The Nonhomomorphicity of Boolean Functions

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

[1] School of Info Tech & Comp Sci, the University of Wollongong, Wollongong NSW 2522, Australia. xianmo@cs.uow.edu.au

[2] School of Comp & Info Tech, Monash University, McMahons Road, Frankston, Melbourne, VIC 3199, Australia. yuliang@pscit.monash.edu.au

URL: http://www.pscit.monash.edu.au/links/

Abstract. We introduce the notion of *nonhomomorphicity* as an alternative criterion that forecasts nonlinear characteristics of a Boolean function. Although both *nonhomomorphicity* and *nonlinearity* reflect a "difference" between a Boolean function and all the affine functions, they are measured from different perspectives. We are interested in nonhomomorphicity due to several reasons that include (1) unlike other criteria, we have not only established tight lower and upper bounds on the nonhomomorphicity of a function, but also precisely identified the mean of nonhomomorphicity over all the Boolean functions on the same vector space, (2) the nonhomomorphicity of a function can be estimated efficiently, and in fact, we demonstrate a fast statistical method that works both on large and small dimensional vector spaces.

Key Words: Boolean Functions, Cryptography, Nonhomomorphicity, Nonlinear Characteristics.

1 Motivation of this Research

It is known that a function f on V_n is affine if and only if f satisfies such property that for any even k with $k \geq 4$,

$$f(u_1) \oplus \cdots \oplus f(u_k) = 0 \tag{1}$$

whenever $u_1 \oplus \cdots \oplus u_k = 0$.

In addition, it can be verified that f is affine if and only if there exists an even k with $k \geq 4$ such that (1) holds whenever $u_1 \oplus \cdots \oplus u_k = 0$. Therefore we regard (1) as a characteristic that is useful in telling a non-affine function from an affine one.

Now consider a non-affine function f on V_n. Let k be an even with $k \geq 4$ and $(u_1, \ldots, u_k)$ be a k-tuples with $u_1 \oplus \cdots \oplus u_k = 0$. If

$$f(u_1) \oplus \cdots \oplus f(u_k) = 0$$

then f satisfies the affine property at the particular vector $(u_1, \ldots, u_k)$. On the other hand, if

$$f(u_1) \oplus \cdots \oplus f(u_k) = 1$$

S. Tavares and H. Meijer (Eds.): SAC'98, LNCS 1556, pp. 280–295, 1999.

then f behaves in a way that is against the affine property at $(u_1, \ldots, u_k)$.

The above observations motivate us to define the number of k-tuples of vectors in V_n, $(u_1, \ldots, u_k)$ with $u_1 \oplus \cdots \oplus u_k = 0$ such that the affine property (1) is satisfied, as the *homomorphicity* of f, and furthermore, the number of k-tuples of vectors in V_n, $(u_1, \ldots, u_k)$ with $u_1 \oplus \cdots \oplus u_k = 0$ such that the affine property (1) is not satisfied, as the *nonhomomorphicity* of f.

While nonhomomorphicity and nonlinearity are similar to each other in that they both reflect a "distance" between a Boolean function and all the affine functions, the former differentiates itself from the latter in the way the "distance" is measured. Nonhomomorphicity has several interesting properties suggesting that it can serve as a useful nonlinearity indicator: (1) unlike other criteria, we have not only established the tight lower and upper bounds on nonhomomorphicity, but also precisely identified the mean of nonhomomorphicity over all the Boolean functions with the same size, (2) the nonhomomorphicity of a function can be estimated efficiently. In fact, we show a fast statistical method for estimating the nonhomomorphicity of a function. The computing time of the statistical method is not relevant to the dimension (number of variables) of the function. This guarantees that we can use a computer program to analyze Boolean functions of higher dimensions efficiently.

2 Introduction to Boolean Functions

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

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 on V_n respectively, then $\tilde{a} * \tilde{b}$ is the sequence of $f \oplus g$.

Let $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$ be two vectors (or sequences), 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.

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

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

Let ℓ_i, $0 \le i \le 2^n - 1$, be the i row of H_n. Then 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. (See for instance Lemma 2 of [7].)

Definition 1. *A function f on V_n is called an* affine *function if $f(x) = c \oplus a_1x_1 \oplus \cdots \oplus a_nx_n$ where and each a_j and c are constant in $GF(2)$. In particular, f is called a* linear *function if $c = 0$.*

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

It is known that the nonlinearity of a function f on V_n can be expressed as

$$N_f = 2^{n-1} - \frac{1}{2}\max\{|\langle \xi, \ell_i \rangle|, 0 \le i \le 2^n - 1\} \tag{3}$$

where ξ is the sequence of f and ℓ_0, $\dots$, ℓ_{2^n-1} are the rows of H_n, namely, the sequences of the linear functions on V_n. (For a proof of (3) see for instance Lemma 6 of [7].) In addition, the maximum nonlinearity of a function is $2^{n-1} - 2^{\frac{1}{2}n-1}$, namely, $N_f \le 2^{n-1} - 2^{\frac{1}{2}n-1}$.

Given a function f on V_n, a $(1,-1)$ matrix defined by $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$, where $\alpha_i, \alpha_j \in V_n$ and $0 \le i, j \le 2^n - 1$, is called the $(1,-1)$ incidence matrix, or simply, the matrix of f. The following is attributed to R. L. McFarland [2]:

$$M = 2^{-n} H_n \operatorname{diag}(\langle \xi, \ell_0 \rangle, \langle \xi, \ell_1 \rangle, \dots, \langle \xi, \ell_{2^n-1} \rangle) H_n \tag{4}$$

where ξ be the sequence of function f on V_n, ℓ_i be the ith row of H_n, and $\operatorname{diag}(a, b, \cdots, c)$ denotes the diagonal matrix whose entries on the diagonal are $a, b, \dots, c$.

A function f on V_n is called a bent function [6] if $\langle \xi, \ell_i \rangle^2 = 2^n$ for every $i = 0, 1, \dots, 2^n - 1$, where ξ is the sequence of f and ℓ_i is a row in H_n. A bent function on V_n exists only when n is a positive even number, and it achieves the highest possible nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$.

3 Homomorphicity and Nonhomomorphicity

The following lemma is important in this paper, as it explores a characteristic property of affine functions which will be useful in studying nonhomomorphicity.

