On Balanced Nonlinear Boolean Functions [1]

Yuliang ZHENG [a] and Xian-Mo ZHANG [b]

[a] *Department of Software and Information Systems, UNC Charlotte, 9201 University City Blvd, Charlotte, NC 28223, USA; Email:* yzheng@uncc.edu.

[b] *Department of Computing, Macquarie University, Sydney, NSW 2109, Australia; Email:* xianmo@ics.mq.edu.au.

Abstract. This paper surveys techniques for studying and constructing balanced Boolean functions that exhibit desirable nonlinear properties including high nonlinearity, good avalanche characteristics and high orders of correlation immunity. Emphasis is placed on techniques that are of combinatorial nature, especially those that utilize extensively Hadamard matrices and hypergraphs.

Keywords. Avalanche, Balance, Bent Function, Boolean Function, Correlation immunity, Global Avalanche Characteristic (GAC), Nonlinearity, Nonlinear Order, Plateaued Function

1. Expressions of Boolean Functions

Let V_n be the vector space of n tuples of elements from $GF(2)$. We write vectors in $(GF(2))^n$ as $(0,\ldots,0,0) = \alpha_0$, $(0,\ldots,0,1) = \alpha_1$, …, $(1,\ldots,1,1) = \alpha_{2^n-1}$, and call α_i the *binary representation* of integer i, $i = 0,1,\ldots,2^n-1$. A Boolean function f is a mapping from V_n to $GF(2)$ or simply, a function f on V_n. We write f as $f(x)$ or $f(x_1,\ldots,x_n)$ where $x = (x_1,\ldots,x_n)$.

We can express a function in a truth table, a sequence, a matrix or algebraic normal form. Specifically, 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 $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$. 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 $GF(2)$. As there exist precisely 2^{2^n} functions on V_n and 2^{2^n} polynomials of degree n on $GF(2)$, each function on V_n can be uniquely expressed as a Boolean polynomial. More formally, we have the following definition:

Definition 1 *A function f on V_n can be uniquely represented by a polynomial on $GF(2)$ whose degree is at most n. Namely,*

$$f(x_1,\ldots,x_n) = \bigoplus_{\alpha\in V_n} g(a_1,\ldots,a_n)x_1^{a_1}\cdots x_n^{a_n} \tag{1}$$

[1] Invited talk at NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security, September 8-18, 2007, Holiday Hotel Universitetsky, Volkovo Village, Zvenigorod (Moscow region), Russia.

where $\alpha = (a_1, \ldots, a_n)$, and g is also a function on V_n. The polynomial representation of f is called the algebraic normal form *(ANF) 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.,*

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

The function g defined in the algebraic normal form (1) is called the Mӧbius transform *of f.*

Let $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$ be two sequences or vectors. When they are from V_m, the *scalar product* of $\tilde{a}$ and $\tilde{b}$, denoted by $\langle \tilde{a}, \tilde{b} \rangle$, is defined as $\langle \tilde{a}, \tilde{b} \rangle = a_1 b_1 \oplus \cdots \oplus a_m b_m$, where the addition and multiplication are over $GF(2)$. When $\tilde{a}$ and $\tilde{b}$ are $(1, -1)$-sequences, $\langle \tilde{a}, \tilde{b} \rangle = \sum_{i=1}^{m} a_i b_i$, where the addition and multiplication are over the reals. An *affine* function f on V_n is a function that takes the form of $f(x_1, \ldots, x_n) = a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$. The *Hamming weight* of a $(0, 1)$-sequence ξ, denoted by $HW(\xi)$, is the number of ones in the sequence. Given two functions f and g on V_n, the *Hamming distance* $d(f, g)$ between them is defined as the Hamming weight of the truth table of $f(x) \oplus g(x)$, where $x = (x_1, \ldots, x_n)$.

2. Useful Mathematical Tools

2.1. Kronecker Product

Notation 1 *Let $A = (a_{ij})$ be an $n \times m$ $(1, -1)$-matrix and B be a $p \times q$ $(1, -1)$-matrix. The* Kronecker product *of A and B, denoted by $A \times B$, is an $np \times mq$ $(1, -1)$-matrix, defined as*

$$A \times B = \begin{bmatrix} a_{11}B \; a_{12}B \cdots a_{1m}B \\ a_{21}B \; a_{22}B \cdots a_{2m}B \\ \cdots \\ a_{n1}B \; a_{n2}B \cdots a_{nm}B \end{bmatrix}$$

Note that $A \times B$ is not necessarily equivalent to $B \times A$.

Lemma 1 *Let A and C be two $n \times m$ $(1, -1)$-matrices, B and D be two $p \times q$ $(1, -1)$-matrices, ξ_1 and ξ_2 be two $(1, -1)$-sequences of length 2^n, η_1 and η_2 be two $(1, -1)$-sequences of length 2^m. Then the following statements hold*

(i) $(A \times B)(C \times D) = (AC) \times (BD)$,

(ii) $\langle \xi_1 \times \eta_1, \xi_2 \times \eta_2 \rangle = \langle \xi_1, \eta_1 \rangle \langle \xi_2, \eta_2 \rangle$,

(iii) *if ξ_1 is the sequence of function g on V_n and η_1 is the sequence of function h on V_m then $\xi_1 \times \eta_1$ is the sequence of $f(x) = g(y) \oplus h(z)$ where $z = (y, x)$, $y \in V_n$ and $z \in V_m$.*

2.2. Sylvester-Hadamard Matrix

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

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

From the structure of Sylvester-Hadamard matrices, we can see that $H_n = H_p \times H_{n-p}$, $p = 0, 1, \ldots, n$, where $\times$ is the Kronecker Product.

