Restriction, Terms and Nonlinearity of Boolean Functions

Yuliang Zheng [a], Xian-Mo Zhang [b] and Hideki Imai [c]

[a] *School of Computing and Information Technology*
Monash University
Frankston, Melbourne, VIC 3199, AUSTRALIA
Email: yuliang@pscit.monash.edu.au

[b] *School of Information Technology & Computer Science*
The University of Wollongong
Wollongong, NSW 2522, AUSTRALIA
xianmo@cs.uow.edu.au

[c] *Institute of Industrial Science*
The University of Tokyo
7-22-1 Roppongi, Minato-ku, Tokyo 106-8558, JAPAN
Email: imai@iis.u-tokyo.ac.jp

Abstract

Nonlinear characteristics of (Boolean) functions is one of the important issues both in the design and cryptanalysis of (private key) ciphers or encryption algorithms. This paper studies nonlinear properties of functions from three different but closely related perspectives: maximal odd weighting subspaces, restrictions to cosets, and hypergraphs, all associated with a function. Main contributions of this work include (1) by using a duality property of a function, we have obtained several results that are related to lower bounds on nonlinearity as well as on the number of terms, of the function, (2) we show that the restriction of a function on a coset has a significant impact on cryptographic properties of the function, (3) we identify relationships between the nonlinearity of a function and the distribution of terms in the algebraic normal form of the function, (4) we prove that cycles of odd length in the terms, as well as quadratic terms, in the algebraic normal form of a function play an important role in determining the nonlinearity of the function. We hope that these results contribute to the study of new cryptanalytic attacks on ciphers, and more importantly, of counter-measures against such attacks.

Key words: Boolean Function, Cryptography, Hypergraph, Nonlinearity, Algebraic Normal Form.

1 Motivation of this Research

In his pioneering work on the theory of secrecy systems [10], Shannon suggested the concept of a "product cipher" which employs a concatenation of several different types of basic transformations. Most modern ciphers, including the Data Encryption Standard or DES [7], have been designed by following Shannon's suggestion.

A core component of these ciphers is the so-called substitution boxes or S-boxes each of which is mathematically identical to a tuple of nonlinear (Boolean) functions on $GF(2)$. Recent progress in cryptanalysis, especially the discovery of linear attacks [5], has highlighted the significance of research into nonlinear characteristics of functions. Well-known indicators that forecast nonlinear characteristics of a function include nonlinearity (or the minimum distance to the affine functions), avalanche effect, algebraic degree, resilience, and correlation immunity to mention a few. While some indicators, such as nonlinearity and avalanche effect, have received extensive studies, many others are yet to be addressed.

Study of these indicators may lead to the discovery of new cryptanalytic attacks, and more importantly, shed light on the design of new ciphers that are secure against an even wider range of possible cryptanalytic attacks.

This paper studies nonlinear properties of functions from three different but closely related perspectives: maximal odd weighting subspaces, restrictions to cosets, and hypergraphs, all associated with a function. Main contributions of this work include (1) by using a duality property of a function, we have obtained several results that are related to lower bounds on nonlinear, as well as on the number of terms, of the function, (2) we identify relationships between the nonlinearity of a function and the distribution of terms in the algebraic normal form of the function, (3) we prove that cycles of odd length in the terms, as well as quadratic terms, in the algebraic normal form of a function play an important role in determining the nonlinearity of the function.

The remainder of this paper is organized as follows. Section 2 presents basic mathematical background, especially duality properties of a function, which is needed in the understanding of results to be presented in other parts of the paper. Section 3 studies maximal odd weighting subspaces and their applications in determining the nonlinearity and the number of terms of a function. This is followed by Section 4 where we investigate how the restriction of a function to a coset is connected to the nonlinearity of the original function. In Section 5, we study nonlinearity properties of a function by the use of graph theory. We show that each function corresponds to a unique hypergraph, which allows us to prove a few bounds on the nonlinearity of the function. The paper is closed by a few remarks in Section 6.

Part of the results presented in this paper were reported at the 1997 International Conference on Information and Communications Security (ICICS'97), Beijing, and the 1998 IEEE International Symposium on Information Theory (ISIT'98), Boston.

2 Preliminaries

We consider 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 $((-1)^{f(\alpha_0)},\ (-1)^{f(\alpha_1)},\ \ldots,\ (-1)^{f(\alpha_{2^n-1})})$, where $\alpha_0 = (0,\ldots,0,0)$, $\alpha_1 = (0,\ldots,0,1)$, ..., $\alpha_{2^{n-1}-1} = (1,\ldots,1,1)$. The *matrix* of f is a $(1,-1)$-matrix of order 2^n defined by $M = ((-1)^{f(\alpha_i\oplus\alpha_j)})$ where $\oplus$ denotes the addition in $GF(2)$. 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 $\tilde{a} * \tilde{b} = (a_1b_1,\cdots,a_mb_m)$. 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, $\langle\tilde{a},\tilde{b}\rangle = a_1b_1 \oplus \cdots \oplus a_mb_m$, where the addition and multiplication are over $GF(2)$, and when $\tilde{a}$ and $\tilde{b}$ are $(1,-1)$-sequences, $\langle\tilde{a},\tilde{b}\rangle = \sum_{i=1}^{m} a_ib_i$, 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

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

Let ℓ_i, $0 \le i \le 2^n-1$, be the i row of H_n. By Lemma 2 of [9], 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 alphabetical order.

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

Definition 1 *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 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.*

The following characterization of nonlinearity will be used in this paper (for a proof see for instance [6,9].)

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

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 linear functions on V_n.

Notation 2 $(b_1, \dots, b_n) \preceq (a_1, \dots, a_n)$ means that $(b_1, \dots, b_n)$ is covered by $(a_1, \dots, a_n)$, namely if $b_j = 1$ then $a_j = 1$. In addition, $(b_1, \dots, b_n) \prec (a_1, \dots, a_n)$ means that $(b_1, \dots, b_n)$ is properly covered by $(a_1, \dots, a_n)$, namely $(b_1, \dots, b_n) \preceq (a_1, \dots, a_n)$ and $(b_1, \dots, b_n) \neq (a_1, \dots, a_n)$.

