New Bounds on the Nonlinearity of Boolean Functions

Xian-Mo Zhang
Department of Computer Science
University of Wollongong
Wollongong, NSW 2522, Australia
xianmo@cs.uow.edu.au

Yuliang Zheng
The Peninsula School of Computing and Information Technology
Monash University, Frankston
Melbourne, VIC 3199, Australia
yzheng@fcit.monash.edu.au

Abstract

It is a well known fact that the nonlinearity of a function f on V_n is bounded from above by $2^{n-1} - 2^{\frac{1}{2}n-1}$. In computer security practice, cryptographic functions are usually constructively obtained in such a way that they support certain mathematical or cryptographic requirements. Hence an important question is how to calculate the nonlinearity of a function when extra information is available. In this paper we derive four (two upper and two lower) bounds on the nonlinearity of a function (see Table 1 on Page 9). Strengths and weaknesses of each bound are also examined. We anticipate that these four bounds will be very useful in calculating the nonlinearity of a cryptographic function when certain extra information on the function is available.

1 Introduction

The significance of nonlinear functions in cryptology is best illustrated by the success of linear cryptanalytic attacks recently discovered by Matsui in [6]. Realizing its importance, cryptographer often wish to find out the nonlinearity of a cryptographic function, or when the exact value is not easily obtainable, a lower and/or an upper bound on the nonlinearity.

A well-known fact about the upper bound on nonlinearity is $N_f \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}$, where N_f denotes the nonlinearity of f and f is a function from V_n (the n-dimensional vector space on $GF(2)$) to $GF(2)$. In contrast, less is known about the lower bound on nonlinearity, other than (to the authors knowledge) some progress made in [11, 14], as well as such trivial facts as $N_f > 0$ if and only if f is nonlinear.

In computer security practice, such as the design of a substitute-box employed by a private key encryption algorithm or a one-way hashing algorithm, or a nonlinear feedback function used in a pseudorandom sequence generator, one usually generates a nonlinear function in such a way that the function would satisfy certain mathematical or cryptographic criteria. A question one would face is how to calculate the nonlinearity of the function using extra information available on the function. If the exact value of the nonlinearity cannot be easily obtained, the next question is how to estimate the nonlinearity using the extra information on the function.

This paper addresses the two questions mentioned above. In particular, we derive four formulas for estimating the nonlinearity of a function, among which two are about upper bound while the other are about lower bounds. We hope that these bounds will be helpful in estimating the nonlinearity of a cryptographic function when extra information on the function is available.

The rest of the paper is organized as follows: Section 2 introduces the basic notions and notations used in this paper. Section 3 proves two upper bounds on nonlinearity, while Section 4 provides details on two lower bounds on nonlinearity.

For a reader who is more interested in the results than in technical details of the proofs, Table 1 on Page 9 summarizes the four bounds on nonlinearity.

2 Definitions

We consider Boolean functions from V_n to $GF(2)$ (or simply functions on V_n), 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 $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f}$ where $\alpha_0 = (0, \ldots, 0, 0)$, $\alpha_1 = (0, \ldots, 0, 1)$, ..., $\alpha_{2^{n-1}-1} = (1, \ldots, 1, 1)$. The *matrix* of f is a $(1,-1)$-matrix of order 2^n defined by $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$. f is said to be *balanced* if its truth table contains an equal number of ones and zeros.

An *affine* function f on V_n is a function that takes the form of $f(x_1, \ldots, x_n) = a_1x_1 \oplus \cdots \oplus a_nx_n \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$.

Definition 1 *The* Hamming weight *of a $(0,1)$-sequence s, denoted by $W(s)$, 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 $x = (x_1, \ldots, x_n)$. The* nonlinearity *of f, denoted by N_f, is the minimum Hamming distance between f and all affine functions on V_n, i.e., $N_f = \min_{i=1,2,\ldots,2^{n+1}} d(f, \varphi_i)$ where φ_1, φ_2, ..., $\varphi_{2^{n+1}}$ are all the affine functions on V_n.*

Note that the maximum nonlinearity of functions on V_n coincides with the covering radius of the first order binary Reed-Muller code $RM(1,n)$ of length 2^n, which is bounded from above by $2^{n-1} - 2^{\frac{1}{2}n-1}$ (see for instance [3]). Hence $N_f \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}$ for any function on V_n.

Next we introduce the definition of propagation criterion from [8].