The following lemma can be proved by induction on n.

Lemma 2 *Let ℓ_i, $0 \leqq i \leqq 2^n - 1$, be the i row of H_n $(n \geqq 1)$. Then ℓ_i is the sequence of a linear function $\varphi_i(x)$ on V_n defined by the scalar product $\varphi_i(x) = \langle \alpha_i, x\rangle$, where α_i is the binary representation of $\alpha_i \in V_n$.*

Let f be a function on V_n and ξ denote the sequence of f, M denote the matrix of f, and ℓ_i denote the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$. Then by definition we have $\xi H_n = (\langle \xi, \ell_0\rangle, \langle \xi, \ell_1\rangle, \ldots, \langle \xi, \ell_{2^n-1}\rangle)$. Note that $\langle \xi(\alpha), \ell_i\rangle = \langle \xi, \ell_i(\alpha)\rangle$ for each $\alpha \in V_n$ and each i, $0 \leqq i \leqq 2^n - 1$, where ℓ_i is also the sequence of a linear function $\varphi_i(x) = \langle \alpha_i, x\rangle$, with α_i being the binary representation of an integer i. As a result we have $H_n M = diag(\langle \xi, \ell_0\rangle, \langle \xi, \ell_1\rangle, \ldots, \langle \xi, \ell_{2^n-1}\rangle)H_n$. This shows that

$$2^{-n} H_n M H_n = diag(\langle \xi, \ell_0\rangle, \langle \xi, \ell_1\rangle, \ldots, \langle \xi, \ell_{2^n-1}\rangle).$$

The following lemma can be viewed as a re-statement of a relation proved in Section 2 of [4].

Lemma 3 *For every function f on V_n, we have*

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

where ξ denotes the sequence of f and ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$.

2.3. Parseval's Equation

Comparing the first terms in two sides of the equality mentioned in Lemma 3, we have Parseval's equation (Page 416, [10]),

Lemma 4 *Let f be a function on V_n and ξ denote the sequence of f. Then $\sum_{i=0}^{2^n-1} \langle \xi, \ell_i\rangle^2 = 2^{2n}$ where ℓ_i denotes the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$.*

2.4. Restrictions of A Function to A Coset

From linear algebra, V_n can be divided into 2^{n-r} disjoint *cosets* of W:

$$V_n = U_0 \cup U_1 \cup \cdots \cup U_{2^{n-r}-1}$$

where $U_0 = W$, $\#U_j = 2^r$, $j = 0, 1, \ldots, 2^{n-r} - 1$, and for any two vectors γ and β in V_n, β and γ belong to the same coset U_j if and only if $\beta \oplus \gamma \in W$. The partition is unique if the order of the cosets is ignored. Each U_j can be expressed as $U_j = \gamma_j \oplus W$ where γ_j is a vector in V_n and $\gamma_j \oplus W$ denotes $\{\gamma_j \oplus \alpha | \alpha \in W\}$ however γ_j is not unique.

Definition 2 *Let f be a function on V_n and W be an r-dimensional linear subspace of W. For a coset $U = \gamma \oplus W$, define the* restriction of f to coset $\gamma \oplus W$, *denoted by f_U, such that $f_U(\alpha) = f(\gamma \oplus \alpha)$ for every $\alpha \in W$. In particular, the* restriction of f to the linear subspace W, *denoted by f_W, such that $f_W(\alpha) = f(\alpha)$ for every $\alpha \in W$.*

2.5. Complementary Subspace

Let W be a p-dimensional subspace of V_n and U be a an $(n-p)$-dimensional linear subspace of V_n such that each vector α in V_n can be uniquely expressed as $\alpha = \beta \oplus \gamma$ where $\beta \in W$ and $\gamma \in U$and U. Then U is called a *complementary subspace* of W, and symmetrically, W is called a *complementary subspace* of U. For a given subspace W, there exist more than one complementary subspace of W, except for the special cases where $W = V_n$ and $W = \{0\}$. Note that $W \cap U = \{0\}$.

3. Cryptographic Criteria

We consider the following important cryptographic criteria which include balance, nonlinearity, avalanche, correlation immunity, algebraic degrees (nonlinearity orders), and (non-existence of) nonzero linear structures.

3.1. Balance

A function is said to be *balanced* if its truth table contains an equal number of ones and zeros. We restate Lemma 12 in [20] as follows.

Lemma 5 *Let f_1 be a function on V_s and f_2 be a function on V_t. Then $f_1(x_1, \ldots, x_s) \oplus f_2(y_1, \ldots, y_t)$ is a balanced function on V_{s+t} if f_1 or f_2 is balanced.*

3.2. Nonlinearity

Definition 3 *The* nonlinearity *of a function f on V_n, denoted by N_f, is the minimal Hamming distance between f and all affine functions on V_n, i.e., $N_f = \min_{i=1,2,\ldots,2^{n+1}} d(f, \varphi_i)$ where φ_1, φ_2, ..., $\varphi_{2^{n+1}}$ are all the affine functions on V_n.*

Lemma 6 *Let f and g be functions on V_n whose sequences are ξ_f and ξ_g respectively. Then the distance between f and g can be calculated by $d(f,g) = 2^{n-1} - \frac{1}{2}\langle \xi_f, \xi_g \rangle$.*

The following characterizations of nonlinearity will be useful (for a proof see for instance [13]).