Definition 3 *A function f on V_n can be uniquely represented by a polynomial on $GF(2)$ whose degree is at most n. Namely,*

$$f(x_1, \dots, x_n) = \bigoplus_{\alpha \in V_n} g(a_1, \dots, a_n) x_1^{a_1} \cdots x_n^{a_n} \tag{2}$$

where $\alpha = (a_1, \dots, a_n)$, and g is also a function on V_n. The polynomial representation of f is called the algebraic normal form *of the function and each $x_1^{a_1} \cdots x_n^{a_n}$ is called a* term *in the algebraic normal form of f. The* algebraic degree*, or simply* degree*, of f, denoted by $deg(f)$, is defined as the number of variables in the longest term of f, i.e.,*

$$deg(f) = \max\{\textit{the Hamming weight of } (a_1, \dots, a_n) \mid g(a_1, \dots, a_n) = 1\}.$$

The function g defined in the algebraic normal form (2) is called the Möbius transform *of f.*

Notation 4 Let W be a subspace of V_n. Denote the dimension of W by $dim(W)$.

Notation 5 Let X be a set. The cardinal number of X, i.e., the number of elements in X, is denoted by $\#X$.

A proof for the following result is provided, as we feel that understanding the proof would be helpful in studying other issues that are more directly related to cryptography.

Theorem 6 *Let f be a function on V_n. Let $\alpha, \beta \in V_n$ $\alpha = (1, \ldots, 1, 0, \ldots, 0)$ where only the first s components are one, and $\beta = (0, \ldots, 0, 1, \ldots, 1, 0, \ldots, 0)$ where only the $(s+1)$th, ..., the $(s+t)$th components are one. Then the number of terms of the form $x_1 \cdots x_s x_{i_1} \cdots x_{i_{t'}}$ where $s+1 \leq i_1 < \cdots < i_{t'} \leq s+t$, that appear in the algebraic normal form of f, is even if $\bigoplus_{\gamma \preceq \alpha} f(\gamma \oplus \beta) = 0$, and the number is odd if $\bigoplus_{\gamma \preceq \alpha} f(\gamma \oplus \beta) = 1$.*

PROOF. Consider a term

$$\chi(x) = x_{j_1} \cdots x_{j_{s'}} x_{i_1} \cdots x_{i_{t'}} \tag{3}$$

in f, where $x = (x_1, \ldots, x_n)$, $1 \leq j_1 < \cdots < j_{s'} \leq s$ and $s+1 \leq i_1 < \cdots < i_{t'} \leq s+t$. For $s' < s$, there are an even number of vectors γ in V_n such that $\gamma \preceq \alpha$ and $\chi(\gamma \oplus \beta) = 1$. Hence

$$\bigoplus_{\gamma \preceq \alpha} \chi(\gamma \oplus \beta) = 0. \tag{4}$$

For $s' = s$, there is only one vector in V_n, $\gamma = \alpha$, such that $\chi(\gamma \oplus \beta) = 1$. Hence

$$\bigoplus_{\gamma \preceq \alpha} \chi(\gamma \oplus \beta) = 1. \tag{5}$$

Now consider a term

$$\omega(x) = x_{j_1} \cdots x_{j_k} \tag{6}$$

in f, where $x = (x_1, \ldots, x_n)$, $1 \leq j_1 < \cdots < j_k$, and $j_k > s+t$. From (6) with $j_k > s+t$, and the structures of α and β,

$$\omega(\gamma \oplus \beta) = 0 \tag{7}$$

for each $\gamma \preceq \alpha$. Denote the set of terms given in (3) by Γ_1 if $s' < s$, and by Γ_2 if $s' = s$. And denote the set of terms given in (6) by Ω. Then we can write f

as

$$f = \bigoplus_{\chi \in \Gamma_1} \chi \oplus \bigoplus_{\chi \in \Gamma_2} \chi \oplus \bigoplus_{\omega \in \Omega} \omega.$$

From (4), (5) and (7), we have

$$\bigoplus_{\gamma \preceq \alpha} f(\gamma \oplus \beta) = \bigoplus_{\gamma \preceq \alpha} \bigoplus_{\chi \in \Gamma_2} \chi(\gamma \oplus \beta). \tag{8}$$

The proof is completed by noting that $\bigoplus_{\gamma \preceq \alpha} f(\gamma \oplus \beta) = 0$ implies that $\#\Gamma_2$ is even, while $\bigoplus_{\gamma \preceq \alpha} f(\gamma \oplus \beta) = 1$ implies that $\#\Gamma_2$ is odd.

Set $\beta = 0$ in Theorem 6 and reorder the variables, we obtain a result well known to coding theorists (see p.372 of [4]):

Corollary 7 *Let f be a function on V_n and $\alpha = (a_1, \ldots, a_n)$ be a vector in V_n. Then the term $x_1^{a_1} \cdots x_n^{a_n}$ appears in f if and only if $\bigoplus_{\gamma \preceq \alpha} f(\gamma) = 1$.*

With the above two results, it is not hard to verify the correctness of the following lemma:

Lemma 8 *Let f and g be function on V_n. Then the following four statements are equivalent*

(i) $f(\alpha) = \bigoplus_{\beta \preceq \alpha} g(\beta)$ *for every vector* $\alpha \in V_n$,
(ii) $g(\alpha) = \bigoplus_{\beta \preceq \alpha} f(\beta)$ *for every vector* $\alpha \in V_n$,
(iii) $f(x_1, \ldots, x_n) = \bigoplus_{\alpha \in V_n} g(a_1, \ldots, a_n) x_1^{a_1} \cdots x_n^{a_n}$ *where* $\alpha = (a_1, \ldots, a_n)$,
(iv) $g(x_1, \ldots, x_n) = \bigoplus_{\alpha \in V_n} f(a_1, \ldots, a_n) x_1^{a_1} \cdots x_n^{a_n}$ *where* $\alpha = (a_1, \ldots, a_n)$.