Lemma 1. *Let f be a function on V_n. Then* *(i) f is an affine function if and only if f satisfies such property that for any even k with $k \geq 4$, $f(u_1) \oplus \cdots \oplus f(u_k) = 0$ whenever $u_1 \oplus \cdots \oplus u_k = 0$,*

(ii) f is an affine function if and only if there exists an even k with $k \geq 4$ such that $f(u_1) \oplus \cdots \oplus f(u_k) = 0$ whenever $u_1 \oplus \cdots \oplus u_k = 0$.

Proof. Let f be a function on V_n. We first prove Part (ii) of the lemma.

Assume that f is affine. By using Definition 1, it is easy to verify that for any even k with $k \geq 4$, $f(u_1) \oplus \cdots \oplus f(u_k) = 0$ whenever $u_1 \oplus \cdots \oplus u_k = 0$. Conversely, assume that there exists an even k with $k \geq 4$ such that $f(u_1) \oplus \cdots \oplus f(u_k) = 0$ whenever $u_1 \oplus \cdots \oplus u_k = 0$. We now prove that f is affine.

Let u_1 and u_2 be any two vectors in V_n. Obviously, the k vectors u_1, u_2, $u_1 \oplus u_2$, $0, \ldots, 0$ satisfy $u_1 \oplus u_2 \oplus (u_1 \oplus u_2) \oplus 0 \oplus \cdots \oplus 0 = 0$. From the assumption,

$$f(u_1) \oplus f(u_2) \oplus f(u_1 \oplus u_2) \oplus f(0) \oplus \cdots \oplus f(0) = 0 \tag{5}$$

Consider two cases: $f(0) = 0$ and $f(0) = 1$.

Case 1: $f(0) = 0$. In this case $f(c\alpha) = cf(\alpha)$ holds for any vector $\alpha \in V_n$ and any value $c \in GF(2)$. Hence (5) can be rewritten as

$$f(u_1 \oplus u_2) = f(u_1) \oplus f(u_2) \tag{6}$$

where u_1 and u_2 are arbitrary.

Let e_j denote the vector in V_n, whose the jth component is one and others are zero. For any fixed value x_j in $GF(2)$, $j = 1, \ldots, n$, from (6), $f(x_1 e_1 \oplus \cdots \oplus x_n e_n) = f(x_1 e_1) \oplus f(x_2 e_2 \oplus \cdots \oplus x_n e_n)$ Applying (6) repeatedly, we have $f(x_1 e_1 \oplus \cdots \oplus x_n e_n) = f(x_1 e_1) \oplus f(x_2 e_2) \oplus \cdots \oplus f(x_n e_n)$ Note that $f(0) = 0$ implies $f(c\alpha) = cf(\alpha)$ where c is any value in $GF(2)$ and α is any vector in V_n. Hence

$$f(x_1 e_1 \oplus \cdots \oplus x_n e_n) = x_1 f(e_1) \oplus \cdots \oplus x_n f(e_n) \tag{7}$$

From the definition of e_j, $x_1 e_1 \oplus \cdots \oplus x_n e_n = (x_1, \ldots, x_n)$. On the other hand, if we write $f(e_j) = a_j$, $j = 1, \ldots, n$ then (7) can be rewritten as $f(x_1, \ldots, x_n) = a_1 x_1 \oplus \cdots \oplus a_n x_n$ This proves that f is linear.

Case 2: $f(0) = 1$. Set $g(x) = 1 \oplus f(x)$. Then g is linear. By using the result in Case 1, $g(x_1, \ldots, x_n) = b_1 x_1 \oplus \cdots \oplus b_n x_n$ where each $b_j \in GF(2)$. Hence $f(x_1, \ldots, x_n) = 1 \oplus b_1 x_1 \oplus \cdots \oplus b_n x_n$ This proves that f is affine.

We now prove Part (i) of the lemma. Assume that f is affine. From Definition 1, it is easy to check that for any even k with $k \geq 4$, $f(u_1) \oplus \cdots \oplus f(u_k) = 0$ whenever $u_1 \oplus \cdots \oplus u_k = 0$. Conversely, assume f satisfies such property that for any even k with $k \geq 4$, $f(u_1) \oplus \cdots \oplus f(u_k) = 0$ whenever $u_1 \oplus \cdots \oplus u_k = 0$. Then from Part (ii) of the lemma, f must be affine. □

From the characteristic property shown in Lemma 1, if a function f on V_n satisfies $f(u_1) \oplus \cdots \oplus f(u_k) = 0$ for a large number of k-tuples $(u_1, \ldots, u_k)$ of vectors in V_n with $u_1 \oplus \cdots \oplus u_k = 0$, then the function behaves more like an affine function. This leads us to introduce a new nonlinearity criterion.

Notation 1. *Let f be a function on V_n and k an even with $4 \leq k \leq 2^n$. For $c \in GF(2)$, denote by $\mathcal{H}_{f,c}^{(k)}$ the collection of ordered k-tuples $(u_1, \ldots, u_k)$ of vectors in V_n with $u_1 \oplus \cdots \oplus u_k = 0$ satisfying $f(u_1) \oplus \cdots \oplus f(u_k) = c$ where $c \in GF(2)$ is constant.*

Definition 3. *Let f be a function on V_n and k an even with $4 \leq k \leq 2^n$. For $c \in GF(2)$, we call $\tilde{h}_{f,0}^{(k)} = \#\mathcal{H}_{f,0}^{(k)}$,* the kth-order homomorphicity *of f, and furthermore, $\tilde{h}_{f,1}^{(k)} = \#\mathcal{H}_{f,1}^{(k)}$,* the kth-order nonhomomorphicity *of f, where $\#S$ denotes the number of elements in a set S.*

Note that there exist $2^{(k-1)n}$ k-tuples of vectors in V_n, $(u_1, \ldots, u_k)$, satisfying $\bigoplus_{j=1}^{k} u_j = 0$. Hence an interesting fact on $\tilde{h}_{f,c}^{(k)}$ follows:

Lemma 2. *Let f be a function on V_n. Then $\tilde{h}_{f,0}^{(k)} + \tilde{h}_{f,1}^{(k)} = 2^{(k-1)n}$.*

We note that Lemma 1 cannot be extended to the case of odd k. This explains why we have not defined homomorphicity or nonhomomorphicity for an odd order.