Definition 2 *Let f be a function on V_n. We say that f satisfies*

1. *the* propagation 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.*
2. *the* propagation criterion of degree k *if it satisfies the propagation criterion with respect to all $\alpha \in V_n$ with $1 \leqq W(\alpha) \leqq k$.*

$f(x) \oplus f(x \oplus \alpha)$ is also called the *directional derivative* of f in the direction α. Further work on the topic can be found in [7].

Given two sequences $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_m)$, their component-wise product is defined by $a * b = (a_1b_1, \ldots, a_mb_m)$.

Definition 3 *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 the* auto-correlation *of f with a shift α,*

$$\Delta(\alpha) = \langle \xi(0), \xi(\alpha) \rangle.$$

Definition 4 *Let f be a function on V_n. The Walsh-Hadamard transform of f is defined as*

$$\hat{f}(\alpha) = 2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x) \oplus \langle \alpha, x \rangle}$$

where $\alpha = (a_1, \ldots, a_n) \in V_n$, $x = (x_1, \ldots, x_n)$, $\langle \alpha, x \rangle$ is the scalar product of α and x, namely, $\langle \alpha, x \rangle = \bigoplus_{i=1}^{n} a_i x_i$, and $f(x) \oplus \langle \alpha, x \rangle$ is regarded as a real-valued function.

A $(1, -1)$-matrix H of order m is called a *Hadamard* matrix if $HH^t = mI_m$, where H^t is the transpose of H and I_m is the identity matrix of order m. A Sylvester-Hadamard matrix of order 2^n, denoted by H_n, is generated by the following recursive relation

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

Let ℓ_i, $0 \leqq i \leqq 2^n - 1$, be the i row (column) of H_n. By Lemma 1 of [10], ℓ_i is the sequence of a linear function $\varphi_i(x)$ defined by the scalar product $\varphi_i(x) = \langle \alpha_i, x \rangle$, where α_i is the ith vector in V_n according to the ascending lexicographic order.

The Walsh-Hadamard transform, also called the discrete Fourier transform, has numerous applications in areas ranging from physical science to communications engineering. It appears in several slightly different forms [9, 5, 4]. The above definition follows the line in [9]. It can be equivalently written as

$$(\hat{f}(\alpha_0), \hat{f}(\alpha_1), \ldots, \hat{f}(\alpha_{2^n-1})) = 2^{-\frac{n}{2}} \xi H_n$$

where α_i is the ith vector in V_n according to the ascending order, ξ is the sequence of f and H_n is the Sylvester-Hadamard matrix of order 2^n.

Definition 5 *A function f on V_n is called a* bent *function if its Walsh-Hadamard transform satisfies*

$$\hat{f}(\alpha) = \pm 1$$

for all $\alpha \in V_n$.

Bent functions on V_n exist only when n is even [9]. They achieve the highest possible nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$.

The following lemma will be used in this paper (For a proof see for instance Lemma 6 of [10].)

Lemma 1 *The nonlinearity of a function f on V_n can be calculated by*

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

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

3 Two Upper Bounds on Nonlinearity

Let f be a function on V_n and ξ be the sequence of f. The following is a special form of the Wiener-Khintchine Theorem [1]:

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

By exploring (2) in different ways, we will obtain two upper bounds on the nonlinearity of functions.

3.1 The First Upper Bound

Our first upper bound can be regarded as a straightforward application of (2). For simplicity, write

$$\eta^* = (\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1}))$$

and

$$\xi^* = (\langle\xi, \ell_0\rangle^2, \ldots, \langle\xi, \ell_{2^n-1}\rangle^2).$$

Then (2) is simplified to $\eta^* H_n = \xi^*$. This causes $(\eta^* H_n)(\eta^* H_n)^T = \xi^* \xi^{*T}$, i.e.,

$$2^n \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = \sum_{j=0}^{2^n-1} \langle\xi, \ell_j\rangle^4.$$

Thus there exists a j_0, $0 \leqq j_0 \leqq 2^n - 1$, such that

$$\langle\xi, \ell_{j_0}\rangle^4 \geqq \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j).$$

Note that $\Delta(\alpha_0) = \Delta(0) = 2^n$. Hence from Lemma 1, we have

Theorem 1 *For any function f on V_n, the nonlinearity of f satisfies*

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt[4]{2^{2n} + \sum_{j=1}^{2^n-1} \Delta^2(\alpha_j)}.$$

It is easy to verify that the equality in Theorem 1 holds if and only if f is bent.

