Auto-Correlations and New Bounds on the Nonlinearity of Boolean Functions

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

[1] The University of Wollongong, Wollongong, NSW 2522, Australia
xianmo@cs.uow.edu.au
[2] 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 the n-dimensional vector space V_n is bounded from above by $2^{n-1} - 2^{\frac{1}{2}n-1}$. In cryptographic practice, nonlinear 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 address this question in the context of auto-correlations, and derive four (two upper and two lower) bounds on the nonlinearity of a function (see Table 1). Strengths and weaknesses of each bound are also examined. In addition, a few examples are given to demonstrate the usefulness of the bounds in practical applications. We anticipate that these four bounds will be very useful in calculating the nonlinearity of a cryptographic function when certain extra information on the auto-correlations of 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, cryptographers 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 $N_f \leq 2^{n-1} - 2^{\frac{1}{2}n-1}$, 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, 13], as well as such trivial facts as $N_f > 0$ if and only if f is nonlinear.

In cryptographic practice, such as the design of a substitution-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 requirements. 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 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. Table 1 summarizes the four bounds on nonlinearity. We hope that these bounds will be particularly helpful in estimating the nonlinearity of a cryptographic function when extra information on the auto-correlations of 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. A few example applications are provided in Section 5, which show the usefulness of the bounds in practice.

2 Definitions

We consider Boolean 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 $\alpha_0 = (0,\ldots,0,0)$, $\alpha_1 = (0,\ldots,0,1)$, $\ldots$, $\alpha_{2^{n-1}-1} = (1,\ldots,1,1)$. 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., $N_f = \min_{i=0,1,\ldots,2^{n+1}-1} d(f,\varphi_i)$ where φ_0, φ_1, $\ldots$, $\varphi_{2^{n+1}-1}$ 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 $N_f \leq 2^{n-1} - 2^{\frac{1}{2}n-1}$ 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 $1 \leq W(\alpha) \leq k$.

$f(x) \oplus f(x \oplus \alpha)$ 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 componentwise product is defined by $a * b = (a_1 b_1, \ldots, a_m b_m)$. The scalar product $\langle a, b \rangle$ of a and b is defined as the sum of the components in $a * b$. Note that depending on where the components of a and b are drawn from, the meaning of a "sum" operation may vary.

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 $f(x) \oplus f(x \oplus \alpha)$. The *auto-correlation* of f with a shift α is defined as

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

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, $0 \leq i \leq 2^n - 1$, 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.

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.

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 6. *The nonlinearity of a function f on V_n can be calculated by*

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

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

As the number of linear functions on V_n is exponential in n, it is impractical to calculate N_f for a large n by examining all linear functions against the formula in Lemma 6.

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, $0 \le j_0 \le 2^n - 1$, such that

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

Note that $\Delta(\alpha_0) = \Delta(0) = 2^n$. Hence from Lemma 6, we have

Theorem 7. *For any function f on V_n, the nonlinearity of f satisfies*

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

It is easy to verify that the bound in Theorem 7 does not exceed the well-known bound $2^{n-1} - 2^{\frac{1}{2}n-1}$. In addition, as the equality holds if f is bent, the bound is tight.

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, $0 \leq t \leq n$, 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.421, [5]).

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 8. *Let f be a function on V_n and ξ be the sequence of f. For any integer t, $0 \leq t \leq n$, 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*

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

We can see that (3) is more general than (2), 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

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

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, $0 \le k_0 \le 2^t - 1$, such that $|\langle \xi, \ell_{j2^t+k_0} \rangle| \ge \sqrt{\sum_{k=0}^{2^{n-t}-1} a_k \Delta(\alpha_{k \cdot 2^t})}$. As $\Delta(\alpha_0) = 2^n$, by using Lemma 6, we have

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

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 $\{\alpha_{2^t}, \alpha_{2^{t+1}}, \ldots, \alpha_{2^{n-1}}\}$ 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 9. *For any integer r, $0 \le r \le n$, 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*

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

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 9 would be preferred. This can be achieved by letting $r = 1$ in Lemma 9. This results in

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

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

Theorem 10. *For any function f on V_n, the nonlinearity of f satisfies*

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

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

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 9, we have

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

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

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

Corollary 11. *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*
$$N_f \le 2^{n-1} - \frac{1}{2}\sqrt{2^n + |\Delta(\beta)| + |\Delta(\gamma)| - |\Delta(\beta \oplus \gamma)|};$$
2. *for $|\Delta(\alpha_{j_1})| \ge |\Delta(\alpha_{j_2})| \ge \cdots \ge |\Delta(\alpha_{j_{2^n-1}})|$ where $(j_1, \ldots, j_{2^n-1})$ is a permutation of $(1, \ldots, 2^n - 1)$, the nonlinearity f satisfies*
$$N_f \le 2^{n-1} - \frac{1}{2}\sqrt{2^n + |\Delta(\alpha_{j_1})| + |\Delta(\alpha_{j_2})| - |\Delta(\alpha_{j_3})|}.$$

None of the bounds in Lemma 9, Theorem 10 and Corollary 11 goes beyond the well-known bound $2^{n-1} - 2^{\frac{1}{2}n-1}$. The equalities in these bounds hold if f is bent, which indicates that all the bounds are tight.

