq 2$. Since $\langle \xi, L_0 \rangle \neq 0$, applying Lemma 8 to (15), we have $\langle \xi, L_0 \rangle^2 = 2^{2n-p}$ and $\langle \xi, L_{(2^{n-p}-1)\cdot 2^p} \rangle = 0$. Due to Lemma 5, $p = n-1$. Since $q > 0$, we have $p + q \geq n$. This contradicts the assumption $p + q = n - 1$. Hence p cannot be even.

Case 2: p is odd. Applying Lemma 8 to (15), we obtain

$$\langle \xi, L_0 \rangle^2 = \langle \xi, L_{(2^{n-p}-1)\cdot 2^p} \rangle^2 = 2^{2n-p-1} \tag{16}$$

Set $i = 2^t$, $t = 0, 1, \ldots, n-p-1$, where $n - p - 1 = q > 0$, and $j = 0$ in (4), we have

$$2^{n-p} \langle \chi_{2^t}, e_0 \rangle = \langle \lambda_0, \ell_{2^t} \rangle \tag{17}$$

where ℓ_{2^t} is the 2^tth row of H_{n-t} and e_0 is the all-one sequence of length 2^p.

Since f satisfies the avalanche criterion of degree p and $HW(\alpha_j) \leq p$, $j = 2^{t+p}, 1 + 2^{t+p}, \ldots, 2^p - 2 + 2^{t+p}$, (11) holds.

Applying (17) to (5), noticing (11) and (14) with $\langle \xi, L_0 \rangle^2 = \langle \xi, L_{(2^{n-p}-1)\cdot 2^p} \rangle^2 = 2^{2n-p+1}$, we have $2^{n-p} \Delta(\alpha_{2^{t+p}+2^p-1}) = 2^{2n-p}$ or 0. In other words, $\Delta(\alpha_{2^{t+p}+2^p-1}) = 2^n$ or 0.

Note that ℓ_{2^t} is the sequence of a linear function ψ on V_{n-p} where $\psi(y) = \langle \beta_{2^t}, y \rangle$, $y \in V_{n-p}$, $\beta_{2^t} \in V_{n-p}$ corresponds to the binary representation of 2^t. Due to (17), it is easy to verify that $\Delta(\alpha_{2^{t+p}+2^p-1}) = 2^n$ (or 0) if and only if $\langle \beta_{2^{n-p}-1}, \beta_{2^t} \rangle = 0$ (or 1) where $\beta_{2^{n-p}-1} \in V_{n-p}$ corresponds to the binary representation of $2^{n-p} - 1$. Note that $\beta_{2^{n-p}-1} = (0, \ldots, 0, 1, \ldots, 1)$ where the number of ones is equal to $n - p$. On the other hand β_{2^t} can be written as $\beta_{2^t} = (0, \ldots, 0, 1, 0, \ldots, 0)$. Since $t \leq n - p - 1$, we conclude that $\langle \beta_{2^{n-p}-1}, \beta_{2^t} \rangle = 1$, for all t with $0 \leq t \leq n - p - 1$. Hence $\Delta(\alpha_{2^{t+p}+2^p-1}) = 0$ for all such t.

Note that $HW(\alpha_{2^{t+p}+2^p-1}) = p + 1$. Permuting the variables, we can prove in a similar way that $\Delta(\alpha) = 0$ holds for each α with $HW(\alpha) = p + 1$. Hence f satisfies the avalanche criterion of degree $p + 1$. Due to $p + q = n - 1$, we have $(p + 1) + q = n$. Using Theorem 3, we conclude that n is odd and f takes the form mentioned in (ii) of Theorem 3. □

From Theorems 3 and 4, we conclude

Corollary 1. *Let f be an unbalanced qth-order correlation immune function on V_n, satisfying the avalanche criterion of degree p. Then*

(i) $p + q \leq n$, and the equality holds if and only if n is odd, $p = n - 1$, $q = 1$ and $f(x) = g(x_1 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus c_1 x_1 \oplus \cdots \oplus c_n x_n \oplus c$, where $x = (x_1, \ldots, x_n)$, g is a bent function on V_{n-1}, $c_1, \ldots, c_n$ and c are all constants in $GF(2)$, satisfying $\bigoplus_{j=1}^{n} c_j = 0$,

(ii) $p + q \leq n - 2$ if $q \neq 1$.

6 Conclusions

We have established a lower bound on nonlinearity over all Boolean functions satisfying the avalanche criterion of degree p. We have shown that the lower bound is tight. We have also characterized the functions that have the minimum nonlinearity. Furthermore, we have found a mutually exclusive relationship between the degree of avalanche and the order of correlation immunity.