4 Calculations of Nonhomomorphicity

4.1 High Order Auto-Correlation

Recall that the auto-correlation of a function is defined as follows:

Definition 4. *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 $f(x) \oplus f(x \oplus \alpha)$. Let $\Delta(\alpha)$ be the scalar product of $\xi(0)$ and $\xi(\alpha)$. Namely*

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

$\Delta(\alpha)$ is called the auto-correlation of f *with a shift α.*

Obviously, $\Delta(\alpha) = 0$ if and only if $f(x) \oplus f(x \oplus \alpha)$ is balanced, i.e., f satisfies the propagation criterion with respect to α. On the other hand, if $|\Delta(\alpha)| = 2^n$, then $f(x) \oplus f(x \oplus \alpha)$ is a constant and hence α is a linear structure of f.

Next we consider a generalization of the definition for auto-correlation. The generalization will turn out to be a useful tool in studying nonhomomorphic characteristics of functions.

Definition 5. *Let f be a function on V_n and $\xi = (a_0, a_1, \ldots, a_{2^n-1})$ be the sequence of f. For a vector $\alpha \in V_n$ and an integer $k = 2, 3, \ldots$, the* kth-order auto-correlation *of f with a shift α, denoted by $\Delta^{(k)}(\alpha)$, is defined as*

$$\Delta^{(2)}(\alpha) = \Delta(\alpha), \;\; \Delta^{(k)}(\alpha) = \sum_{j=0}^{2^n-1} [a_j \Delta^{(k-1)}(\alpha_j \oplus \alpha)], \; k = 3, 4, \ldots$$

where $\Delta(\alpha)$ is the auto-correlation of f as defined in Definition 4, and α_j is the vector corresponding to the integer j.

It is important to point out that nonhomomorphicity, high order auto-correlation and high order derivation introduced in [4] are three completely different concepts. Let f be a function on V_n. In [4], the *derivation* of f at vector β, denoted by $\Delta_\beta f(x)$, is defined as follows

$$\Delta_\beta f(x) = f(x) \oplus f(x \oplus \beta).$$

and the *kth-order derivation* of f at vectors $\beta_1, \ldots, \beta_k$, denoted by $\Delta^{(k)}_{\beta_1,\ldots,\beta_k} f(x)$, is defined recursively as

$$\Delta^{(k)}_{\beta_1,\ldots,\beta_k} f(x) = \Delta(\Delta^{(k-1)}_{\beta_1,\ldots,\beta_{k-1}} f(x)).$$

We can see the kth-order derivation of f at vectors $\beta_1, \ldots, \beta_k$, $\Delta^{(k)}_{\beta_1,\ldots,\beta_k} f(x)$, is itself a *function* on V_n. In contrast, both the kth-order nonhomomorphicity and the kth-order auto-correlation of f with a shift β are fixed integer values. To examine further how the three concepts differ, consider a bent function f of degree s. For k even with $k > s$, the kth-order derivation of f at vectors $\beta_1, \ldots, \beta_k$, $\Delta^{(k)}_{\beta_1,\ldots,\beta_k} f(x)$, is obviously the zero function. In contrast, for the kth-order auto-correlation of f, we have $\Delta^{(k)}(0) = 2^{-n} \sum_{i=0}^{2^n-1} \langle \xi, \ell_i \rangle^k = 2^{\frac{1}{2}nk}$ (which follows from Corollary 1 and Lemma 3 to be introduced later on), and for the kth-order nonhomomorphicity of f, we have $\tilde{h}^{(k)}_{f,1} = 2^{(k-1)n-1} - 2^{\frac{1}{2}nk-1}$, which follows from Theorem 3 in Section 5.

To examine the properties of the kth-order auto-correlation $\Delta^{(k)}(\alpha)$, we consider a matrix defined by $(\Delta^{(k)}(\alpha_i \oplus \alpha_j))$ where $i, j = 0, 1, \ldots, 2^n - 1$. Note that the diagonal of the matrix $(\Delta^{(k)}(\alpha_i \oplus \alpha_j))$ is composed of 2^n repetitions of $\Delta^{(k)}(0)$. By simple induction on k, we have the following result:

Theorem 1. *Let f be a function on V_n, M be the matrix of f and ξ be the sequence of f. Then*

$$(\Delta^{(k)}(\alpha_i \oplus \alpha_j)) = M^k = 2^{-n} H_n \, diag(\langle \xi, \ell_0 \rangle^k, \langle \xi, \ell_1 \rangle^k, \ldots, \langle \xi, \ell_{2^n-1} \rangle^k) H_n$$

where ℓ_0, ℓ_1, …, ℓ_{2^n-1} are the rows of H_n.

This result shows that the two matrices, $(\Delta^{(k)}(\alpha_i \oplus \alpha_j))$ and

$$\mathrm{diag}(\langle \xi, \ell_0 \rangle^k, \langle \xi, \ell_1 \rangle^k, \ldots, \langle \xi, \ell_{2^n-1} \rangle^k)$$

are similar in the sense that from the former one can easily find out the latter through the use of H_n, and vice versa. Furthermore, it is not hard to see that the sum of the entries on the diagonal of $(\Delta^{(k)}(\alpha_i \oplus \alpha_j))$ is identical to that of $\mathrm{diag}(\langle \xi, \ell_0 \rangle^k, \langle \xi, \ell_1 \rangle^k, \ldots, \langle \xi, \ell_{2^n-1} \rangle^k)$. In other words,

$$\sum_{i=0}^{2^n-1} \Delta^{(k)}(\alpha_i \oplus \alpha_i) = 2^n \Delta^{(k)}(0) = \sum_{i=0}^{2^n-1} \langle \xi, \ell_i \rangle^k.$$

Hence we have proved

Corollary 1. *Let f be a function on V_n, M be the matrix of f and ξ be the sequence of f. Then $\Delta^{(k)}(0) = 2^{-n}\sum_{i=0}^{2^n-1}\langle\xi,\ell_i\rangle^k$.*

For $k = 2$, we have $\Delta^{(2)}(0) = 2^n$. This indicates that Corollary 1 embodies Parseval's equation (Page 416 of [5]) $\sum_{i=0}^{2^n-1}\langle\xi,\ell_i\rangle^2 = 2^{2n}$ as a special case in which $k = 2$.