3.2 The Second Upper Bound

In order to derive the second upper bound on nonlinearity, we generalize (2) in the following direction. For any integer t, $0 \leqq t \leqq n$, rewrite (2) as

$$(\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1}))(H_{n-t} \times H_t) = (\langle\xi, \ell_0\rangle^2, \ldots, \langle\xi, \ell_{2^n-1}\rangle^2)$$

where $\times$ denotes the Kronecker product (see p.442, [12]).

Now set

$$\sigma_j = \sum_{k=0}^{2^t-1} \langle\xi, \ell_{j2^t+k}\rangle^2,$$

where $j = 0, 1, \ldots, 2^{n-t}-1$, Let $e = (1, \ldots, 1)$ be the all-one sequence of length 2^t and I denote the identity matrix of order 2^{n-t}. Then

$$(\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1}))(H_{n-t} \times H_t)(I \times e^T) = (\langle\xi, \ell_0\rangle^2, \ldots, \langle\xi, \ell_{2^n-1}\rangle^2)(I \times e^T).$$

Note that $(H_{n-t} \times H_t)(I \times e^T) = (H_{n-t} I) \times (H_t e^T)$ and $H_t e^T = (2^t, 0, \ldots, 0)^T$. Hence

$$(\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1}))(H_{n-t} \times (2^t, 0, \ldots, 0)^T) = (\sigma_0, \sigma_1, \ldots, \sigma_{2^{n-t}-1})$$

and

$$2^t(\Delta(\alpha_0), \Delta(\alpha_{2^t}), \Delta(\alpha_{2\cdot 2^t}), \ldots, \Delta(\alpha_{(2^{n-t}-1)2^t}))H_{n-t} = (\sigma_0, \sigma_1, \ldots, \sigma_{2^{n-t}-1}).$$

Thus we have proved the following result:

Lemma 2 *Let f be a function on V_n and ξ be the sequence of f. For any integer t, $0 \leqq t \leqq n$, set $\sigma_j = \sum_{k=0}^{2^t-1} \langle \xi, \ell_{j2^t+k} \rangle^2$, where $j = 0, 1, \ldots, 2^{n-t}-1$. Then*

$$2^t(\Delta(\alpha_0), \Delta(\alpha_{2^t}), \Delta(\alpha_{2\cdot 2^t}), \ldots, \Delta(\alpha_{(2^{n-t}-1)2^t}))H_{n-t} = (\sigma_0, \sigma_1, \ldots, \sigma_{2^{n-t}-1}). \tag{3}$$

The generality of (3) than (2) can be seen by noting the fact that the two equations become identical when $t = 0$.

Now compare the jth components in the two sides of (3), we have

$$2^t \sum_{k=0}^{2^{n-t}-1} a_k \Delta(\alpha_{k\cdot 2^t}) = \sigma_j, \tag{4}$$

where $j = 0, 1, \ldots, 2^{n-t}-1$ and $(a_0, a_1, \ldots, a_{2^{n-t}-1})$ denotes the jth row (column) of H_{n-t}. Since we also have $\sigma_j = \sum_{k=0}^{2^t-1} \langle \xi, \ell_{j2^t+k} \rangle^2$, for any fixed j there is a k_0, $0 \leqq k_0 \leqq 2^t - 1$, such that $|\langle \xi, \ell_{j2^t+k_0} \rangle| \geqq \sqrt{\sum_{k=0}^{2^{n-t}-1} a_k \Delta(\alpha_{k\cdot 2^t})}$. As $\Delta(\alpha_0) = 2^n$, by using Lemma 1, we have

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \sum_{k=1}^{2^{n-t}-1} a_k \Delta(\alpha_{k\cdot 2^t})}.$$

Now note that $\alpha_0, \alpha_{2^t}, \alpha_{2\cdot 2^t}, \ldots, \alpha_{(2^{n-t}-1)2^t}$ form a $(n-t)$-dimensional linear subspace of V_n with $\{\alpha_{2^t}, \alpha_{2^{t+1}}, \ldots, \alpha_{2^n}$ as its basis, and that the nonlinearity of a function is invariant under a nondegenerate linear transformation on the input coordinates. Set $r = n - t$. By using a nondegenerate linear transformation on the input coordinates, we have proved the following lemma:

Lemma 3 *For any integer r, $0 \leqq r \leqq n$, let $\beta_1, \ldots, \beta_r$ be r linearly independent vectors in V_n. Write $\gamma_j = c_1\beta_1 \oplus \cdots \oplus c_r\beta_r$, where $j = 0, 1, \ldots, 2^r - 1$ and $(c_1, \ldots, c_r)$ is the binary representation of integer j. Then*

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \sum_{j=1}^{2^r-1} a_j \Delta(\gamma_j)}$$

holds for every row (column), denoted by $(a_0, a_1, \ldots, a_{2^r-1})$, of H_r, where $a_0 = 1$ due to the structure of a Sylvester-Hadamard matrix.