There are still many interesting questions yet to be answered in this line of research. As an example, we believe that the upper bounds in Theorems 2 and 3 can be further improved, especially when p and q are neither too small, say close to 1, nor too large, say close to $n-1$.

Acknowledgment

The second author was supported by a Queen Elizabeth II Fellowship (227 23 1002).

References

1. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, Vol. 4, No. 1:3–72, 1991.
2. P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In *Advances in Cryptology - CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 87–100. Springer-Verlag, Berlin, Heidelberg, New York, 1991.
3. C. Carlet and P. Codes. On the propagation criterion of degree l and order k. In *Advances in Cryptology - EUROCRYPT'98*, volume 1403 of *Lecture Notes in Computer Science*, pages 462–474. Springer-Verlag, Berlin, Heidelberg, New York, 1998.
4. Claude Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, 3:135–145, 1993.
5. D. Coppersmith. The development of DES, 2000. (Invited talk at CRYPTO2000).
6. H. Feistel. Cryptography and computer privacy. *Scientific American*, 228(5):15–23, 1973.
7. Xiao Guo-Zhen and J. L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Transactions on Information Theory*, 34(3):569–571, 1988.
8. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, New York, Oxford, 1978.
9. M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, Berlin, Heidelberg, New York, 1994.
10. W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89*, volume 434 of *Lecture Notes in Computer Science*, pages 549–562. Springer-Verlag, Berlin, Heidelberg, New York, 1990.

11. K. Nyberg. On the construction of highly nonlinear permutations. In *Advances in Cryptology - EUROCRYPT'92*, volume 658 of *Lecture Notes in Computer Science*, pages 92–98. Springer-Verlag, Berlin, Heidelberg, New York, 1993.
12. B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, volume 437 of *Lecture Notes in Computer Science*, pages 155–165. Springer-Verlag, Berlin, Heidelberg, New York, 1991.
13. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.
14. J. Seberry, X. M. Zhang, and Y. Zheng. On constructions and nonlinearity of correlation immune functions. In *Advances in Cryptology - EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 181–199. Springer-Verlag, Berlin, Heidelberg, New York, 1994.
15. J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. *Information and Computation*, 119(1):1–13, 1995.
16. C. E. Shannon. Communications theory of secrecy system. *Bell Sys. Tech. Journal*, Vol. 28:656–751, 1949.
17. T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30 No. 5:776–779, 1984.
18. A. F. Webster and S. E. Tavares. On the design of S-boxes. In *Advances in Cryptology - CRYPTO'85*, volume 219 of *Lecture Notes in Computer Science*, pages 523–534. Springer-Verlag, Berlin, Heidelberg, New York, 1986.
19. R. Yarlagadda and J. E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceedings (Part E)*, 136:112–123, 1989.
20. X. M. Zhang and Y. Zheng. Auto-correlations and new bounds on the nonlinearity of boolean functions. In *Advances in Cryptology - EUROCRYPT'96*, volume 1070 of *Lecture Notes in Computer Science*, pages 294–306. Springer-Verlag, Berlin, Heidelberg, New York, 1996.
21. X. M. Zhang and Y. Zheng. Characterizing the structures of cryptographic functions satisfying the propagation criterion for almost all vectors. *Design, Codes and Cryptography*, 7(1/2):111–134, 1996. special issue dedicated to Gus Simmons.
22. X. M. Zhang and Y. Zheng. Cryptographically resilient functions. *IEEE Transactions on Information Theory*, 43(5):1740–1747, 1997.
23. X. M. Zhang and Y. Zheng. On plateaued functions. *IEEE Transactions on Information Theory*, 2000. (accepted).
24. Y. Zheng and X. M. Zhang. Plateaued functions. In *Advances in Cryptology - ICICS'99*, volume 1726 of *Lecture Notes in Computer Science*, pages 284–300. Springer-Verlag, Berlin, Heidelberg, New York, 1999.
25. Y. Zheng and X. M. Zhang. Improved upper bound on the nonlinearity of high order correlation immune functions. In *Selected Areas in Cryptography, 7th Annual International Workshop, SAC2000*, volume xxxx of *Lecture Notes in Computer Science*, pages xxx–xxx. Springer-Verlag, Berlin, Heidelberg, New York, 2000. (in Pre-Proceedings pages 258-269).
26. Y. Zheng and X. M. Zhang. Strong linear dependence and unbiased distribution of non-propagative vectors. In *Selected Areas in Cryptography, 6th Annual International Workshop, SAC'99*, volume 1758 of *Lecture Notes in Computer Science*, pages 92–105. Springer-Verlag, Berlin, Heidelberg, New York, 2000.