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, 13]. 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 ($n \ge 2$) 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 12. *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

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

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 13. *For any function f on V_n, the nonlinearity of f satisfies*

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

Proof. Obviously, $W(f) \geq \tau(+-)$. By using Lemma 12, $W(f) \geq 2^{n-2} - \frac{1}{4}\Delta(\alpha_1)$, 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

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

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

Now we introduce the first lower bound on nonlinearity:

Theorem 14. *For any function f on V_n, the nonlinearity of f satisfies*

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

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

Proof. For any fixed s, $0 \leq s \leq 2^n - 1$, 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 13, $N_g \geq 2^{n-2} - \frac{1}{4}|\Delta'(\alpha_1)|$. Since A is nondegenerate, $N_g = N_f$. Hence $N_f \geq 2^{n-2} - \frac{1}{4}|\Delta(\alpha_s)|$. As s is arbitrary, $N_f \geq 2^{n-2} - \frac{1}{4}\Delta_{min}$. □

Theorem 14 is tight. This can be seen from the following fact. Let $f(x) = x_1\varphi(y) \oplus \psi(y)$ be a function on V_n, where $x = (x_1, \ldots, x_n)$, $y = (x_3, \ldots, x_n)$, φ and ψ are linear functions on V_{n-2} and $\varphi \neq \psi$. Note that f is quadratic. Using the truth table of f, we can verify that the nonlinearity of f is $N_f = 2^{n-2}$. Obviously, $\Delta(\alpha_{2^{n-1}}) = 0$, where $\alpha_{2^{n-1}} = (1, 0, \ldots, 0)$ is the binary representation of integer 2^{n-1}. This means that the equality in Theorem 14 holds for such a function $f(y) = x_1\varphi(y) \oplus \psi(y)$.

4.2 The Second Lower Bound

By using a result in [2], the authors pointed out in [13] 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

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

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

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

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) or (7) are too far from the real value. For example, let g be a bent function on V_n (n must be even). Suppose $n \geq 4$. 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 $N_f \geq 0$. 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, $0 \leq t \leq n$, 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),

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

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

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

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

Note that $\Delta(\alpha_0) = 2^n$. By using Lemma 6, the nonlinearity of f satisfies

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

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

Theorem 15. *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*

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

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

Since $|\Delta(\alpha)| \leq 2^n$ for each $\alpha \in V_n$, from Theorem 15, we have

Corollary 16. *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*

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

Theorem 15 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 $N_f \geq 2^{n-1} - \frac{1}{2}\sqrt{2^n + (|\Re| - 1)\Delta_{max}}$. As $\Delta_{max} \leq 2^n$, this estimate is clearly better than (6). On the other hand, if $\Re \cap W = \{\alpha_0 = 0\}$ then $N_f \geq 2^{n-1} - 2^{n-\frac{1}{2}r-1}$, which is exactly (7).

Corollary 16 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:

Corollary 17. *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*

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

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

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

5.1 For the Two Upper Bounds

The upper bounds stated in Theorems 7 and 10, as well as those in Corollary 11, all represent an improvement on the well-known upper bound $N_f \leq 2^{n-1} - 2^{\frac{1}{2}n-1}$. We found that the two upper bounds described in Theorems 7 and 10, 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,

Table 1. Upper and Lower Bounds on Nonlinearity

Upper Bounds	Theorem 7: $N_f \leq 2^{n-1} - \frac{1}{2}\sqrt[4]{2^{2n} + \sum_{j=1}^{2^n-1} \Delta^2(\alpha_j)}$
	Theorem 10: $N_f \leq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \Delta_{max}}$
Lower Bounds	Theorem 14: $N_f \geq 2^{n-2} - \frac{1}{4}\lvert\Delta_{min}\rvert$
	Theorem 15: $N_f \geq 2^{n-1} - 2^{\frac{1}{2}(n-r)-1}\sqrt{2^n + (\lvert\Re \cap W\rvert - 1)\Delta_{max}}$

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, $r = 0, 1, \ldots, n$.

when $|\Re| = 2$, by Corollary 2 of [13], 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 7,

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

while using Theorem 10,

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

For this particular example, the right hand side of (9) is clearly less than that of (8). Consequently, Theorem 10 provides a better estimate than Theorem 7 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 7,

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

while applying Theorem 10,

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

One can check that the right hand side of (10) is less than that of (11). Hence for such a function g Theorem 7 provides more accurate information than Theorem 10 does.