In practice, simpler forms than that in Lemma 3 would be preferred. This can be achieved by letting $r = 1$ in Lemma 3. This results in

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n \pm \Delta(\beta)},$$

for any nonzero vector $\beta \in V_n$. Thus we have derived a simple formula for the upper bound on nonlinearity:

Theorem 2 *For any function f on V_n, the nonlinearity of f satisfies*

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \Delta_{max}},$$

where $\Delta_{max} = \max\{|\Delta(\alpha)| \,|\, \alpha \in V_n, \alpha \neq 0\}$.

It is easy to verify that the equality in Theorem 2 holds if and only if f is bent.

In situations where a more accurate estimate of nonlinearity is required, slightly more involved forms can be used. In particular, by substituting r with 2 in Lemma 3, we have

(i) $N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \Delta(\beta) + \Delta(\gamma) + \Delta(\beta \oplus \gamma)}$,

(ii) $N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \Delta(\beta) - \Delta(\gamma) - \Delta(\beta \oplus \gamma)}$,

(iii) $N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n - \Delta(\beta) + \Delta(\gamma) - \Delta(\beta \oplus \gamma)}$,

(iv) $N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n - \Delta(\beta) - \Delta(\gamma) + \Delta(\beta \oplus \gamma)}$.

where β and γ are nonzero vectors in V_n with $\beta \neq \gamma$. These four formulas are subsumed in the following corollary:

Corollary 1 *Let f be a function on V_n. Then*

1. *for any nonzero vectors $\beta, \gamma \in V_n$ with $\beta \neq \gamma$, the nonlinearity f satisfies*

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + |\Delta(\beta)| + |\Delta(\gamma)| - |\Delta(\beta \oplus \gamma)|};$$

2. *for $|\Delta(\alpha_{j_1})| \geqq |\Delta(\alpha_{j_2})| \geqq \cdots \geqq |\Delta(\alpha_{j_{2^n-1}})|$ where $(j_1, \ldots, j_{2^n-1})$ is a permutation of $(1, \ldots, 2^n - 1)$, the nonlinearity f satisfies*

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + |\Delta(\alpha_{j_1})| + |\Delta(\alpha_{j_2})| - |\Delta(\alpha_{j_3})|}.$$

4 Two Lower Bounds on Nonlinearity

In comparison with upper bounds, far less is known about lower bounds on nonlinearity, although some progress in this direction has been made in [11, 14]. This section proves two lower bounds on nonlinearity, of which the first lower bound has an extremely simple form while the second reveals an intimate relationship between the lower bound on nonlinearity and the propagation characteristic.

4.1 The First Lower Bound

Let $\xi = (a_0, a_1, \ldots, a_{2^n-1}) = (\overline{b_0}, \overline{b_1}, \ldots, \overline{b_{2^{n-1}-1}})$ be the sequence of a function on V_n where each $\overline{b}_j = (a_{2j}, a_{2j+1})$ is called a *basis*. A basis, say $\overline{b}_j$, is called a $(++)$-*basis* if $\overline{b}_j = \pm(1,1)$ and is called a $(+-)$-*basis* if $\overline{b}_j = \pm(1,-1)$. A fact is that any $(1,-1)$-sequence of length 2^n ($n \geqq 2$) is a concatenation of $(++)$-bases and $(+-)$-bases.

In the following discussion, the number of $(++)$-bases in a sequence under consideration will be denoted by $\tau(++)$ and the number of $(+-)$-bases by $\tau(+-)$.

Lemma 4 *Let ξ be the sequence of a function f on V_n. Then $\tau(++) = 2^{n-2} + \frac{1}{4}\Delta(\alpha_1)$ and $\tau(+-) = 2^{n-2} - \frac{1}{4}\Delta(\alpha_1)$, where $\alpha_1 = (0, \ldots, 0, 1)$, the binary representation of integer 1.*

Proof. Write $\xi = a_0, a_1, a_2, a_3, \ldots, a_{2^n-2}, a_{2^n-1}$. Thus $\xi(\alpha_1) = a_1, a_0, a_3, a_2, \ldots, a_{2^n-1}, a_{2^n-2}$ and thus

$$\Delta(\alpha_1) = \langle \xi, \xi(\alpha_1) \rangle = \sum_{j=0}^{2^{n-1}-1} (a_{2j}a_{2j+1} + a_{2j+1}a_{2j}).$$