Lemma 7 *The nonlinearity of f on V_n can be expressed by*

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

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

Using Parseval's equation (Lemma 4) and Lemma 7, we conclude

Lemma 8 *For any function f on V_n, the nonlinearity N_f of f satisfies $N_f \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}$.*

3.3. Avalanche Characteristics

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. Set $\Delta_f(\alpha) = \langle \xi(0), \xi(\alpha) \rangle$, the scalar product of $\xi(0)$ and $\xi(\alpha)$. $\Delta_f(\alpha)$ is called the auto-correlation of f with a shift α. We write $\Delta_M = \max\{|\Delta(\alpha)| | \alpha \in V_n, \alpha \neq 0\}$. We omit the subscript of $\Delta_f(\alpha)$ if no confusion occurs.

We say that f satisfies the *avalanche criterion with respect to* α if $f(x) \oplus f(x \oplus \alpha)$ is a balanced function, i.e., $\Delta(\alpha) = 0$, where $x = (x_1, \ldots, x_n)$ and α is a vector in V_n. Furthermore f is said to satisfy the *avalanche criterion of degree k* if it satisfies the avalanche criterion with respect to every nonzero vector α with $HW(\alpha) \leqq k$.

The avalanche criterion was called the propagation criterion in [15], as well as in all our earlier papers dealing with the subject. Historically, Feistel was apparently the first person who coined the term of "avalanche" and realized its importance in the design of a block cipher [7]. According to Coppersmith [5], a member of the team who designed DES, avalanche properties were employed in selecting the S-boxes used in the cipher, which contributed to the strength of the cipher against various attacks including differential [1] and linear [12] attacks. The *strict avalanche criterion (SAC)* is the same as the avalanche criterion of degree one. The SAC was first introduced by Webster and Tavares for the design of Boolean functions involved in S-boxes. Preneel *et al* (see [15]) later generalized this concept by proposing the avalanche criterion. In an event when f does not satisfy the avalanche criterion with respect to a vector α, it is desirable that $f(x) \oplus f(x \oplus \alpha)$ is almost balanced. That is we require $|\Delta(\alpha)|$ to be a small value.

Notation 2 *Let f be a function on V_n. Set $\Re_f = \{\alpha | \Delta(\alpha) \neq 0,\ \alpha \in V_n\}$. In other words, $\Re_f$ is the set of all the vectors where f does not satisfy the avalanche criterion.*

We simply write $\Re_f$ as $\Re$ if no confusion occurs. $\#\Re$ and the distribution of $\Re$ reflect the avalanche criterion. Obviously $0 \in \Re_f$ for any function on V_n where 0 denotes the zero vector.

3.4. Global Avalanche Characteristics

Definition 4 *Let f be a function on V_n. Then the* sum-of-squares *indicator for the global avalanche characteristic (GAC) of f is defined by $\sigma_f = \sum_{\alpha \in V_n} \Delta^2(\alpha)$ and the* absolute *indicator for the characteristic is defined by $\Delta_f = \max_{\alpha \in V_n, \alpha \neq 0} |\Delta(\alpha)|$.*

GAC was introduced in [28]. The smaller the σ_f and the Δ_f, the better the GAC of a function.

3.5. Correlation Immunity

The concept of correlation immune functions was introduced by Siegenthaler [22]. Correlation immune functions are used in the design of running key generators in stream ciphers to resist the correlation attack. They are also used in the design of one-way hash functions. Xiao and Massey gave an equivalent definition of a correlation immune function [2,9].

Definition 5 *A function f is called a k*th-order correlation immune function *if*

$$\sum_{x \in V_n} f(x)(-1)^{\langle \beta, x \rangle} = 0$$

for all $\beta \in V_n$ with $1 \leqq HW(\beta) \leqq k$, where the sum, $f(x)$ and $\langle \beta, x \rangle$ are regarded as real-valued functions.

From the first equality in Section 4.1 of [2], Definition 5 can be equivalently stated as follows:

Definition 6 *Let f be a function on V_n and let ξ be its sequence. Then f is called a* kth-order correlation immune function *if and only if $\langle \xi, \ell \rangle = 0$ for every ℓ, the sequence of a linear function $\varphi(x) = \langle \alpha, x \rangle$ on V_n constrained by $1 \leqq WH(\alpha) \leqq k$.*

Let f be a function on V_n, and ξ be its sequence. Then $\langle \xi, \ell_i \rangle = 0$, where ℓ_i is the ith row of H_n, if and only if $f \oplus \langle \alpha_i, x \rangle$ is balanced, where α_i is the binary representation of an integer i, $0 \leqq i \leqq 2^n - 1$. This observation leads to the following result:

Lemma 9 *Let f be a function on V_n, ξ be its sequence, Then f is a kth-order correlation immune function, if and only if $f \oplus \langle \alpha, x \rangle$ is balanced, where α is any vector in V_n, constrained by $1 \leqq WH(\alpha) \leqq k$.*