3 Maximal Odd Weighting Subspaces with Applications

The focus of this section is on maximal odd weighting subspace to be defined in the following. We show the usefulness of this simple concept by proving two interesting results, one is on a lower bound on the nonlinearity of a function, and the other is on a lower bound on the number of terms in the algebraic normal form of a function.

Definition 9 *Let f be a function on V_n and W be an s-dimensional subspace of V_n. The* restriction *of f to W, denoted by f_W, is a function on W defined by $f_W(\alpha) = f(\alpha)$ for every $\alpha \in W$.*

Definition 10 *Let f be a function on V_n. A subspace U of V_n is called a maximal odd weighting subspace of f if the Hamming weight of f_U is odd, while the Hamming weight of $f_{U'}$ is even for every subspace U' of V_n with $U' \supset U$.*

A maximal odd weighting subspace of a function is not necessarily a subspace with the maximum dimension, even if the Hamming weight of the restrictions of f to the subspace is odd. This is best explained with the following example.

Example 11 *Let $f(x_1, x_2, x_3, x_4) = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_3x_4 \oplus x_3$ be a function on V_4, whose truth table is* 0010001000100100. *The eight vectors* (0000), (0001), (0100), (0101), (1000), (1001), (1100) *and* (1101) *form a* 3*-dimensional subspace, say W, such that the Hamming weight of f_W, is one (odd), where f_W is defined in Definition 9. Since f has an even Hamming weight, the* 3*-dimensional subspace W is a maximal odd weighting subspace of f. However, the four vectors* (0000), (0001), (0010) *and* (0011) *form a* 2*-dimensional subspace, say U, such that the Hamming weight of f_W is one (odd). There are three* 3*-dimensional subspaces containing U:*

$$\begin{aligned} U' &= \{(0000), (0001), (0010), (0011), (0100), (0101), (0110), (0111)\} \\ U'' &= \{(0000), (0001), (0010), (0011), (1000), (1001), (1010), (1011)\} \\ U''' &= \{(0000), (0001), (0010), (0011), (1100), (1101), (1110), (1111)\} \end{aligned}$$

We note that the Hamming weights of $f_{U'}$, $f_{U''}$ and $f_{U'''}$ are all two (even). We also note that the 4*-dimensional subspace containing U is V_4 itself and the Hamming weight of f is four (even). Hence both W and U are maximal odd weighting subspaces of f.*

As will be shown in the forthcoming subsections, the concept of maximal odd weighting subspace of a function plays an important role, primarily due to the fact that the dimension of a subspace is relevant to the structure of the function.

3.1 A Lower Bound on Nonlinearity

In this subsection we show how the dimension of a maximal odd weighting subspace of a function is connected to the lower bound on the nonlinearity of the function.

Definition 12 *Let f be a function on V_n, $x_{j_1} \cdots x_{j_t}$ and $x_{i_1} \cdots x_{i_s}$ be two terms in the algebra normal form of function f. $x_{j_1} \cdots x_{j_t}$ is said to be* covered *by $x_{i_1} \cdots x_{i_s}$ if $\{j_1, \ldots, j_t\}$ is a subset of $\{i_1, \ldots i_s\}$, and $x_{j_1} \cdots x_{j_t}$ is said to be* properly covered *by $x_{i_1} \cdots x_{i_s}$ if $\{j_1, \ldots, j_t\}$ is a proper subset of $\{i_1, \ldots i_s\}$.*

Theorem 13 *Let f be a function on V_n and U be a maximal odd weighting subspace of f. If $dim(U) = s$ then the Hamming weight of f is at least 2^{n-s}.*

PROOF. Let U be an s-dimensional subspace of V_n. Then V_n is the union of 2^{n-s} disjoint *cosets* of U

$$V_n = \Pi_0 \cup \Pi_1 \cup \cdots \cup \Pi_{2^{n-s}-1} \tag{9}$$

where

(i) $\Pi_0 = U$,
(ii) for any $\alpha, \beta \in V_n$, α, β belong to the same class, say Π_j, if and only if $\alpha \oplus \beta \in \Pi_0 = U$. From (i) and (ii), it follows that
(iii) $\Pi_j \cap \Pi_i = \emptyset$ for $j \neq i$, where $\emptyset$ denotes the empty set.

Note that each Π_j can be expressed as $\Pi_j = \beta_j \oplus U$ for a $\beta_j \in V_n$, where $\beta_j \oplus U = \{\beta_j \oplus \alpha | \alpha \in U\}$. And let $N_j = \#\{\alpha | \alpha \in \Pi_j,\ f(\alpha) = 1\}$, where Π_j is defined in (9), $j = 0, 1, \ldots, 2^{s-1}$. Since $\Pi_0 = U$, N_0 is odd. Note that $\Pi_0 \cup \Pi_j$ is a $(s+1)$-dimensional subspace of V_n, $j = 1, \ldots, 2^{n-s} - 1$.

Since $\Pi_0 = U$ is a maximal odd weighting subspace of f, the Hamming weight of the restriction of f to $\Pi_0 \cup \Pi_j$ is even. In other words, $N_0 + N_j$ is even. This proves that each N_j is odd, $j = 1, \ldots, 2^{n-s}-1$. Hence $N_0 + N_1 + \cdots + N_{2^{n-s}-1} \geq 2^{n-s}$, namely, the Hamming weight of f is at least 2^{n-s}.

Theorem 14 *Let f be a function on V_n and U be a maximal odd weighting subspace of f. Let $dim(U) = s$ ($s \geq 2$). Then the nonlinearity N_f of f satisfies $N_f \geq 2^{n-s}$.*

PROOF. Let φ be any affine function on V_n. Let W be any subspace of dimension at least two. Note that the Hamming weight of φ_W is even. Hence the Hamming weight of $(f \oplus \varphi)_W$ is odd if and only if the Hamming weight of f_W is odd. This proves that U is also a maximal odd weighting subspace of $f \oplus \varphi$. According to Theorem 13, the Hamming weight of $f \oplus \varphi$ is at least 2^{n-s}. As the Hamming weight of $f \oplus \varphi$ determines $d(f, \varphi)$, the theorem is proved.