4.2 Expression of Nonhomomorphicity by Other Indicators

Recall (3), the nonlinearity of a function f on V_n is related to the maximum $|\langle\xi,\ell_i\rangle|$, where ξ is the sequence of f and ℓ_i is the ith row of H_n. We give a precise expression of nonhomomorphicity by using the same indicator.

Theorem 2. *For a function f on V_n and k an even with $4 \le k \le 2^n$. $\tilde{h}_{f,0}^{(k)}$ and $\tilde{h}_{f,1}^{(k)}$ can be expressed as follows:*

(i) $\tilde{h}_{f,0}^{(k)} = 2^{(k-1)n-1} + \frac{1}{2}\Delta^{(k)}(0) = 2^{(k-1)n-1} + 2^{-n-1}\sum_{i=0}^{2^n-1}\langle\xi,\ell_i\rangle^k$

(ii) $\tilde{h}_{f,1}^{(k)} = 2^{(k-1)n-1} - \frac{1}{2}\Delta^{(k)}(0) = 2^{(k-1)n-1} - 2^{-n-1}\sum_{i=0}^{2^n-1}\langle\xi,\ell_i\rangle^k$

where ξ is the sequence of f and ℓ_i denotes the ith row of H_n.

Proof. We need only to prove that $\tilde{h}_{f,1}^{(k)} = 2^{(k-1)n-1} - \frac{1}{2}\Delta^{(k)}(0)$, as the rest part of the theorem follows from Corollary 1 and the fact that $\tilde{h}_{f,0}^{(k)} + \tilde{h}_{f,1}^{(k)} = 2^{(k-1)n}$.

Write $\xi = (a_0, a_1, \ldots, a_{2^n-1})$ where each $a_j = \pm 1$. Consider $u_j \in V_n$, $j = 1,\ldots,k$, and $\bigoplus_{j=1}^k u_j = 0$. Clearly, $\bigoplus_{j=1}^k f(u_j) = 1$ if and only if $\Pi_{j=1}^k a_{u_j} = -1$ where the subscript u_j in a_{u_j} is viewed as the integer representation of vector u_j. It is easy to verify

$$\frac{1}{2}(1 - \Pi_{j=1}^k a_{u_j}) = \begin{cases} 1 \text{ if } \bigoplus_{j=1}^k f(u_j) = 1 \\ 0 \text{ if } \bigoplus_{j=1}^k f(u_j) = 0 \end{cases}$$

Hence

$$\begin{aligned}
\tilde{h}_{f,1}^{(k)} &= \frac{1}{2}\sum_{\bigoplus_{j=1}^k u_j = 0}(1 - a_{u_j}a_{u_2}\cdots a_{u_k}) \\
&= \frac{1}{2}\sum_{u_1,\ldots,u_{k-1}\in V_n}(1 - a_{u_1}a_{u_2}\cdots a_{u_{k-1}}a_{u_1\oplus u_2\oplus\cdots\oplus u_{k-1}}) \\
&= 2^{(k-1)n-1} - \frac{1}{2}\sum_{u_1,\ldots,u_{k-1}\in V_n} a_{u_1}a_{u_2}\cdots a_{u_{k-1}}a_{u_1\oplus u_2\oplus\cdots\oplus u_{k-1}} \\
&= 2^{(k-1)n-1} \\
&\quad - \frac{1}{2}\sum_{u_1,\ldots,u_{k-2}\in V_n} a_{u_1}a_{u_2}\cdots a_{u_{k-2}}\sum_{u_{k-1}\in V_n} a_{u_{k-1}}a_{u_1\oplus u_2\oplus\cdots\oplus u_{u_{k-2}}\oplus u_{k-1}}
\end{aligned}$$

$$
\begin{aligned}
&= 2^{(k-1)n-1} - \frac{1}{2} \sum_{u_1,\ldots,u_{k-2}\in V_n} a_{u_1}a_{u_2}\cdots a_{u_{k-2}}\Delta^{(2)}(u_1\oplus u_2\oplus\cdots\oplus u_{k-2}) \\
&= 2^{(k-1)n-1} \\
&\quad - \frac{1}{2} \sum_{u_1,\ldots,u_{k-3}\in V_n} a_{u_1}a_{u_2}\cdots a_{u_{k-3}} \sum_{u_{k-2}\in V_n} a_{u_{k-2}}\Delta^{(2)}(u_1\oplus u_2\oplus\cdots\oplus u_{k-2}) \\
&= 2^{(k-1)n-1} - \frac{1}{2} \sum_{u_1,\ldots,u_{k-3}\in V_n} a_{u_1}a_{u_2}\cdots a_{u_{k-3}}\Delta^{(3)}(u_1\oplus u_2\oplus\cdots\oplus u_{k-3}) \\
&\ \ \vdots \\
&= 2^{(k-1)n-1} - \frac{1}{2} \sum_{u_1,u_2\in V_n} a_{u_1}a_{u_2}\Delta^{(k-2)}(u_1\oplus u_2) \\
&= 2^{(k-1)n-1} - \frac{1}{2} \sum_{u_1\in V_n} a_{u_1\in V_n} \sum_{u_2\in V_n} a_{u_2}\Delta^{(k-2)}(u_1\oplus u_2) \\
&= 2^{(k-1)n-1} - \frac{1}{2} \sum_{u_1\in V_n} a_{u_1\in V_n}\Delta^{(k-1)}(u_1) = 2^{(k-1)n-1} - \frac{1}{2}\Delta^{(k)}(0).
\end{aligned}
$$

This completes the proof. □

5 Bounds on Nonhomomorphicity

First we introduce Hölder's Inequality [3] that will be used in our discussions on lower and upper bounds. It states that for real numbers $c_j \geq 0$, $d_j \geq 0$, $j = 1, \ldots, k$, p and q with $p > 1$ and $\frac{1}{p} + \frac{1}{q} = 1$, the following is true:

$$
(\sum_{j=1}^{k} c_j^p)^{1/p}(\sum_{j=1}^{k} d_j^q)^{1/q} \geq \sum_{j=1}^{k} c_j d_j \tag{8}
$$

where the quality holds if and only if there exists a constant $\nu \geq 0$ such that $c_j = \nu d_j$ for each $j = 1, \ldots, k$.