Notation 3 *Let f be a function on V_n and ξ denote the sequence of f. Set $\Im_f = \{i \mid \langle \xi, \ell_i \rangle \neq 0, \ 0 \leqq i \leqq 2^n - 1\}$ where ℓ_i is the ith row of H_n and $\Im_f^* = \{\alpha \mid f(x) \oplus \langle \alpha, x \rangle$ is unbalanced, $\alpha \in V_n\}$.*

Since $\langle \xi, \ell_i \rangle = 0$ if and only if $f(x) \oplus \langle \alpha, x \rangle$ is balanced, $i \in \Im_f$ if and only if $\alpha_i \in \Im_f^*$ where α_i is the binary representation of integer i. Hence any result on $\Im$ (or $\Im^*$) can be translated into that on $\Im^*$ (or $\Im$). We simply write $\Im_f$ as $\Im$ and $\Im_f^*$ as $\Im^*$ if no confusion occurs. It is easy to verify that $\#\Im$ and $\#\Im^*$ are invariant under any nonsingular linear transformation on the variables where $\#$ denotes the cardinal number of a set. $\#\Im$ and the distribution of $\Im$ are closely related to correlation immunity. Specifically, using Parseval's equation (Lemma 4), $\sum_{i=0}^{2^n-1} \langle \xi, \ell_i \rangle^2 = 2^{2n}$, we can see that $\#\Im_f > 0$. Further one can verify that $\#\Im_f = 1$ if and only if f is affine.

3.6. Algebraic Degree

The *algebraic degree* (also *nonlinear order*) of a function f, denoted by $deg(f)$, has been defined in Definition 1. Higher algebraic degrees are desirable in cryptography.

3.7. Linear Structures and Linearity

Let f be a function on V_n. $\alpha \in V_n$ is called a *linear structure* of f if $|\Delta(\alpha)| = 2^n$ (i.e., $f(x) \oplus f(x \oplus \alpha)$ is a constant). For any function f, we have $\Delta(\alpha_0) = 2^n$, where α_0 is the zero vector on V_n. It is easy to verify that the set of all linear structures of a function f form a linear subspace of V_n, whose dimension is called the *linearity of* f, and denoted by L_f. We note that nonzero linear structures are considered cryptographically undesirable.

Lemma 10 *If the linearity of f is p, then there exists a nonsingular $n \times n$ matrix B over $GF(2)$ such that $f(xB) = g(y) \oplus h(z)$, where $x = (y, z)$, $y \in V_q$, $z \in V_p$, $p + q = n$ and g is a function on V_q that has no nonzero linear structures, and h is a linear function on V_p.*

4. Nonsingular Affine Transformations, Affine Translates and Some Special Functions

Let f be a function on V_n, B be a nonsingular $n \times n$ matrix over $GF(2)$ and β be a vector in V_n. Set $g(x) = f(xB \oplus \beta)$. Then g is called a *nonsingular affine transformation of f on variables*. It turns out that nonlinear properties of a Boolean function are in general invariable under a nonsingular affine transformation.

Lemma 11 *Let f be a function on V_n and $g(x) = f(xB \oplus \beta)$ where B is a nonsingular $n \times n$ matrix and β is a vector in V_n. Then (i) $N_f = N_g$, (ii) $deg(f) = deg(g)$, (iii) f is balanced if and only if g is balanced, (iv) $\#\Re_g = \#\Re_f$ and $\Re_g = \Re_f B^{-1}$, where $XB = \{\alpha B | \alpha \in X\}$, (v) $\Im^*_g = \Im^*_f B^T$, (vi) $\sigma_g = \sigma_f$, (vii) $\Delta_g = \Delta_f$.*

Let f be a function on V_n and ψ be an affine function on V_n. Then $f \oplus \psi$ is called a *affine translate of f*.

Lemma 12 *Let f be a function on V_n and $\varphi(x) = \langle \beta, x \rangle$, a linear function on V_n, where β is a vector in V_n. Let $g(x) = f(x) \oplus \varphi(x)$ be the affine translate of f. Then (i) $N_f = N_g$, (ii) $deg(f) = deg(g)$, (iii) $\Re_g = \Re_f$, (iv) $\Im^*_g = \alpha \oplus \Im^*_f$, where $\beta \oplus X = \{\beta \oplus \gamma | \gamma \in X\}$.*

The concept of bent functions was first introduced in [16].

Definition 7 *A function f on V_n is called a* bent function *if $\langle \xi, \ell_i \rangle^2 = 2^n$ for every $i = 0, 1, \ldots, 2^n - 1$, where ℓ_i is the ith row of H_n.*

A bent function on V_n exists only when n is even, and it achieves the maximum nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$. From [16] we have the following:

Theorem 1 *Let f be a function on V_n. The following statements are equivalent: (i) f is bent, (ii) the nonlinearity of f, N_f, satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}n-1}$, (iii) $\Delta(\alpha) = 0$ for any nonzero α in V_n, (iv) $\Re_f = \{0\}$ where 0 is the zero vector in V_n, (v) the matrix of f is an Hadamard matrix.*

Bent functions have following additional properties [16]:

Proposition 1 *Let f be a bent function on V_n and ξ denote the sequence of f. Then (i) the degree of f is at most $\frac{1}{2}n$, (ii) for any nonsingular $n \times n$ matrix B over $GF(2)$ and any vector $\beta \in V_p$, $g(x) = f(xB \oplus \beta)$ is a bent function, (iii) for any affine function ψ on V_n, $f \oplus \psi$ is a bent function, (iv) $2^{-\frac{1}{2}n}\xi H_n$ is the sequence of a bent function, (v) $HW(f) = 2^{n-1} \pm 2^{\frac{1}{2}n-1}$.*

We note that bent functions are not balanced. As a result these functions find few direct applications in cryptography.