Theorem 15 *Let $t \geq 2$. If $x_{j_1} \cdots x_{j_t}$ is a term in a function f on V_n and it is not properly covered (see Definition 12) by any other term in the same function, then the nonlinearity N_f of f satisfies $N_f \geq 2^{n-t}$.*

PROOF. Write $\alpha = (a_1, \ldots, a_n)$ where $a_j = 1$ for $j \in \{j_1, \ldots, j_t\}$ and $a_j = 0$ for $j \notin \{j_1, \ldots, j_t\}$. Set

$$U = \{\gamma |\ \gamma \preceq \alpha\}.$$

Obviously U is a t-dimensional subspace of V_n. Since $x_{j_1} \cdots x_{j_t}$ is a term in f on V_n, by using Corollary 7, $\bigoplus_{\gamma \preceq \alpha} f(\gamma) = 1$ or $\bigoplus_{\gamma \in U} f(\gamma) = 1$, i.e., the Hamming weight of f_U is odd.

We now prove that U is a maximal odd weighting subspace of f. Assume that U is not a maximal odd weighting subspace of f. Then there is an s-dimensional subspace of V_n, say W, such that U is a proper subset of W, i.e., $s > t$ and the Hamming weight of f_W is odd ($\bigoplus_{\gamma \in W} f(\gamma) = 1$). Since U is a proper subspace of W, we can express W as a union of 2^{s-t} disjoint cosets of U

$$W = U \cup (\beta_1 \oplus U) \cup \cdots \cup (\beta_{2^{s-t}-1} \oplus U) \tag{10}$$

where each $\beta \preceq \overline{\alpha}$, and $\overline{\alpha} \oplus \alpha = (1, \ldots, 1)$. Since both the Hamming weights of f_U and f_W are odd, there is a coset, say $\beta_k \oplus U$, $1 \leq k \leq 2^{s-t} - 1$, such that the Hamming weight of $f_{\beta_k \oplus U}$ is even, i.e.,

$$\bigoplus_{\gamma \preceq \alpha} f(\beta_k \oplus \gamma) = 0. \tag{11}$$

Applying Theorem 6 to (11), there are an even number of terms covering $x_{j_1} \cdots x_{j_t}$. Since the term $x_{j_1} \cdots x_{j_t}$ itself appears in f, there is another term properly covering $x_{j_1} \cdots x_{j_t}$. This contradicts the condition in the theorem, namely the term $x_{j_1} \cdots x_{j_t}$ is not properly covered by any other term in f. The contradiction indicates that U is a maximal odd weighting subspace of f. By noting Theorem 14, the proof is completed.

Example 16 *Let*

$$\begin{aligned} f(x_1, \ldots, x_{10}) = {} & x_1x_2x_3x_4x_5x_6x_7 \oplus x_3x_4x_5x_6x_7x_8x_9 \oplus x_7x_8x_9x_{10} \oplus \\ & x_4x_6x_8x_{10} \oplus x_1x_5x_9 \oplus x_2x_4 \oplus x_6 \end{aligned}$$

be a function on V_{10}. *The term* $x_1x_5x_9$ *is not properly covered by any other term in* f. *By using Corollary 15, the nonlinearity* N_f *of* f *satisfies* $N_f \geq 2^{10-3} = 2^7$.

Example 17 *Let*

$$\begin{aligned} f(x_1, \ldots, x_{10}) = {} & x_1x_2x_3x_4x_5x_6x_7 \oplus x_3x_4x_5x_6x_7x_8x_9 \oplus x_7x_8x_9x_{10} \oplus \\ & x_4x_6x_8x_{10} \oplus x_1x_3x_5 \oplus x_2x_8 \oplus x_1 \oplus x_2 \end{aligned}$$

be a function on V_{10}. The term x_2x_8 is not properly covered by any other term in f. Thus, the nonlinearity N_f of f satisfies $N_f \geq 2^{10-2} = 2^8$.

We note that the lower bound in Theorem 14 is tight:

Corollary 18 *For any n and any s with $2 \leq s \leq n$, there is a function on V_n, say f, together with an s-dimensional subspace, say U, such that U is a maximal odd weighting subspace of f and the nonlinearity N_f of f satisfies $N_f = 2^{n-s}$.*

PROOF. Let g be a function on V_s, defined as $g(\beta) = 1$ if and only if $\beta = 0$. Set $f(z, y) = g(y)$, a function on V_n, where $z \in V_{n-s}$ and $y \in V_s$. Since the Hamming weight of f is 2^{n-s} ($s \geq 2$), $d(f, h) \geq 2^{n-s}$ where h is any affine function on V_n and the equality holds if h is the zero function on V_n. Hence the nonlinearity N_f of f satisfies $N_f = 2^{n-s}$. On the other hand, set

$$U = \{(0, \ldots, 0, b_1, \ldots, b_s) | b_j \in GF(2)\}$$

where the number of zeros is $n - s$.

We now verify that the s-dimensional subspace U is a maximal odd weighting subspace of f. Let W be a k-dimensional subspace of V_n such that U is a prefer subspace of W. We can express W as a union of 2^{k-s} disjoint cosets of U

$$W = U \cup (\beta_1 \oplus U) \cup \cdots \cup (\beta_{2^{k-s}-1} \oplus U)$$

Since U is a subspace, we can choose each β_j as a vector of the form $(c_1, \ldots, c_{n-s}, 0, \ldots, 0)$. From the construction of f, the Hamming weight of $f_{\beta_j \oplus U}$ is odd (one). Hence the Hamming weight of f_W is even. This proves that U is a maximal odd weighting subspace of f.

Finally we note that Theorem 14 cannot be further improved by extending s to $s = 1$, as the condition of $s \geq 2$ in the proof of the theorem cannot be removed. For example, let f be a function on V_n, whose truth table is given as follows

$$0110011010011001.$$

It is easy to verify that (0000) and (0001) form a maximal 1-dimensional subspace, denoted by U. Theorem 14 is not applicable due to the fact that

$dim(U) = 1$. In fact, f is a linear function, hence its nonlinearity is 0. Nevertheless, Theorem 13 can be applied, which tells us that the Hamming weight of f must be at least $2^{4-1} = 8$.