Note that

$$a_{2j}a_{2j+1} + a_{2j+1}a_{2j} = \begin{cases} 2 & \text{if } (a_{2j}a_{2j+1}) \text{ is a } (++)\text{-basis} \\ -2 & \text{if } (a_{2j}a_{2j+1}) \text{ is a } (+-)\text{-basis} \end{cases}$$

Thus $\Delta(\alpha_1) = 2(\tau(++) - \tau(+-))$. On the other hand, $2(\tau(++) + \tau(+-)) = 2^n$. Hence $\tau(++) = 2^{n-2} + \frac{1}{4}\Delta(\alpha_1)$ and $\tau(+-) = 2^{n-2} - \frac{1}{4}\Delta(\alpha_1)$. □

Lemma 5 *For any function f on V_n, the nonlinearity of f satisfies*

$$N_f \geqq 2^{n-2} - \frac{1}{4}|\Delta(\alpha_1)|.$$

Proof. Obviously, $W(f) \geqq \tau(+-)$. By using Lemma 4, $W(f) \geqq 2^{n-2} - \frac{1}{4}\Delta(\alpha_1)$, where $W(f)$ is the Hamming weight of f i.e. the number of ones f assumes.

Set $g_j(x) = f(x) \oplus \varphi_j(x)$, where φ_j is the linear function on V_n, whose sequence is ℓ_i, $j = 0, 1, \ldots, 2^n - 1$.

Similarly to $\Delta(\alpha)$ for f, we can write $\Delta^{(j)}$ to denote the auto-correlation of g_j. It is easy to verify that

$$\Delta^{(j)}(\alpha_1) = \begin{cases} \Delta(\alpha_1) & \text{if } \varphi_j(\alpha_1) = 0 \\ -\Delta(\alpha_1) & \text{if } \varphi_j(\alpha_1) = 1 \end{cases}$$

By the same reasoning for $W(f)$, we have

$$W(f \oplus \varphi_j) \geqq \begin{cases} 2^{n-2} - \frac{1}{4}\Delta(\alpha_1) & \text{if } \varphi_j(\alpha_1) = 0 \\ 2^{n-2} + \frac{1}{4}\Delta(\alpha_1) & \text{if } \varphi_j(\alpha_1) = 1 \end{cases}$$

Finally, note that $d(f, \varphi_j) = W(f \oplus \varphi_j)$. Hence we have $N_f \geqq 2^{n-2} - \frac{1}{4}|\Delta(\alpha_1)|$. □

Theorem 3 *For any function f on V_n, the nonlinearity of f satisfies*

$$N_f \geqq 2^{n-2} - \frac{1}{4}\Delta_{min},$$

where $\Delta_{min} = \min\{|\Delta(\alpha)| | \alpha \in V_n, \alpha \neq 0\}$.

Proof. For any fixed s, $0 \leqq s \leqq 2^n - 1$, let A be a nondegenerate matrix of order n, over $GF(2)$, such that $\alpha_1 A = \alpha_s$. Define $g(x) = f(xA)$. Set $xA = u$. Hence $g(x) = f(u)$ where $xA = u$. Note that

$$g(x) \oplus g(x \oplus \alpha_1) = f(xA) \oplus f(xA \oplus \alpha_1 A) = f(u) \oplus f(u \oplus \alpha_s). \tag{5}$$

Similarly to $\Delta(\alpha)$ defined for f, we can write $\Delta'(\alpha)$ as the auto-correlation of g.

From (5), $\Delta'(\alpha_1) = \Delta(\alpha_s)$. By using Lemma 5, $N_g \geqq 2^{n-2} - \frac{1}{4}|\Delta'(\alpha_1)|$. Since A is nondegenerate, $N_g = N_f$. Hence $N_f \geqq 2^{n-2} - \frac{1}{4}|\Delta(\alpha_s)|$. As s is arbitrary, $N_f \geqq 2^{n-2} - \frac{1}{4}\Delta_{min}$. □

4.2 The Second Lower Bound

In [2] it was pointed out that if f, a function on V_n, satisfies the propagation criterion with respect to all but a subset $\Re$ of vectors in V_n, then the nonlinearity of f satisfies

$$N_f \geqq 2^{n-1} - 2^{\frac{n}{2}-1}|\Re|^{\frac{1}{2}}. \tag{6}$$

More recently, a further improvement has been made in [11]:

$$N_f \geqq 2^{n-1} - 2^{n-\frac{1}{2}\rho-1} \tag{7}$$

where ρ is the maximum dimension of the linear sub-spaces in $\{0\} \cup \Re^c$ and $\Re^c = V_n - \Re$. (see Theorem 11, [11]).