By using Hölder's Inequality, we can prove

Lemma 3. *Let f be a function on V_n and k an even integer with $k \geq 4$. Then*

$$
\sum_{i=0}^{2^n-1} \langle \xi, \ell_i \rangle^k \geq 2^{n+\frac{1}{2}nk}
$$

where the equality holds if and only if n is even and f is bent.

Armed with the above result, next we show a bound on nonhomomorphicity.

Theorem 3. *Let f be a function on V_n and k an even integer with $k \geq 4$. Then the following statements hold:*

(i) $\tilde{h}_{f,1}^{(k)}$ *satisfies*

$$2^{(k-1)n-1} - \frac{1}{2}(2^n - 2N_f)^k \le \tilde{h}_{f,1}^{(k)} \le 2^{(k-1)n-1} - 2^{\frac{1}{2}nk-1} \qquad (9)$$

where N_f *denotes the nonlinearity of* f*,*

(ii) An equality in (9) holds if and only if f *is bent. In other words,* f *is bent if and only if*

$$\tilde{h}_{f,1}^{(k)} = 2^{(k-1)n-1} - 2^{\frac{1}{2}nk-1}.$$

Recall that the nonlinearity of a function reaches the minimum nonlinearity if and only if the function is affine while the nonlinearity of a function reaches the maximum nonlinearity if and only if the function is bent. The above theorem shows there exists a consistent relationship between nonlinearity and nonhomomorphicity, especially when the order of nonhomomorphicity is large. Thus, if $\tilde{h}_{f,1}^{(k)}$ is large, we expect that f is closer to a bent function than to an affine one, and conversely if $\tilde{h}_{f,1}^{(k)}$ is small, then the function is closer to affine than to bent.

As $\tilde{h}_{f,0}^{(k)} + \tilde{h}_{f,1}^{(k)} = 2^{(k-1)n}$, we have the following complementary result:

Corollary 2. *Let* f *be a function on* V_n *and* k *an even integer with* $k \ge 4$*. Then the following statements hold:*

(i) $\tilde{h}_{f,0}^{(k)}$ *satisfies*

$$2^{(k-1)n-1} + 2^{\frac{1}{2}nk-1} \le \tilde{h}_{f,0}^{(k)} \le 2^{(k-1)n-1} + \frac{1}{2}(2^n - 2N_f)^k 2^{(k-1)n-1} \quad (10)$$

where N_f *denotes the nonlinearity of* f*,*

(ii) An equality in (10) holds if and only if f *is bent. In other words,* f *is bent if and only if*

$$\tilde{h}_{f,0}^{(k)} = 2^{(k-1)n-1} + 2^{\frac{1}{2}nk-1}.$$

A consequence of Theorem 3 and Corollary 2 is

Corollary 3. *Let* f *be a function on* V_n *and* k *an even integer with* $k \ge 4$*. Then* $\tilde{h}_{f,0}^{(k)} - \tilde{h}_{f,1}^{(k)} \ge 2^{\frac{1}{2}nk}$*, and the equality holds if and only if* f *is bent.*

An implication of the above corollary is that there exists no function on V_n such that $\tilde{h}_{f,0}^{(k)} = \tilde{h}_{f,1}^{(k)}$.

6 Comparing Nonhomomorphicity and Nonlinearity

A natural question on nonhomomorphicity is how it is related to other nonlinear characteristics, such as nonlinearity which indicates the minimum distance between a particular function and all the affine functions. It turns out that nonhomomorphicity and nonlinearity are two indicators that are not directly comparable. We demonstrate this by inspecting three specific functions f, g and h on V_{2s} with $s \ge 5$.

Recall that the rows in H_s, the Sylvester-Hadamard matrix of order 2^s, are denoted by ℓ_i, $i = 0, 1, \ldots, 2^s - 1$. The three functions are defined as follows:

1. f — the sequence of f is the concatenation of ℓ_1, ℓ_2, ..., ℓ_{2^s-1} with ℓ_1 being repeated twice, i.e., $\ell_1, \ell_1, \ell_2, \ldots, \ell_{2^s-1}$.
2. g — the sequence of g is composed of four repetitions of a bent sequence η of length 2^{2s-2}, i.e., η, η, η, η.
3. h — the sequence of f is the concatenation of ℓ_1, ℓ_4, ..., ℓ_{2^s-1} with ℓ_1 being repeated four times, i.e., $\ell_1, \ell_1, \ell_1, \ell_1, \ell_4, \ldots, \ell_{2^s-1}$.

By using (3), we know that the nonlinearities of the three functions are $N_f = N_g = 2^{2s-1} - 2^s$, and $N_h = 2^{2s-1} - 2^{s+1}$.

Consider k even with $k \geq 4$. By Theorem 2, we have the following nonhomomorphic characteristics for the three functions:

$$\begin{aligned}
\tilde{h}^{(k)}_{f,1} &= 2^{2(k-1)s-1} - 2^{-2s-1}(2^{sk+2s} - 2^{sk+s+1} + 2^{sk+k+s-1}) \\
\tilde{h}^{(k)}_{g,1} &= 2^{2(k-1)s-1} - 2^{-2s-1} \cdot 2^{sk+k+2s-2} \\
\tilde{h}^{(k)}_{h,1} &= 2^{2(k-1)s-1} - 2^{-2s-1}(2^{sk+2s} - 2^{sk+s+2} + 2^{sk+2k+s-2})
\end{aligned}$$

Thus for these three functions f, g and h, their nonlinearities and nonhomomorphic characteristics are related as follows:

(i) f v.s. g: $N_f = N_g$, but $\tilde{h}^{(k)}_{f,1} > \tilde{h}^{(k)}_{g,1}$.
(ii) f v.s. h: $N_f > N_h$, and $\tilde{h}^{(k)}_{f,1} > \tilde{h}^{(k)}_{h,1}$.
(iii) g v.s. h: $N_g > N_h$, but $\tilde{h}^{(k)}_{g,1} < \tilde{h}^{(k)}_{h,1}$ if $k \leq s-1$, and $\tilde{h}^{(k)}_{g,1} > \tilde{h}^{(k)}_{h,1}$ if $k \geq s$.