An interesting theorem of [4] explores a relationship between $\#\Im$ and $\#\Re$.

Theorem 2 *For any function f on V_n, we have $(\#\Im)(\#\Re) \geqq 2^n$, where the equality holds if and only if there exists a nonsingular $n \times n$ matrix B over $GF(2)$ and a vector $\beta \in V_n$ such that $f(xB \oplus \beta) = g(y) \oplus h(z)$, where $x = (y, z)$, $x \in V_n$, $y \in V_p$, $z \in V_q$, $p + q = n$, g is a bent on V_p and h is a linear function on V_q.*

Based on the above theorem, the concept of *partially-bent* functions was also introduced in the same paper [4].

Definition 8 *A function on V_n is called a* partially-bent function *if $(\#\Im)(\#\Re) = 2^n$.*

One can see that partially-bent functions include both bent functions and affine functions. Applying Theorem 2 together with properties of linear structures, or using Theorem 2 of [25] directly, we have

Proposition 2 *A function f on V_n is a partially-bent function if and only if each $|\Delta(\alpha)|$ takes the value of 2^n or 0 only. Equivalently, f is a partially-bent function if and only if $\Re$ is composed of linear structures.*

In a later part of this paper we will examine relationships between partially bent functions and *plateaued functions*.

5. Constructing Highly Nonlinear Balanced Boolean Functions

The main goal of this section to show how to construct balanced functions that have extremely high nonlinearity. We start with investigating properties of two sequences obtained by "splitting" a bent sequence.

Lemma 13 *Let $f(x_1, x_2, \ldots, x_{2k})$ be a bent function on V_{2k}, η_0 be the sequence of $f(0, x_2, \ldots, x_{2k})$, and η_1 be the sequence of $f(1, x_2, \ldots, x_{2k})$. Then for any affine sequence ℓ of length 2^{2k-1}, we have $-2^k \leqq \langle \eta_0, \ell \rangle \leqq 2^k$ and $-2^k \leqq \langle \eta_1, \ell \rangle \leqq 2^k$.*

5.1. Highly Nonlinear Balanced Functions on V_{2k}

Note that an even number $n \geqq 4$ can be expressed as $n = 4t$ or $n = 4t + 2$, where $t \geqq 1$. As the first step towards our goal, we prove

Lemma 14 *For any integer* $t \geqq 1$ *there exists*

(i) *a balanced function* f *on* V_{4t} *such that* $N_f \geqq 2^{4t-1} - 2^{2t-1} - 2^t$,
(ii) *a balanced function* f *on* V_{4t+2} *such that* $N_g \geqq 2^{4t+1} - 2^{2t} - 2^t$.

Proof. (i) Let ℓ_i be the ith row of H_{2t} where $i = 0, 1, \dots, 2^{2t} - 1$. Then $\xi = (\ell_0, \ell_1, \dots, \ell_{2^{2t}-1})$ is a bent sequence of length 2^{4t}. Note that except for $\ell_0 = (1, 1, \dots, 1)$, all other ℓ_i ($i = 1, \dots, 2^{2t} - 1$) are balanced sequences of length 2^{2t}. Therefore replacing the all-one (or "flat") leading sequence ℓ_0 with a balanced sequence renders ξ balanced. The crucial idea here is to select a replacement with a high nonlinearity, since the nonlinearity of the resulting function depends largely on that of the replacement. The replacement we select is $\ell_0^* = (e_1, e_1, e_2, \dots, e_{2^t-1})$, where e_i is the ith row of H_t. Note that the leading sequence in ℓ_0^* is e_1 but not $e_0 = (1, 1, \dots, 1)$. ℓ_0^* is a balanced sequence of length 2^{2t}, since all e_i, $i = 1, \dots, 2^t - 1$, are balanced sequences of length 2^t. Replacing ℓ_0 by ℓ_0^*, we get a balanced sequence $\xi^* = (\ell_0^*, \ell_1, \dots, \ell_{2^{2t}-1})$. Denote by f^* the function corresponding to the sequence ξ^*, and consider the nonlinearity of f^*. Let φ be an arbitrary affine function on V_{4t}, and let L be the sequence of φ. By using Lemma 2, L is a row of $\pm H_{4t}$. Since $H_{4t} = H_{2t} \otimes H_{2t}$, L can be expressed as $L = \pm \ell_i \otimes \ell_j$, where ℓ_i and ℓ_j are two row of H_{2t}. Assume that $\ell_i = (a_0, a_1, \dots, a_{2^{2t}-1})$. Then $L = \pm(a_0\ell_j, a_1\ell_j, \dots, a_{2^{2t}-1}\ell_j)$. A property of a Hadamard matrix is that its rows are mutually orthogonal. Hence $\langle \ell_p, \ell_q \rangle = 0$ for $p \neq q$. Thus

$$|\langle \xi^*, L\rangle| \leqq |\langle \ell_0^*, \ell_j\rangle| + |\langle \ell_j, \ell_j\rangle| \leqq |\langle \ell_0^*, \ell_j\rangle| + 2^{2t}.$$