A shortcoming with (6) and (7) is that when $|\Re|$ is large, estimates provided by (6) and (7) are too far from the real value. For example, let g be a bent function on V_n (n must be even). Suppose $n \geqq 4$. Now we construct a function f on V_n: $f(x) = g(x)$ if $x \neq 0$ and $f(0) = 1 \oplus g(0)$. Since $W(g)$ is even, $W(f)$ must be odd. Hence f does not satisfy the propagation characteristics with respect to any vectors and hence $|\Re| = 2^n$. In this case both (6) and (7) give the trivial inequality $N_f \geqq 0$. This problem is addressed in the rest of this section.

Let f, a function on V_n, satisfy the propagation criterion with respect to all but a subset $\Re$ of vectors in V_n. For any integer t, $0 \leqq t \leqq n$, set

$$\Omega = \{\alpha_0, \alpha_{2^t}, \alpha_{2\cdot 2^t}, \ldots, \alpha_{(2^{n-t}-1)2^t}\}.$$

Recall $\alpha_0, \alpha_{2^t}, \alpha_{2\cdot 2^t}, \ldots, \alpha_{(2^{n-t}-1)2^t}$ form a $(n-t)$-dimensional linear subspace of V_n, and $\{\alpha_{2^t}, \alpha_{2^{t+1}}, \ldots, \alpha_{2^{n-1}}\}$ is a basis of this subspace.

From (4),

$$\sigma_j \leqq 2^t(\Delta(\alpha_0) + (|\Re \cap \Omega| - 1)\Delta_{max}),$$

where $\Delta_{max} = \max\{|\Delta(\alpha)| | \alpha \in V_n, \alpha \neq 0\}$ and $\sigma_j = \sum_{k=0}^{2^t-1} \langle \xi, \ell_{j2^t+k}\rangle^2$, $j = 0, 1, \ldots, 2^{n-t} - 1$. Hence

$$\langle \xi, \ell_{j2^t+k}\rangle^2 \leqq 2^t(\Delta(\alpha_0) + (|\Re \cap \Omega| - 1)\Delta_{max}),$$

$j = 0, 1, \ldots, 2^{n-t} - 1$, $k = 0, 1, \ldots, 2^t - 1$.

Note that $\Delta(\alpha_0) = 2^n$. By using Lemma 1, the nonlinearity of f satisfies

$$N_f \geqq 2^{n-1} - 2^{\frac{1}{2}t-1}\sqrt{2^n + (|\Re \cap \Omega| - 1)\Delta_{max}}.$$

Set $r = n - t$. By using a nondegenerate linear transformation on the variables, we have

Theorem 4 *Let f, a function on V_n, satisfy the propagation criterion with respect to all but a subset $\Re$ of vectors in V_n. Let W be any r-dimensional linear subspace of V_n, $r = 0, 1, \ldots, n$. Then the nonlinearity of f satisfies*

$$N_f \geqq 2^{n-1} - 2^{\frac{1}{2}(n-r)-1}\sqrt{2^n + (|\Re \cap W| - 1)\Delta_{max}},$$

where $\Delta_{max} = \max\{|\Delta(\alpha)| | \alpha \in V_n, \alpha \neq 0\}$.

Since $|\Delta(\alpha)| \leqq 2^n$ for each $\alpha \in V_n$, from Theorem 4, we have

Corollary 2 *Let f, a function on V_n, satisfy the propagation criterion with respect to all but a subset $\Re$ of vectors in V_n. Let W be any r-dimensional linear subspace of V_n, $r = 0, 1, \ldots, n$. Then the nonlinearity of f satisfies*

$$N_f \geqq 2^{n-1} - 2^{n-\frac{1}{2}r-1}\sqrt{|\Re \cap W|}.$$

Theorem 4 is more general and gives a better estimate of lower bound than all other known lower bounds. To see this, let $W = V_n$ i.e. $r = n$. Hence we have $N_f \geqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + (|\Re| - 1)\Delta_{max}}$. As $\Delta_{max} \leqq 2^n$, this estimate is clearly better than (6). On the other hand, if $\Re \cap W = \{\alpha_0 = 0\}$ then $N_f \geqq 2^{n-1} - 2^{n-\frac{1}{2}r-1}$, which is exactly (7).