Properties of these three functions clearly show that nonlinearity and nonhomomorphicity are not comparable indicators. They, however, can be used to complement each other in studying cryptographic properties of functions.

The two functions g and h are of particular interest: while $\tilde{h}^{(k)}_{g,1} < \tilde{h}^{(k)}_{h,1}$ for $k \leq s-1$, their positions are reversed for $k \geq s$. This motivates us to examine the behavior of nonhomomorphicity as k becomes large.

Theorem 4. *Let f and g be two functions on V_n. If $\tilde{h}^k_{f,1} \neq \tilde{h}^k_{g,1}$, then there is an even positive k_0, such that $\tilde{h}^k_{f,1} < \tilde{h}^k_{g,1}$ for every even k with $k \geq k_0$, or $\tilde{h}^k_{f,1} > \tilde{h}^k_{g,1}$ for every even k with $k \geq k_0$.*

Assume that $N_f > N_g$. Then from (3), we have

$$\max\{|\langle \xi, \ell_i \rangle|, 0 \leq i \leq 2^n - 1\} < \max\{|\langle \eta, \ell_i \rangle|, 0 \leq i \leq 2^n - 1\}.$$

Using a similar proof to that for the above theorem, we can show

Theorem 5. *Let f and g be two functions on V_n. If $N_f > N_g$, then there is an even positive k_0, such that $\hbar^k_{f,1} > \hbar^k_{g,1}$ for every even k with $k \geq k_0$.*

While Theorem 5 shows that nonhomomorphicity and nonlinearity are consistent when the dimension k is large, the three example functions f, g and h, together with Theorems 4 and 5, do indicate that nonhomomorphic characteristics of a function cannot be fully predicted by other cryptographic criteria, such as nonlinearity. Therefore, nonhomomorphicity can serve as another important indicator that forecasts certain cryptographically useful properties of the function.

Comparing (ii) of Theorem 2 and (3), we find that although both nonlinearity and nonhomomorphicity reflect non-affine characteristics, the former focuses on the maximum $|\langle \xi, \ell_i \rangle|$ while the latter is more concerned over all $|\langle \xi, \ell_i \rangle|$.

7 The Mean of Homomorphicity and Nonhomomorphicity

Let f be a function on V_n, χ denote an indicator (a criterion or a value), and χ_f denote the indicator of f. Note that there precisely 2^{2^n} functions on V_n. We are concerned with the mean of the indicator χ over all the functions on V_n, denoted by $\overline{\chi}$, i.e. $\overline{\chi} = 2^{-2^n} \sum_f \chi_f$.

The upper and lower bounds on χ_f cannot provide sufficient information on the distribution of χ of a majority of functions. For this reason, we argue that the mean of the indicator χ over all the functions on V_n, i.e. $\overline{\chi} = 2^{-2^n} \sum_f \chi_f$, should also be investigated. Note that there exist precisely 2^{2^n} functions with n variables.

Notation 2. *Let O_k (k is even) denote the collection of k-tuples $(u_1, \ldots, u_k)$ of vectors in V_n satisfying $u_{j_1} = u_{j_2}, \ldots, u_{j_{k-1}} = u_{j_k}$, where $\{j_1, j_2, \ldots, j_k\} = \{1, 2, \ldots, k\}$. Write $o_k = \#O_k$.*

It is easy to verify

Lemma 4. *Let n and k be positive integers and $u_1 \oplus \cdots \oplus u_k = 0$, where each u_j is a fixed vector in V_n. Then*

$$f(u_1) \oplus \cdots \oplus f(u_k) = 0$$

holds for every function f on V_n if and only if k is even and $(u_1, \ldots, u_k) \in O_k$.

Lemma 5. *In Notation 2, let k be an even with $2 \leq k \leq 2^n$. Then*

$$o_k = \sum_{t=1}^{k/2} \binom{2^n}{t} \sum_{p_1+\cdots+p_t=k/2,\ p_j>0} \frac{(k)!}{(2p_1)! \cdots (2p_t)!}$$

Proof. Let $(u_1, \ldots, u_k) \in O_k$. Then the multiple set $\{u_1, \ldots, u_k\}$ can be divided into t disjoint subsets $\Pi_1, \ldots, \Pi_t$ where (1) $1 \leq t \leq k$, (2) each Π_j is a $2p_j$ ($p_j > 0$) copy of a vector β_j i.e. $\Pi_j = \{\beta_j, \ldots, \beta_j\}$ and $|\Pi_j| = 2p_j$, (3) $\beta_j \neq \beta_i$, if $j \neq i$, (4) $\{u_1, \ldots, u_k\} = \Pi_1 \cup \cdots \cup \Pi_t$.

Note that there exist $\binom{2^n}{t}$ different choices of t distinguished vectors $\beta_1, \dots, \beta_t$ from V_n. Arranging each multiple set $\{u_1, \dots, u_k\}$, we obtain precisely $(k)!/(2p_1)! \cdots (2p_t)!$ distinguished ordered sets. Note that $2p_1 + \cdots + 2p_t = k$ and $1 \le t \le k/2$. The proof is completed. □

From Lemma 4, if $(u_1, \dots, u_k) \in O_k$ then $f(u_1) \oplus \cdots \oplus f(u_k) = 0$ holds for every function f on V_n. Therefore, in this case $f(u_1) \oplus \cdots \oplus f(u_k) = 0$ with $u_1 \oplus \cdots \oplus u_k = 0$ does not really reflect an affine property. Hence we focus on $\mathcal{H}_{f,0}^{(k)} - O_k$ and $\mathcal{H}_{f,1}^{(k)}$.

Theorem 6. *Let k be an even with $2 \le k \le 2^n$. Then*

(i) the mean of $\tilde{h}_{f,0}^{(k)}$ over all the functions on V_n i.e. $2^{-2^n} \sum_f \tilde{h}_{f,0}^{(k)}$, satisfies

$$2^{-2^n} \sum_f \tilde{h}_{f,0}^{(k)} = \frac{1}{2} o_k + 2^{(k-1)n-1}$$

where o_k is given in Lemma 5.

(ii) the mean of $\tilde{h}_{f,1}^{(k)}$ over all the functions on V_n i.e. $2^{-2^n} \sum_f \tilde{h}_{f,1}^{(k)}$, satisfies

$$2^{-2^n} \sum_f \tilde{h}_{f,1}^{(k)} = -\frac{1}{2} o_k + 2^{(k-1)n-1}$$

Proof. To prove Part (i), we consider two cases for $(u_1, \dots, u_k) \in \mathcal{H}_{f,0}^{(k)}$.