We proceed to estimate $|\langle \ell_0^*, \ell_j\rangle|$. Note that $H_{2t} = H_t \otimes H_t$, ℓ_j can be expressed as $\ell_j = e_u \otimes e_v$, where e_u and e_v are rows of H_t. Write $e_u = (b_0, \dots, b_{2^t-1})$. Then $\ell_j = (b_0 e_v, \dots, b_{2^t-1} e_v)$. Similarly to the discussion for $|\langle \xi^*, L\rangle|$, we have

$$|\langle \ell_0^*, \ell_j\rangle| \leqq \begin{cases} 2|\langle e_2, e_2\rangle| = 2^{t+1}, & \text{if } v = 2,\\ |\langle e_v, e_v\rangle| = 2^t, & \text{if } v = 3, \dots, 2^t,\\ 0, & \text{if } v = 1 \end{cases}$$

Thus $\langle \ell_0^*, \ell_j\rangle| \leqq 2^{t+1}$ and hence $|\langle \xi^*, L\rangle| \leqq 2^{t+1} + 2^{2t}$. By using Lemma 7, $d(f^*, \varphi) \geqq 2^{4t-1} - \frac{1}{2}\langle \xi^*, L\rangle \geqq 2^{4t-1} - 2^{2t-1} - 2^t$. Since φ is arbitrary, $N_{f^*} \geqq 2^{4t-1} - 2^{2t-1} - 2^t$.

(ii) Now consider the case of V_{4t+2}. Let ℓ_i, $i = 0, 1, \dots, 2^{2t+1} - 1$, be the ith row of H_{2t+1}. Then $\xi = (\ell_0, \ell_1, \dots, \ell_{2^{2t+1}-1})$ is a bent sequence of length 2^{4t+2}. The replacement for the all-one leading sequence $\ell_0 = (1, 1, \dots, 1) \in V_{2t+1}$ is the following balanced sequence $\ell_0^* = (e_{2^t}, e_{2^t+1}, \dots, e_{2^{t+1}-1})$, the concatenation of the 2^tth, the $(2^t + 1)$th, ..., and the $(2^{t+1} - 1)$th rows of H_{t+1}. Let $\xi^* = (\ell_0^*, \ell_1, \dots, \ell_{2^{2t+1}-1})$, and let f^* the function corresponding to the balanced sequence. Similarly to the case of V_{4t}, let φ be a affine function on V_{4t+2} and let L be its sequence. L can be expressed as $L = \pm \ell_i \otimes \ell_j$ where ℓ_i and ℓ_j are rows of H_{2t+1}. Hence

$$|\langle \xi^*, L\rangle| \leqq |\langle \ell_0^*, \ell_j\rangle| + |\langle \ell_j, \ell_j\rangle| \leqq |\langle \ell_0^*, \ell_j\rangle| + 2^{2t+1}$$

Since ℓ_0^* is obtained by splitting the bent sequence $(e_0, e_1, \dots, e_{2^{t+1}-1})$, where e_i is a row of H_{t+1}, by Lemma 13, we have $|\langle \ell_0^*, \ell_j\rangle| \leqq 2^{t+1}$. From this it follows that $|\langle \xi^*, L\rangle| \leqq 2^{t+1} + 2^{2t+1}$ and $N_{f^*} \geqq 2^{4t+1} - 2^{2t} - 2^t$. □

With the above result as a basis, we consider an iterative procedure to further improve the nonlinearity of a function constructed. Note that an even number $n \geqq 4$ can be expressed as $n = 2^m$, $m \geqq 2$, or $n = 2^s(2t+1)$, $s \geqq 1$ and $t \geqq 1$. Consider the case when $n = 2^m$, $m \geqq 2$. We start with the bent sequence obtained by concatenating the rows of $H_{2^{m-1}}$. The sequence consists of $2^{2^{m-1}}$ sequences of length $2^{2^{m-1}}$. Now we replace the all-one leading sequence with a bent sequence of the same length, which is obtained by concatenating the rows of $H_{2^{m-2}}$. The length of the new leading sequence becomes $2^{2^{m-2}}$. It is replaced by another bent sequence of the same length. This replacing process is continued until the length of the all-one leading sequence is $2^2 = 4$. To finish the procedure, we replace the leading sequence $(1,1,1,1)$ with $(1,-1,1,-1)$. The last replacement makes the entire sequence balanced. By induction on $s = 2,3,4,\ldots$, it can be proved that the nonlinearity of the function obtained is at least

$$2^{2^m-1} - \frac{1}{2}(2^{2^{m-1}} + 2^{2^{m-2}} + \cdots + 2^{2^2} + 2 \cdot 2^2).$$