Corollary 2 shows a subtle relationship between the nonlinearity and the propagation characteristic: the nonlinearity is not only influenced by the size of $\Re$ but also by the distribution of $\Re$. This is expressed in a different way in the following corollary:

Table 1: Upper and Lower Bounds on Nonlinearity

Upper Bounds	Theorem 1: $N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt[4]{2^{2n} + \sum_{j=1}^{2^n-1} \Delta^2(\alpha_j)}$
	Theorem 2: $N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \Delta_{max}}$
Lower Bounds	Theorem 3: $N_f \geqq 2^{n-2} - \frac{1}{4}\lvert\Delta_{min}\rvert$
	Theorem 4: $N_f \geqq 2^{n-1} - 2^{\frac{1}{2}(n-r)-1}\sqrt{2^n + (\lvert\Re \cap W\rvert - 1)\Delta_{max}}$

where
$\Delta(\alpha) = \langle \xi(0), \xi(\alpha) \rangle$ is the auto-correlation of f with a shift α,
$\Delta_{max} = \max\{|\Delta(\alpha)| | \alpha \in V_n, \alpha \neq 0\}$,
$\Delta_{min} = \min\{|\Delta(\alpha)| | \alpha \in V_n, \alpha \neq 0\}$,
$\Re$ is the set of vectors where the propagation criterion is not fulfilled by f, and
W is any r-dimensional linear subspace of V_n, $r = 0, 1, \ldots, n$.

Corollary 3 *Let f, a function on V_n, satisfy the propagation criterion with respect to all but a subset $\Re$ of vectors in V_n. If the nonlinearity of f satisfies*

$$N_f \leqq 2^{n-1} - 2^{n-\frac{1}{2}r-1}p,$$

where r is an integer, $0 \leqq r \leqq n$, and $p > 0$, then there is a r-dimensional linear subspace of V_n, say W, such that $|\Re \cap W| \geqq p^2$.

Table 1 summarizes the main results obtained in this paper, namely two upper and two lower bounds on the nonlinearity of cryptographic functions.

5 Examples and Applications

Obviously, the upper bounds stated in Theorems 1 and 2, as well as those in Corollary 1, all represent an improvement on the well-known upper bound $N_f \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}$. We found that the two upper bounds described in Theorems 1 and 2, however, have different strengths and weaknesses. This is illustrated by examining the following two different cases.

In the first case, we consider a function f on V_n satisfying the propagation criterion with respect to all but a small subset $\Re$ of vectors in V_n. In particular, when $|\Re| = 2$, by Corollary 2 of [14], there exists a nondegenerate matrix A of order n over $GF(2)$ such that

$$f(xA) = c_1 x_1 \oplus g(y)$$

where $g(y)$ is a bent function on V_{n-1} and $x = (x_1, y) \in V_n$. In the same paper it was also proved that the two vectors in $\Re$, say $\beta_0 = 0$ and $\beta_1 \neq 0$, satisfy $\Delta(\beta_j) = \pm 2^n$, $j = 0, 1$.

Using Theorem 1,

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt[4]{2^{2n} + 2^{2n}} = 2^{n-1} - \frac{1}{2}\sqrt[4]{2} \cdot 2^{\frac{1}{2}n}, \tag{8}$$

while using Theorem 2,

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + 2^n} = 2^{n-1} - \frac{1}{2}\sqrt{2} \cdot 2^{\frac{1}{2}n}. \tag{9}$$

Obviously, for this particular example, the right hand side of (9) is less than that of (8). In other wards, Theorem 2 provides a better estimate than Theorem 1 does.

In the second case, we consider a function g on V_n that is defined as $g(x) = 0$ if $x \neq 0$ and $g(0) = 1$. It is easy to check that for such a function g, $\Delta(\alpha) = \pm(2^n - 4)$ if $\alpha \neq 0$, namely $\Re = V_n$.

Applying Theorem 1,

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt[4]{2^{2n} + (2^n - 1)(2^n - 4)^2}, \tag{10}$$

while applying Theorem 2,

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + (2^n - 4)} = 2^{n-1} - \frac{1}{2}\sqrt{2^{n+1} - 4}. \tag{11}$$

One can check that the right hand side of (10) is less than that of (11). Hence for such a function g Theorem 1 provides more accurate information than Theorem 2 does.