Case 1: $(u_1, \dots, u_k) \in O_k$. From Lemma 4, $f(u_1) \oplus \cdots \oplus f(u_k) = 0$ holds for every function f on V_n.

Case 2: $(u_1, \dots, u_k) \in \mathcal{H}_{f,0}^{(k)} - O_k$. Note that $f(u_1) \oplus \cdots \oplus f(u_k)$ takes the value zero and the value one with an equal probability of a half for a random function f on V_n. Therefore

$$\begin{aligned} 2^{-2^n} \sum_f \tilde{h}_{f,0}^{(k)} &= 2^{-2^n} \sum_f \# O_k + 2^{-2^n} \sum_f \#(\mathcal{H}_{f,0}^{(k)}(0) - O_k) = o_k + \frac{1}{2}[2^{(k-1)n} - o_k] \\ &= \frac{1}{2} o_k + 2^{(k-1)n-1} \end{aligned}$$

This proves (i) of the theorem.

Part (ii) can be proven in a similar way, once again by noting that $f(u_1) \oplus \cdots \oplus f(u_k)$ takes the value zero and the value one with an equal probability of a half, for a a random function f on V_n. □

A function whose nonhomomorphicity is larger than the mean, namely $\tilde{h}_{f,1}^{(k)} > 2^{-2^n} \sum_f \tilde{h}_{f,1}^{(k)}$, indicates that the function is more nonlinear. The converse also holds.

8 Relative Nonhomomorphicity

The concept of relative nonhomomorphicity introduced in this section is useful for a statistical tool to be introduced later.

Notation 3. *Let k be an even with $k \geq 4$ and R_k denote the collection of ordered k-tuples $(u_1, \ldots, u_k)$ of vectors in V_n satisfying $u_1 \oplus \cdots \oplus u_k = 0$.*

We have noticed

$$\#R_k = 2^{(k-1)n} \text{ and } \#(R_k - O_k) = 2^{(k-1)n} - o_k. \tag{11}$$

From the proof of Theorem 6, if $(u_1, \ldots, u_k) \in R_s - O_k$ then $f(u_1) \oplus \cdots \oplus f(u_k)$ takes the value zero and the value one with equal probability.

Definition 6. *Let f be a function on V_n and k be an even with $k \geq 4$. Define the* kth-order relative nonhomomorphicity *of f, denoted by $\rho_{f,1}^{(k)}$, as $\rho_{f,1}^{(k)} = \frac{\tilde{h}_{f,1}^{(k)}}{\#(R_k - O_k)}$, i.e. $\rho_{f,1}^{(k)} = \frac{\tilde{h}_{f,1}^{(k)}}{2^{(k-1)n} - o_k}$.*

From Theorem 6, we obtain

Corollary 4. *Let k be an even with $2 \leq k \leq 2^n$. Then the mean of $\rho_{f,1}^{(k)}$ over all the functions on V_n i.e. $2^{-2^n} \sum_f \rho_{f,1}^{(k)}$, satisfies $2^{-2^n} \sum_f \rho_{f,1}^{(k)} = \frac{1}{2}$.*

From Corollary 4,

$$\rho_{f,1}^{(k)} \begin{cases} \geq \frac{1}{2} & \text{then the nonhomomorphicity of } f \text{ is not smaller than the mean} \\ < \frac{1}{2} & \text{then the nonhomomorphicity of } f \text{ is smaller than the mean} \end{cases} \tag{12}$$

In practice, if $\rho_{f,1}^{(k)}$ is much smaller than $\frac{1}{2}$, then f should be considered cryptographically weak.

9 Estimating Nonhomomorphicity

As shown in Theorem 2, the nonhomomorphicity of a function can be determined precisely. In this section, however, we introduce a statistical method to estimate nonhomomorphicity. Such a method is useful in fast analysis of functions.

Denote a real-valued $(0, 1)$ function on $R_k - O_k$, $t(u_1, \ldots, u_k)$, as follows

$$t(u_1, \ldots, u_k) = \begin{cases} 1, \text{ if } f(u_1) \oplus \cdots \oplus f(u_k) = 1 \\ 0, \text{ otherwise} \end{cases}$$

Hence from the definition of nonhomomorphicity we have

$$\tilde{h}_{f,1}^{(k)} = \sum_{(u_1,\ldots,u_k) \in R_k - O_k} t(u_1, \ldots, u_k)$$

Let Ω be a random subset of $R_k - O_k$. Write $\omega = \#\Omega$ and

$$\bar{t} = \frac{1}{\omega} \sum_{(u_1,\dots,u_k)\in\Omega} t(u_1,\dots,u_k) \tag{13}$$

Note that this is the "sample mean" [1]. In particular, $\Omega = R_n^{(k)} - O_k$, $\bar{t}$ is identified with the "true mean" or "population mean" [1], namely, $\rho_{f,1}^{(k)}$.

Now consider $\sum_{(u_1,\dots,u_k)\in\Omega}(t(u_1,\dots,u_k) - \bar{t})^2$. We have

$$\begin{aligned}\sum_{(u_1,\dots,u_k)\in\Omega} (t(u_1,\dots,u_k) - \bar{t})^2 = &\sum_{(u_1,\dots,u_k)\in\Omega} t^2(u_1,\dots,u_k) \\ &- 2\bar{t}\cdot \sum_{(u_1,\dots,u_k)\in\Omega} t(u_1,\dots,u_k) + \omega\bar{t}^2\end{aligned}$$

Note that $t^2(u_1,\dots,u_k) = t(u_1,\dots,u_k)$. From (13),

$$\begin{aligned}\sum_{(u_1,\dots,u_k)\in\Omega} (t(u_1,\dots,u_k) - \bar{t})^2 &= \omega\bar{t} - 2\omega\bar{t}^2 + \omega\bar{t}^2 = \omega\bar{t} - 2\omega\bar{t}^2 + \omega\bar{t}^2 \\ &= \omega\bar{t}(1-\bar{t})\end{aligned} \tag{14}$$