3.2 A Lower Bound on the Number of Terms

In the design of a cipher, a designer generally prefers a function that has a large number of terms in its algebraic normal form to one that has few, although the former may require more circuitry than the latter in hardware implementation. A good example is S-boxes employed in DES all of which appear to contain a large number of terms. In what follows we show that maximal odd weighting subspaces can be used in bounding from below the number of terms of a function.

Theorem 19 *Let f be a function on V_n such that $f(\alpha) = 1$ for a vector $\alpha \in V_n$, and $f(\beta) = 0$ for every vector β with $\alpha \prec \beta$, where $\prec$ is defined as in Notation 2. Then f has at least 2^{n-t} terms, where t denotes the Hamming weight of α.*

PROOF. First we note that Theorem 13 can be equivalently stated as follows:

Let f be a function on V_n and g be the Möbius transform of f defined in (2). Let $g(\alpha) = 1$ for a vector $\alpha \in V_n$, and $g(\beta) = 0$ for every vector β with $\alpha \prec \beta$, where $\prec$ is defined in Notation 2. Then the Hamming weight of f is at least 2^{n-t}.

The equivalence between (iii) and (iv) in Lemma 8 allows us to interchange f and g in the above statement. Thus we have:

Let f be a function on V_n and g be defined in (2). Let $f(\alpha) = 1$ for a vector $\alpha \in V_n$, and $f(\beta) = 0$ for every vector β with $\alpha \prec \beta$. Then the Hamming weight of g is at least 2^{n-t}. This completes the proof.

Applying Theorem 19, it is not hard to verify

Corollary 20 *Let f be a function on V_n such that $f(\alpha) = 0$ for a vector $\alpha \in V_n$, and $f(\beta) = 1$ for every vector β with $\alpha \prec \beta$, where $\prec$ is defined as in Notation 2. Then f has at least*

(i) $2^{n-s} - 1$ *terms if* $f(0) = 0$,
(ii) $2^{n-s} + 1$ *terms if* $f(0) = 1$,

where s denotes the Hamming weight of α.

Example 21 *Let f be a function on V_6, whose truth table is given as follows*

$$1000110111110010001101001100100001111100011001101001011010001010$$

Note that the value of $f(001011)$ is one, while the values of $f(001111)$, $f(011011)$, $f(011111)$, $f(101011)$, $f(101111)$, $f(111011)$ and $f(111111)$ are all zero. Applying Theorem 19 to the vector (001011), we conclude that f has at least $2^{6-3} = 8$ terms.

Example 22 *Let f be a function on V_6, whose truth table is given as follows*

$$1000110111110011001101011101100101111010111011110010111110011010$$

Note that $f(000011)$ assumes the value zero, while $f(000111)$, $f(001011)$, $f(001111)$, $f(010011)$, $f(010111)$, $f(011011)$, $f(011111)$, $f(100011)$, $f(100111)$, $f(101011)$, $f(101111)$, $f(110011)$, $f(110111)$, $f(111011)$ and $f(111111)$ all assume the value one. Applying (ii) of Corollary 20 to the vector (000011), we can see that f has at least $2^{6-2} + 1 = 17$ terms.

The lower bounds on the number of terms given by Theorem 19 and Corollary 20 are tight, due to Corollary 18 and Lemma 8.

4 Restrictions of a Function

Restricting a function is another approach that can be used in studying the properties of the function. In this section we investigate restriction of a function to a coset which is a set of vectors induced by a subspace. We show a relationship between the nonlinearity of a function and that of the restriction of the function to a coset. Using this relationship we further obtain a number of results that relate nonlinearity to the number of terms in the algebraic normal form of the function. First we introduce the following lemma which is a special case of Lemma 3 in [1] with $G = V_n$, $r = 2$ and $k = n$.

Lemma 23 *Let f be a function on V_n ($n \geq 2$). If f satisfies the property that for every $(n-1)$-dimensional subspace, say W, the Hamming weight of f_W is even, where f_W is defined in Definition 9, then the Hamming weight of f is also even.*

The next definition is more general than Definition 9

Definition 24 *Let f be a function on V_n and U be an s-dimensional subspace of V_n. The* restriction *of f to a coset $\Pi_j = \beta_j \oplus U$, $j = 0, 1, \ldots, 2^{n-s} - 1$, denoted by f_{Π_j}, is a function on U, and it is defined by $f_{\Pi_j}(\alpha) = f(\beta_j \oplus \alpha)$ for every $\alpha \in U$.*

4.1 Nonlinearity of the Restriction of a Function to a Coset

Theorem 25 *Let f be a function on V_n, W be a p-dimensional subspace of V_n and Π be a coset of W. Then*

$$\max\{|\langle\gamma, e_j\rangle|, 0 \le j \le 2^p - 1\} \le \max\{|\langle\xi, \ell_j\rangle|, 0 \le j \le 2^n - 1\}$$

where γ is the sequence of f_Π, ξ is the sequence of f, e_j is the jth row of the 2^pth order Sylvester-Hadamard matrix H_p, ℓ_i is the ith row of the 2^nth order Sylvester-Hadamard matrix H_n, and ξ_i is the sequence of f.

PROOF. We first prove the theorem for the case of $\Pi = W$. Set $q = n - p$. We now prove the theorem by induction on q. When $q = 0$, the theorem is obviously true. Now assume that the theorem is true for $0 \le q \le k - 1$. Consider the case when $q = k$. Let U be an $(n-1)$-dimensional subspace of V_n such that W is a subspace of U. Let l_i denote the ith row of the 2^{n-1}th order Sylvester-Hadamard matrix H_{n-1}. Also let η to denote the sequence of f_U. Now applying the same assumption to W and U, we have

$$\max\{|\langle\gamma, e_j\rangle|, 0 \le j \le 2^p - 1\} \le \max\{|\langle\eta, l_j\rangle|, 0 \le j \le 2^{n-1} - 1\}$$

Again, by using the assumption,

$$\max\{|\langle\eta, l_j\rangle|, 0 \le j \le 2^{n-1} - 1\} \le \max\{|\langle\xi, \ell_j\rangle|, 0 \le j \le 2^n - 1\}$$

The proof for the particular case of $\Pi = W$ is done. To complete the proof for the theorem, we note that the above discussions also hold for a function g satisfying $f(x) = g(x \oplus \alpha)$, where α is any fixed vector in V_n.