Theorem 1 generally provides a more accurate estimate on the upper bound of nonlinearity than Theorem 2 when $\Re$ is large, but less so when $\Re$ is small.

Let f, a function on V_n, satisfy the propagation criterion with respect to all but a subset $\Re$ of vectors in V_n. From Theorem 1,

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt[4]{2^{2n} + |\Re|\Delta^2_{min}},$$

where $\Delta_{min} = \min\{|\Delta(\alpha)||\alpha \in V_n, \alpha \neq 0\}$.

It is easy to verify that $|\Delta(\alpha)|$ is divisable by four. Thus $\Delta(\alpha) \neq 0$ implies $|\Delta(\alpha)| \geqq 4$. From Theorem 1,

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt[4]{2^{2n} + 16|\Re|}.$$

From Theorem 3 of [13], if f is a non-bent cubic function then $\Delta_{max} \geqq 2^{\frac{1}{2}(n+1)}$, where $\Delta_{max} = \max\{|\Delta(\alpha)||\alpha \in V_n, \alpha \neq 0\}$.

By using Theorem 2

$$N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + 2^{\frac{1}{2}(n+1)}}.$$

Using Theorem 3, we obtain Theorem 12 of [11]: if a function f on V_n satisfies the propagation criterion with respect to a vector then the nonlinearity of f satisfies $N_f \geqq 2^{n-2}$, in other words, if the nonlinearity of f is less than 2^{n-2} then f does not satisfy the propagation criterion with respect to any vector.

Any function on V_n, f, can be written as $f(x) = p(y)x_t \oplus q(y)$, for a fixed t, $1 \leqq t \leqq n$, where $x = (x_1, \dots, x_n)$, $y = (x_1, \dots, t-1, t+1, x_n)$, p and q are functions on V_{n-1}. We can conclude that the nonlinearity of f, N_f, satisfies $N_f \geqq 2^{n-2}$ if p is balanced. In fact, it is obvious that f satisfies the propagation with respect to $\alpha_{2^{n-t}} = (0, \dots, 0, 1, 0, \dots, 0)$, where only the tth component is nonzero. From Theorem 3, $N_f \geqq 2^{n-2}$.

6 Conclusion

Two upper and two lower bounds on the nonlinearity of a Boolean function have been established. These bounds could be particularly useful when certain structural information on a Boolean function is available. All the bounds have been primarily based on the auto-correlation of a function under consideration. This opens up a possible new avenue for future research, that is to extend the results so that they take into account other factors such as linear structures, algebraic degree and global avalanche characteristics (GAC) introduced in [13].

References

[1] K. G. Beauchamp. *Applications of Walsh and Related Functions with an Introduction to Sequency Functions*. Microelectronics and Signal Processing. Academic Press, London, New York, Tokyo, 1984.

[2] Claude Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, 3:135–145, 1993.

[3] G. D. Cohen, M. G. Karpovsky, Jr. H. F. Mattson, and J. R. Schatz. Covering radius — survey and recent results. *IEEE Transactions on Information Theory*, IT-31(3):328–343, 1985.

[4] J. F. Dillon. A survey of bent functions. *The NSA Technical Journal*, pages 191–215, 1972. (unclassified).

[5] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, New York, Oxford, 1978.

[6] M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT'93*, volume 765, Lecture Notes in Computer Science, pages 386–397. Springer-Verlag, Berlin, Heidelberg, New York, 1994.

[7] B. Preneel, R. Govaerts, and J. Vandewalle. Boolean functions satisfying higher order propagation criteria. In *Advances in Cryptology - EUROCRYPT'91*, volume 547, Lecture Notes in Computer Science, pages 141–152. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[8] 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, Lecture Notes in Computer Science, pages 155–165. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

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

[10] J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. *Information and Computation*, 119(1):1–13, 1995.

[11] J. Seberry, X. M. Zhang, and Y. Zheng. The relationship between propagation characteristics and nonlinearity of cryptographic functions. *Journal of Universal Computer Science*, 1(2):136–150, 1995. (available at `http://hgiicm.tu-graz.ac.at/`).

[12] Jennifer Seberry and Mieko Yamada. Hadamard matrices, sequences and block designs. In J. Dinitz and D. Stinson, editors, *Surveys in Contemporary Design Theory*, Wiley-Interscience Series in Discrete Mathematics. John Wiley, New York, 1992.

[13] X. M. Zhang and Y. Zheng. GAC — the criterion for global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science*, 1(5):316–333, 1995. (available at `http://hgiicm.tu-graz.ac.at/`).

[14] 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.