Hence the quantity of $\sqrt{\frac{1}{\omega-1}\sum_{(u_1,\dots,u_k)\in\Omega}(t(u_1,\dots,u_k) - \bar{t})^2}$, which is called the "sample standard deviation" [1] and is usually denoted by μ, can be expressed as

$$\mu = \sqrt{\frac{1}{\omega-1}\sum_{(u_1,\dots,u_k)\in\Omega}(t(u_1,\dots,u_k) - \bar{t})^2} = \sqrt{\frac{\omega\bar{t}(1-\bar{t})}{\omega-1}} \tag{15}$$

By using (4.4) in Section 4.B of [1], the "true mean" or "population mean", $\rho_{f,1}^{(k)}$, can be bounded by

$$\bar{t} - Z_{e/2}\frac{\mu}{\sqrt{\omega}} < \rho_{f,1}^{(k)} < \bar{t} + Z_{e/2}\frac{\mu}{\sqrt{\omega}} \tag{16}$$

where $Z_{e/2}$ denotes the value Z of a "standardized normal distribution" which to its right a fraction $e/2$ of the data, (16) holds with a probability of $(1-e)100\%$ [1].

For example,

when $e = 0.2$, $Z_{e/2} = 1.28$, and (16) holds with a probability of 80%,
when $e = 0.1$, $Z_{e/2} = 1.64$, and (16) holds with a probability of 90%,
when $e = 0.05$, $Z_{e/2} = 1.96$, and (16) holds with a probability of 95%,
when $e = 0.02$, $Z_{e/2} = 2.33$, and (16) holds with a probability of 98%,
when $e = 0.01$, $Z_{e/2} = 2.57$, and (16) holds with a probability of 99%,
when $e = 0.001$, $Z_{e/2} = 3.3$, and (16) holds with a probability of 99.9%.

From (13), $0 \leq \overline{t} < 1$ and it is easy to verify that μ in (15) satisfies $0 \leq \mu \leq \frac{1}{2}\sqrt{\frac{\omega}{\omega-1}}$, This implies that (16) can be simply replaced by

$$\overline{t} - \frac{Z_{e/2}}{2\sqrt{\omega - 1}} < \rho_{f,1}^{(k)} < \overline{t} + \frac{Z_{e/2}}{2\sqrt{\omega - 1}}, \tag{17}$$

where (17) holds with $(1-e)100\%$ probability. Hence if ω i.e. $\#\Omega$ is large, then the lower bound and the upper bound on $\rho_{f,1}^{(k)}$ in (16) are closer to each other. On the other hand, if we choose $\omega = \#\Omega$ large enough then $Z_{e/2}\frac{\mu}{\sqrt{\omega}}$ is sufficiently small, and hence (16) and (17) will provide us with useful information. For instance, viewing Corollary 4 and (17), we can choose $\omega = \#\Omega$ such that $\frac{Z_{e/2}}{2\sqrt{\omega-1}} < 10^{-p}$. Hence $\omega \geq Z_{e/2} \cdot 10^{2p}$ is large enough. In this case (17) is specialized as

$$\overline{t} - 10^{-p} < \rho_{f,1}^{(k)} < \overline{t} + 10^{-p} \tag{18}$$

where (18) holds with $(1-e)100\%$ probability.

In summary , we can analyze the nonhomomorphic characteristics of a function on V_n in the following steps:

1. we randomly fix even k with $k \geq 4$, for example, $k = 4, 6$ or 8, and randomly fix a large integer ω, for example, $\omega \geq Z_{e/2} \cdot 10^{2p}$, and randomly choose a subset of $R_k - O_k$, say Ω, with $\#\Omega = \omega$,
2. by using (13), we determine $\overline{t}$, i.e. "the sample mean",
3. by using (18), we determine the range of $\rho_{f,1}^{(k)}$ with a high reliability,
4. viewing $\rho_{f,1}^{(k)}$ in (18), from Corollary 4,

$$\rho_{f,1}^{(k)} \begin{cases} \geq \frac{1}{2} \text{ then } f \text{ is not less nonhomomorphic than the mean} \\ > \frac{1}{2} \text{ then } F \text{ is less nonhomomorphic than the mean} \end{cases} \tag{19}$$

   where (19) holds with $(1-e)\%$ probability,
5. if $\rho_{f,1}^{(k)}$ is much smaller than $\frac{1}{2}$ then f should be considered as cryptographically weak.

We have noticed that the statistical analysis has following advantages:

(1) the relative nonhomomorphicity, $\rho_{f,1}^{(k)}$ can be precisely identified by the use of "population mean" or "true mean",
(2) by using this method we do not need to search through the entire V_n,
(3) the method is highly reliable.

10 Extensions to S-boxes

Obviously, the concept of nonhomomorphicity of a Boolean function can be extended to that of an S-box in a straightforward way. Analysis of the general case of an S-box, however, has turned out to be far more complex. Nevertheless, we have obtained a number of interesting results on S-boxes, some of which encompass results presented in this paper. We will report the new results in a forthcoming paper. In the same paper we will also discuss how to utilize nonhomomorphic characteristics of an S-box employed by a block cipher in analyzing cryptographic weaknesses of the cipher.

11 Conclusions

Nonhomomorphicity is a new indicator for nonlinear characteristics of a function. It can complement the more widely used indicator of nonlinearity. Two useful properties of nonhomomorphicity are: (1) the mean of nonhomomorphicity over all the Boolean functions over the same vector space can be precisely identified, (2) the nonhomomorphicity of a function can be estimated efficiently, regardless of the dimension of the vector space.

12 Acknowledgment

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

References

1. Stephen A. Book. *Statistics*. McGraw-Hill Book Company, 1977.
2. J. F. Dillon. A survey of bent functions. *The NSA Technical Journal*, pages 191–215, 1972. (unclassified).
3. Friedhelm Erwe. *Differential And Integral Calculus*. Oliver And Boyd Ltd, Edinburgh And London, 1967.
4. X. Lai. Higher order derivatives and differential cryptanalysis. In *Proceedings of the Symposium on Communication, Coding and Cryptography, in the Honor of James L. Massey on the Occasion of his 60's Birthday*, pages 227–233. Kluwer Academic Publishers, 1994.
5. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, New York, Oxford, 1978.
6. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.
7. J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. *Information and Computation*, 119(1):1–13, 1995.