Theorem 7 generally provides a more accurate estimate on the upper bound of nonlinearity than Theorem 10 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 7,

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

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

It is easy to verify that $|\Delta(\alpha)|$ is divisible by four. Thus $\Delta(\alpha) \neq 0$ implies $|\Delta(\alpha)| \geq 4$. From Theorem 7,

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

Now we consider another example. From Theorem 3 of [12], if f is a non-bent cubic function then $\Delta_{max} \geq 2^{\frac{1}{2}(n+1)}$, where $\Delta_{max} = \max\{|\Delta(\alpha)||\alpha \in V_n, \alpha \neq 0\}$. Applying Theorem 10 in this paper, we have

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

On the other hand, from Theorem 14 in this paper, 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 $N_f \geq 2^{n-2}$. 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.

5.2 For the Two Lower Bounds

First, we consider an arbitrary function f on V_n, f. f can always be written as $f(x) = p(y)x_t \oplus q(y)$, for a fixed t, $1 \leq t \leq n$, where $x = (x_1, \ldots, x_n)$, $y = (x_1, \ldots, x_{t-1}, x_{t+1}, \ldots, x_n)$, p and q are functions on V_{n-1}. We can conclude that the nonlinearity of f, N_f, satisfies $N_f \geq 2^{n-2}$ if p is balanced. This follows from the fact that f satisfies the propagation criterion with respect to $\alpha_{2^{n-t}} = (0, \ldots, 0, 1, 0, \ldots, 0)$, whose tth component is the only nonzero bit. Hence according to Theorem 14, we have $N_f \geq 2^{n-2}$.

Now we consider another example that is related to Theorem 15. Let f be a function on V_n, whose nonlinearity N_f satisfies $N_f = 2^{n-2}$. The function $f(x) = x_1\varphi(y) \oplus \psi(y)$ presented at the end of Subsection 4.1 is an example of such a function. For any function f with $N_f = 2^{n-2}$, the equality in Corollary 17 which is derived from Theorem 15, holds when $p = 2^{\frac{1}{2}r-1}$, where r is an arbitrary integer, $2 \leq r \leq n$. Using the same corollary, one can see that there is a r-dimensional linear subspace of V_n, say W, such that $|\Re \cap W| \geq 2^{r-2}$. In particular, when $r = n$, i.e. $W = V_n$, we have $|\Re| \geq 2^{n-2}$.

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 [12].

Acknowledgments: We would like to thank the anonymous referees for Eurocrypt'96 whose comments helped in improving the presentation of this paper.

References

1. Beauchamp, K. G.: Applications of Walsh and Related Functions with an Introduction to Sequency Functions. Academic Press London, New York, Tokyo 1984.
2. Carlet, C.: Partially-bent functions. Designs, Codes and Cryptography **3** (1993) 135–145.
3. Cohen, G. D., Karpovsky, M. G., H. F. Mattson, J., Schatz, J. R.: Covering radius — survey and recent results. IEEE Transactions on Information Theory **IT-31** (1985) 328–343.
4. Dillon, J. F.: A survey of bent functions. The NSA Technical Journal (1972) 191–215. (unclassified)
5. MacWilliams, F. J., Sloane, N. J. A.: The Theory of Error-Correcting Codes. North-Holland Amsterdam, New York, Oxford 1978.
6. Matsui, M.: Linear cryptanalysis method for DES cipher. In Advances in Cryptology - EUROCRYPT'93 (1994) vol. 765, LNCS Springer-Verlag, Berlin, New York pp. 386–397.
7. Preneel, B., Govaerts, R., Vandewalle, J.: Boolean functions satisfying higher order propagation criteria. In Advances in Cryptology - EUROCRYPT'91 (1991) vol. 547, LNCS Springer-Verlag, Berlin, New York pp. 141–152.
8. Preneel, B., Leekwijck, W. V., Linden, L. V., Govaerts, R., Vandewalle, J.: Propagation characteristics of boolean functions. In Advances in Cryptology - EUROCRYPT'90 (1991) vol. 437, LNCS Springer-Verlag, Berlin, New York pp. 155–165.
9. Rothaus, O. S.: On "bent" functions. Journal of Combinatorial Theory **Ser. A, 20** (1976) 300–305.
10. Seberry, J., Zhang, X. M., Zheng, Y.: Nonlinearity and propagation characteristics of balanced boolean functions. Information and Computation **119** (1995) 1–13.
11. Seberry, J., Zhang, X. M., Zheng, Y.: The relationship between propagation characteristics and nonlinearity of cryptographic functions. Journal of Universal Computer Science **1** (1995) 136–150. (available at `http://hgiicm.tu-graz.ac.at/`)
12. Zhang, X. M., Zheng, Y.: GAC — the criterion for global avalanche characteristics of cryptographic functions. Journal of Universal Computer Science **1** (1995) 316–333. (available at `http://hgiicm.tu-graz.ac.at/`)
13. Zhang, X. M., Zheng, Y.: Characterizing the structures of cryptographic functions satisfying the propagation criterion for almost all vectors. Design, Codes and Cryptography **7** (1996) 111–134.

This article was processed using the LaTeX macro package with LLNCS style