Applying the above theorem, we obtain the following two interesting results:

Corollary 26 *Let f be a function on V_n, W be a p-dimensional subspace of V_n, Π be a coset of W, and f_Π be the restriction of f to Π. Then the nonlinearity of f and the nonlinearity of f_Π are related by*

$$N_f - N_{f_\Pi} \le 2^{n-1} - 2^{p-1}.$$

Corollary 27 *Let f be a function on V_n, W be a p-dimensional subspace of V_n, and Π be a coset of W. If the restriction of f to Π, f_Π, is an affine function, then the nonlinearity N_f of f satisfies*

$$N_f \leq 2^{n-1} - 2^{p-1}.$$

4.2 Relating Nonlinearity to Terms in Algebraic Normal Form

The following result is an application of Corollary 27.

Theorem 28 *Let f be a function on V_n and J be a subset of $\{1, \ldots, n\}$ such that f does not contain any term $x_{j_1} \cdots x_{j_t}$ where $j_1, \ldots, j_t \in J$. Then the nonlinearity N_f of f satisfies*

$$N_f \leq 2^{n-1} - 2^{s-1}$$

where $s = \#J$.

PROOF. Let $U = \{(a_1, \ldots, a_n) | a_j = 0 \text{ if } j \notin J\}$. Note that U is an s-dimensional subspace of V_n. Write

$$f(x_1, \ldots, x_n) = \bigoplus_{\alpha \in V_n} g(a_1, \ldots, a_n) x_1^{a_1} \cdots x_n^{a_n}$$

where $\alpha = (a_1, \ldots, a_n)$ and g is also a function on V_n. From the property of f and J, we have $g(\alpha) = 0$ for all $\alpha \in U$. By using Lemma 8, $f(\alpha) = \bigoplus_{\beta \preceq \alpha} g(\beta)$. Hence $f(\alpha) = 0$ for all $\alpha \in U$. That is, $f_U = 0$. By using Corollary 27, we have proved that $N_f \leq 2^{n-1} - 2^{s-1}$.

Example 29 *Consider a function on V_6, $f = x_1 \oplus x_3x_4 \oplus x_1x_2x_3 \oplus x_2x_3x_4 \oplus x_3x_4x_5 \oplus x_4x_5x_6$. $J = \{2, 3, 5, 6\}$ satisfies the condition mentioned in Theorem 28. Hence $N_f \leq 2^5 - 2^3 = 24$. Note that the nonlinearity of a function on V_6 is upper bounded by $2^5 - 2^2 = 28$.*

The following statement can be viewed as an improvement on Theorem 28.

Theorem 30 *Let f be a function on V_n and J be a subset of $\{1, \ldots, n\}$ such that f does not contain any term $x_{j_1} \cdots x_{j_t}$ where $t > 1$ and $j_1, \ldots, j_t \in J$. Then the nonlinearity N_f of f satisfies*

$$N_f \leq 2^{n-1} - 2^{s-1}$$

where $s = \#J$.

PROOF. Write $f = f^* \oplus \psi$ where ψ is an affine function and f^* has no affine term. Note that $N_{f^*} = N_f$. By Theorem 28, we have $N_{f^*} \le 2^{n-1} - 2^{s-1}$.

Example 31 *Consider a function on* V_{10},

$$f(x_1,\dots,x_{10}) = x_1x_2x_3x_4x_5x_6x_7 \oplus x_2x_3x_4x_5x_6x_7x_8 \oplus x_6x_7x_8x_9 \oplus x_7x_8x_9x_{10} \oplus x_2x_3x_{10} \oplus x_4x_8 \oplus x_1 \oplus x_3.$$

$J = \{1,3,4,5,6,7,9,10\}$ *satisfies the condition mentioned in Theorem 30. Hence* $N_f \le 2^9 - 2^7 = 384$*. Note that the nonlinearity of a function on* V_{10} *is upper bounded by* $2^9 - 2^4 = 496$*.*

The next two statements can be obtained from Theorems 28 and 30 respectively, by setting $J = \{1,\dots,n\} - P$.

- **Statement 1**: Let f be a function on V_n and P be a subset of $\{1,\dots,n\}$ such that for any term $x_{j_1}\cdots x_{j_t}$ in f, $\{j_1,\dots,j_t\} \cap P \neq \emptyset$ holds, where $\emptyset$ denotes the empty set. Then the nonlinearity N_f of f satisfies

  $$N_f \le 2^{n-1} - 2^{n-p-1}$$

  where $p = \#P$.
- **Statement 2**: Let f be a function on V_n and P be a subset of $\{1,\dots,n\}$ such that for any term $x_{j_1}\cdots x_{j_t}$ with $t > 1$ in f, $\{j_1,\dots,j_t\} \cap P \neq \emptyset$ holds, where $\emptyset$ denotes the empty set. Then the nonlinearity N_f of f satisfies

  $$N_f \le 2^{n-1} - 2^{n-p-1}$$

  where $p = \#P$.

Note that bent functions on V_n have nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$. By using Theorem 30 we conclude

Corollary 32 *Let f be a function on V_n satisfying $N_f \ge 2^{n-1} - 2^{s-1}$. Then f contains at least $n - s$ non-affine terms. In particular, if f is bent, then it contains at least $\frac{1}{2}n$ non-affine terms.*

PROOF. Let f contain exactly q non-affine terms. Suppose that $q < n - s$. From each non-affine term, we choose arbitrarily a single variable and collect those single variables together to form a set P. Obviously P satisfies the condition in Statement 2 and $\#P \le q$. Hence we have $N_f \le 2^{n-1} - 2^{n-\#P-1} \le 2^{n-1} - 2^{n-q-1} < 2^{n-1} - 2^{s-1}$. This contradicts the condition that $N_f \ge 2^{n-1} - 2^{s-1}$.