The modifying procedure for the case of $n = 2^s(2t+1)$, $s \geqq 1$ and $t \geqq 1$, is the same as that for the case of $n = 2^m$, $m \geqq 2$, except for the last replacement. In this case, the replacing process is continued until the length of the all-one leading sequence is 2^{2t+1}. The last leading sequence is replaced by $\ell_0^* = (e_{2^t}, e_{2^t+1}, \ldots, e_{2^{t+1}-1})$, the second half of the bent sequence $(e_0, e_1, \ldots, e_{2^{t+1}-1})$, where each e_i is a row of H_{t+1}. Again by induction on $s = 1,2,3,\ldots$, it can be proved that the nonlinearity of the resulting function is at least

$$2^{2^s(2t+1)-1} - \frac{1}{2}(2^{2^{s-1}(2t+1)} + 2^{2^{s-2}(2t+1)} + \cdots + 2^{2(2t+1)} + 2^{2t+1} + 2^{t+1}).$$

We have completed the proof for the following

Theorem 3 *For any even number $n \geqq 4$, there exists a balanced function f^* on V_n whose nonlinearity is*

$$N_{f^*} \geqq \begin{cases} 2^{2^m-1} - \frac{1}{2}(2^{2^{m-1}} + 2^{2^{m-2}} + \cdots + 2^{2^2} + 2 \cdot 2^2), \; n = 2^m, \\ 2^{2^s(2t+1)-1} - \frac{1}{2}(2^{2^{s-1}(2t+1)} + 2^{2^{s-2}(2t+1)} \\ + \cdots + 2^{2(2t+1)} + 2^{2t+1} + 2^{t+1}), \; n = 2^s(2t+1). \end{cases}$$

5.2. Highly Nonlinear Balanced Functions on V_{2k+1}

Lemma 15 *Let f_1 be a function on V_s and f_2 be a function on V_t. Then $f_1(x_1,\ldots,x_s) \oplus f_2(y_1,\ldots,y_t)$ is a balanced function on V_{s+t} if either f_1 or f_2 is balanced.*

Let ξ_1 be the sequence of f_1 on V_s and ξ_2 be the sequence of f_2 on V_t. Then it is easy to verify that the Kronecker product $\xi_1 \otimes \xi_2$ is the sequence of $f_1(x_1,\ldots,x_s) \oplus f_2(y_1,\ldots,y_t)$.

Lemma 16 *Let f_1 be a function on V_s and f_2 be a function on V_t. Let g be a function on V_{s+t} defined by*

$$g(x_1,\ldots,x_s,y_1,\ldots,y_s) = f_1(x_1,\ldots,x_s) \oplus f_2(y_1,\ldots,y_t).$$

Suppose that ξ_1 and ξ_2, the sequences of f_1 and f_2 respectively, satisfy $\langle \xi_1, \ell \rangle \leqq P_1$ and $\langle \xi_2, \ell \rangle \leqq P_2$ for any affine sequence ℓ of length 2^n, where P_1 and P_2 are positive integers. Then the nonlinearity of g satisfies $N_g \geqq 2^{s+t-1} - \frac{1}{2} P_1 \cdot P_2$.

Proof. Note that $\xi = \xi_1 \otimes \xi_2$ is the sequence of g. Let φ be an arbitrary affine function on V_{s+t} and let ℓ be the sequence of φ. Then ℓ can be expressed as $\ell = \pm \ell_1 \otimes \ell_2$ where ℓ_1 is a row of H_s and ℓ_2 is a row of H_t. Since $\langle \xi, \ell \rangle = \langle \xi_1 \otimes \xi_2, \pm \ell_1 \otimes \ell_2 \rangle = \pm \langle \xi_1, \ell_1 \rangle \langle \xi_2, \ell_2 \rangle$, we have $|\langle \xi, \ell \rangle| = |\langle \xi_1, \ell_1 \rangle| \cdot |\langle \xi_2, \ell_2 \rangle| \leqq P_1 \cdot P_2$ and by using Lemma 7 $d(g, \varphi) \geqq 2^{s+t-1} - \frac{1}{2} P_1 \cdot P_2$. Due to the arbitrariness of φ, $N_g \geqq 2^{s+t-1} - \frac{1}{2} P_1 \cdot P_2$. □

Let ξ_1 be a balanced sequence of length 2^{2k} that is constructed using the method in the proof of Theorem 3, where $k \geqq 2$, Let ξ_2 be a sequence of length 2^{15} obtained by the method of [14]. Note that the nonlinearity of ξ_2 is 16276, and there are 13021 such sequences. Denote by f_1 the function corresponding to ξ_1 and by f_2 the function corresponding to ξ_2. Let

$$\begin{aligned} & f(x_1, \ldots, x_{2k}, x_{2k+1}, \ldots, x_{2k+15}) = f_1(x_1, \ldots, x_{2k}) \\ & \oplus f_2(x_{2k+1}, \ldots, x_{2k+15}) \end{aligned} \tag{2}$$

Then

Theorem 4 *The function f defined by (2) is a balanced function on V_{2k+15}, $k \geqq 2$, whose nonlinearity is at least*

$$N_f \geqq \begin{cases} 2^{2^m+14} - 108(2^{2^{m-1}} + 2^{2^{m-2}} + \cdots + 2^{2^2} + 2 \cdot 2^2), \ 2k = 2^m, \\ 2^{2^s(2t+1)+14} - 108(2^{2^{s-1}(2t+1)} + 2^{2^{s-2}(2t+1)} \\ + \cdots + 2^{2(2t+1)} + 2^{2t+1} + 2^{t+1}), \ 2k = 2^s(2t+1). \end{cases}$$