5 Hypergraph of a Boolean Function

5.1 König Property

Let $X = \{x_1, \ldots, x_n\}$ be a finite set. Set $\Im = \{E_1, \ldots, E_m\}$, where each E_j is a subset of X. The *hypergraph*, denoted by Γ, is the pair $\Gamma = (X, \Im)$.

Each x_j is called a *vertex*, each E_j is called an *edge*, n and m are called the *order* and the *size* of Γ respectively. If $\#E_j = 1$ for a j then the vertex in E_j is called an *isolated vertex*.

A sequence $x_1E_1x_2E_2 \cdots x_pE_px_1$ is called a *cycle* of length p, where $p > 1$, all the E_j and x_j, $1 \leq j \leq p$, are distinct, and $x_j, x_{j+1} \in E_j$, $j = 1, \ldots, p$.

A subset of X, say S, is a *stable set* of Γ, if $E_j \not\subseteq S$, $j = 1, \ldots, m$. The maximum cardinality of a stable set is called the *stability number* of Γ, denoted by $\kappa(\Gamma)$.

A subset of X, say Y, is a *transversal* of Γ, if $Y \cap E_j \neq \emptyset$, $j = 1, \ldots, m$. The minimum cardinality of a transversal is called the *transversal number* of Γ, denoted by $\tau(\Gamma)$.

A subset of $\Im$, say $B = \{E_{j_1}, \ldots, E_{j_q}\}$, is a *matching* of Γ, if $E_{j_t} \cap E_{j_s} = \emptyset$, for $t \neq s$. The maximum number of edges in a matching is called the *matching number* of Γ, denoted by $\nu(\Gamma)$.

The following equality and inequality can be found on Page 405 of [3]:

$$\tau(\Gamma) + \kappa(\Gamma) = n \tag{12}$$

and

$$\nu(\Gamma) \leq \tau(\Gamma). \tag{13}$$

Γ is said to satisfy the *König Property* if the equality in (13) holds. The following lemma can be deduced from Theorem 3.5 of [3], established by Berge and Las Vergnas in 1970.

Lemma 33 *If a hypergraph Γ has no cycle with odd length, then Γ satisfies the* König Property.

Definition 34 *For any function on V_n, say f, we can define the* hypergraph *of f, denoted by $\Gamma(f)$, by the following rule: Let $X = \{x_1, \ldots, x_n\}$. A subset of X, $E_j = \{x_{j_1}, \ldots, x_{j_t}\}$ is referred to as an edge of $\Gamma(f)$ if and only if $x_{j_1} \cdots x_{j_t}$*

is a term of f. Denote the stability number of $\Gamma(f)$ by $\kappa(f)$, transversal number of $\Gamma(f)$ by $\tau(f)$ and matching number of $\Gamma(f)$ by $\nu(f)$.

5.2 Applications to Nonlinearity

Corollary 35 *Let f be a function on V_n. Write $f = f^* \oplus \psi$, where ψ is an affine function and f^* has no affine term. Let $\kappa(f^*)$ denote the stability number of $\Gamma(f^*)$. Then*

$$N_f \leq 2^{n-1} - 2^{\kappa(f^*)-1}$$

or equivalently

$$\kappa(f^*) \leq 1 + log_2(2^{n-1} - N_f).$$

In particular, if f is a bent function, then $\kappa(f^*) \leq \frac{1}{2}n$ and $\tau(f^*) \geq \frac{1}{2}n$.

To prove the corollary, we note that $N_{f^*} = N_f$. Then applying Theorem 30, we have $N_{f^*} \leq 2^{n-1} - 2^{\kappa(f^*)-1}$.

Next we introduce a key result of this section.

Theorem 36 *Let f be a bent function on V_n. Then (the algebraic normal form of) f contains precisely $\frac{1}{2}n$ disjoint quadratic terms if $\Gamma(f)$ contains no cycle of odd length. Equivalently, $\Gamma(f)$ must contain a cycle of odd length if f contains less than $\frac{1}{2}n$ disjoint quadratic terms.*

PROOF. Write $f = f^* \oplus \psi$ where ψ is an affine function and f^* has no affine term. If $\Gamma(f)$ contains no cycle of odd length, then $\Gamma(f^*)$ too contains no cycle of odd length. By using Lemma 33, we have $\tau(f^*) = \nu(f^*)$. From Corollary 35, $\nu(f^*) \geq \frac{1}{2}n$. Hence there exists a matching B of $\Gamma(f^*)$. Without loss of generality, let $B = \{E_1, \dots, E_\nu\}$, where each E_j is an edge of $\Gamma(f^*)$, $\nu = \nu(f^*) = \tau(f^*) \geq \frac{1}{2}n$ and $E_j \cap E_i = \emptyset$, for $j \neq i$. Note that

$$\#E_1 + \cdots + \#E_\nu = \#(E_1 \cup \cdots \cup E_\nu) \leq n. \tag{14}$$

On the other hand, since $\Gamma(f^*)$ has no isolated vertex, each E_j has at least two elements. Hence

$$\#E_1 + \cdots + \#E_\nu \geq 2\nu \geq n. \tag{15}$$

Comparing (15) with (14), we have

$$\#E_1 + \cdots + \#E_\nu = n. \tag{16}$$

Note that (16) with $\nu \geq \frac{1}{2}n$ holds if and only if $\nu = \frac{1}{2}n$ and $\#E_j = 2$, $j = 1, \ldots, \nu = \frac{1}{2}n$. This proves that f^* contains $\frac{1}{2}n$ disjoint quadratic terms, and so does f.

Theorem 37 *Let f be a function on V_n, whose nonlinearity N_f satisfies*

$$N_f \geq 2^{n-1} - 2^{\frac{2}{3}n-t-1}$$

where t is real with $1 \leq t \leq \frac{1}{6}n$. Then f contains at least $3t$ disjoint quadratic terms if $\Gamma(f)$ contains no cycle of odd length. Equivalently, $\Gamma(f)$ contains at least one cycle of odd length if f contains less than $3t$ disjoint quadratic terms.

PROOF. Write $f = f^* \oplus \psi$ where ψ is an affine function and f^* has no affine term. If $\Gamma(f)$ contains no cycle of odd length, then $\Gamma(f^*)$ too contains no cycle of odd length. Recall that $N_f = N_{f^*}$. By using Lemma 33, $\tau(f^*) = \nu(f^*)$. From Corollary 35, $\nu(f^*) \geq n - (\frac{2}{3}n - t) = \frac{1}{3}n + t$. Hence there exists a matching B of $\Gamma(f^*)$. Again, without loss of generality, we can assume that $B = \{E_1, \ldots, E_\nu\}$, where each E_j is an edge of $\Gamma(f^*)$, $\nu = \nu(f^*) = \tau(f^*) \geq \frac{1}{3}n + t$ and $E_j \cap E_i = \emptyset$, for $j \neq i$.

Note that

$$\#E_1 + \cdots + \#E_\nu = \#(E_1 \cup \cdots \cup E_\nu) \leq n. \tag{17}$$

Let there be k sets E_j, where $E_j \subseteq B$ with $\#E_j = 2$. Then

$$\#(E_1 + \cdots + E_\nu) \geq 2k + 3(\nu - k) \geq 2k + 3(\frac{1}{3}n + t - k). \tag{18}$$

Comparing (17) and (18), we have $k \geq 3t$.

Corollary 38 *Let f be a function on V_n, whose nonlinearity N_f satisfies*

$$N_f > 2^{n-1} - 2^{\frac{2}{3}n-1}.$$

Then f contains at least one quadratic term if $\Gamma(f)$ contains no cycle of odd length. That is, $\Gamma(f)$ must contain a cycle of odd length if f contains no quadratic term.

PROOF. Since $N_f > 2^{n-1} - 2^{\frac{2}{3}n-1}$, there exists a real number t, $0 < t \leq \frac{1}{6}n$, such that $N_f \geq 2^{n-1} - 2^{\frac{2}{3}n-t-1} > 2^{n-1} - 2^{\frac{2}{3}n-1}$. By using Theorem 37, the proof is completed.

Theorems 36, 37 and Corollary 38 show that the existence of a cycle of odd length in Γ or of quadratic terms in f plays an important role in highly nonlinear functions.

It should be pointed out that the existence of $\frac{1}{2}n$ disjoint quadratic terms and the existence of a cycle of odd length in $\Gamma(f)$ are not mutually exclusive. This can be demonstrated by the following example.

Example 39 *It is known that there exist four types of bent functions on V_6 each of which is not equivalent to other three by any linear transformation on the variables [8]:*

(i) $f_1(x_1,\ldots,x_6) = x_1x_4 \oplus x_2x_5 \oplus x_3x_6$,
(ii) $f_2(x_1,\ldots,x_6) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$,
(iii) $f_3(x_1,\ldots,x_6) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5$,
(iv) $f_4(x_1,\ldots,x_6) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6$.

f_1 and f_2: Obviously, neither $\Gamma(f_1)$ nor $\Gamma(f_2)$ contains a cycle of odd length. Both f_1 and f_2 contain three disjoint quadratic terms: x_1x_4, x_2x_5, x_3x_6.

f_3: Let E_j be the jth term, $j = 1,\ldots,7$, where the order is from left to right in the algebraic normal form of f_3. $\Gamma(f_3)$ contains a cycle of length 5: $x_4E_7x_5E_6x_3E_1x_2E_3x_1E_4x_4$. In addition, f_3 contains three disjoint quadratic terms: x_1x_4, x_2x_6, x_3x_5.

f_4: Let E_j be the jth term, $j = 1,\ldots,10$, where the order is from the left to the right in the algebraic normal form of f_4. $\Gamma(f_4)$ contains a cycle of length 3: $x_3E_1x_2E_2x_4E_3x_3$. It also contains three disjoint quadratic terms: x_1x_4, x_2x_6, x_3x_5.

6 Future Work

Results in this paper show that maximal odd weight subspaces, restrictions to a coset, terms in the algebraic normal form and hypergraphs of a function are useful tools in the study of cryptographic properties, especially the nonlinearity, of the function. A possible future research topic is to investigate whether these tools can be used in the study of the algebraic degree of a function. Another topic is to explore these indicators in analyzing the security of ciphers used in the real world, and the design of functions that would strengthen a cipher against various attacks.

Acknowledgement

We would like to thank Claude Carlet for his many insightful comments that have helped improve the presentation of the paper.

References

[1] Claude Carlet, Two New Classes of Bent Functions, *Advances in Cryptology - EUROCRYPT'93*, (Springer-Verlag, Berlin, Heidelberg, New York, **765**, Lecture Notes in Computer Science, 1994), 77-101.

[2] , J. F. Dillon, A Survey of Bent Functions, *The NSA Technical Journal* (unclassified), (1972), 191-215.

[3] R. L. Graham and M. Grötschel and L. Lovász, *Handbook of Combinatorics* **I**, (Elsevier Science B. V., 1995).

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

[5] M. Matsui, Linear Cryptanalysis Method for DES Cipher, *Advances in Cryptology - EUROCRYPT'93*, (Springer-Verlag, Berlin, Heidelberg, New York, **765**, Lecture Notes in Computer Science, 1994), 386-397.

[6] W. Meier and O. Staffelbach, Nonlinearity Criteria For Cryptographic Functions, *Advances in Cryptology - EUROCRYPT'89*, (Springer-Verlag, Berlin, Heidelberg, New York, **434**, Lecture Notes in Computer Science, 1990), 549-562.

[7] National Bureau Standards, Data Encryption Standard, *Federal Information Processing Standards Publication FIPS PUB 46*, (U.S. Department of Commerce, 1977).

[8] O. S. Rothaus, On "Bent" Functions, *Journal of Combinatorial Theory*, **Ser. A, 20**, (1976), 300-305.

[9] J. Seberry and X. M. Zhang and Y. Zheng, Nonlinearity and Propagation Characteristics of Balanced Boolean Functions, *Information and Computation*, **119 (1)** (1995), 1-13.

[10] C. E. Shannon, Communications Theory of Secrecy System, *Bell Sys. Tech. Journal*, **28** (1949), 656-751.