Proof. Let $\xi = \xi_1 \otimes \xi_2$. Then ξ is the sequence of f. Let ℓ be an arbitrary affine sequence of length 2^{2k+15}. Then $\ell = \pm \ell_1 \otimes \ell_2$, where ℓ_1 is a linear sequence of length 2^{2k} and ℓ_2 is a linear sequence of length 2^{15}. Thus

$$\langle \xi_1, \ell_1 \rangle \leqq \begin{cases} 2^{2^{m-1}} + 2^{2^{m-2}} + \cdots + 2^{2^2} + 2 \cdot 2^2, \ 2k = 2^m, \\ 2^{2^{s-1}(2t+1)} + 2^{2^{s-2}(2t+1)} + \cdots + 2^{2(2t+1)} \\ +2^{2t+1} + 2^{t+1}, \ 2k = 2^s(2t+1). \end{cases}$$

and

$$\langle \xi_2, \ell_2 \rangle \leqq 2 \cdot (2^{14} - 16276) = 216$$

By Lemma 16, the theorem is true. □

The nonlinearity of a function on V_{2k+15} constructed in this section is larger than that obtained by concatenating or splitting bent sequences for all $k \geqq 7$.

6. Upper Bounds and Lower Bounds on Nonlinearity

Let f be a function on V_n and ξ be the sequence of f. By the equality in Lemma 3 in different ways, we will obtain two upper bounds on the nonlinearity of functions.

6.1. Two Upper Bounds

6.1.1. The first Upper Bound

Our first upper bound can be regarded as a straightforward application Lemma 3. 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 the equality in Lemma 3 is simplified to $\eta^* H_n = \xi^*$. This causes $(\eta^* H_n)(\eta^* H_n)^T = \xi^* \xi^{*T}$, i.e., $2^n \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = \sum_{j=0}^{2^n-1} \langle\xi, \ell_j\rangle^4$. Thus there exists a j_0, $0 \leqq j_0 \leqq 2^n - 1$, such that $\langle\xi, \ell_{j_0}\rangle^4 \geqq \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)$. Note that $\Delta(\alpha_0) = \Delta(0) = 2^n$. Hence from Lemma 7, we have

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

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

It is easy to verify that the bound in Theorem 5 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.

6.1.2. The Second Upper Bound

In order to derive the second upper bound on nonlinearity, we generalize the equality in Lemma 3 in the following direction. For any integer t, $0 \leqq t \leqq n$, rewrite the equality in Lemma 3 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 × denotes the Kronecker product.

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

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

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

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

and

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

Thus we have proved the following result:

Lemma 17 *Let f be a function on V_n and ξ be the sequence of f. For any integer t, $0 \leqq t \leqq n$, set $\sigma_j = \sum_{k=0}^{2^t-1} \langle \xi, \ell_{j2^t+k} \rangle^2$, where $j = 0, 1, \ldots, 2^{n-t} - 1$. Then*

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

We can see that (3) is more general than the equality in Lemma 3, by noting the fact that the two equations become identical when $t = 0$. Now compare the jth components in the two sides of (3), we have

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

where $j = 0, 1, \ldots, 2^{n-t} - 1$ and $(a_0, a_1, \ldots, a_{2^{n-t}-1})$ denotes the jth row (column) of H_{n-t}. Since we also have $\sigma_j = \sum_{k=0}^{2^t-1} \langle \xi, \ell_{j2^t+k} \rangle^2$, for any fixed j there is a k_0, $0 \leqq k_0 \leqq 2^t - 1$, such that $|\langle \xi, \ell_{j2^t+k_0} \rangle| \geqq \sqrt{\sum_{k=0}^{2^{n-t}-1} a_k \Delta(\alpha_{k \cdot 2^t})}$. As $\Delta(\alpha_0) = 2^n$, by using Lemma 7, we have

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

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

Lemma 18 *For any integer r, $0 \leqq r \leqq n$, let $\beta_1, \ldots, \beta_r$ be r linearly independent vectors in V_n. Write $\gamma_j = c_1\beta_1 \oplus \cdots \oplus c_r\beta_r$, where $j = 0, 1, \ldots, 2^r - 1$ and $(c_1, \ldots, c_r)$ is the binary representation of integer j. Then*

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

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

In practice, simpler forms than that in Lemma 18 would be preferred. This can be achieved by letting $r = 1$ in Lemma 18. This results in

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

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

Theorem 6 *For any function f on V_n, the nonlinearity of f satisfies*

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

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

6.2. Two Lower Bounds on Nonlinearity

6.2.1. The First Lower Bound

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

Lemma 19 *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

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

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

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

Proof. Obviously, $HW(f) \geqq \tau(+-)$. By using Lemma 19, $HW(f) \geqq 2^{n-2} - \frac{1}{4}\Delta(\alpha_1)$, where $HW(f)$ 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 $HW(f)$, we have

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

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

Now we introduce the first lower bound on nonlinearity:

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

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

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

Proof. For any fixed s, $0 \leqq s \leqq 2^n - 1$, let A be a nonsingular 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 20, $N_g \geqq 2^{n-2} - \frac{1}{4}|\Delta'(\alpha_1)|$. Since A is nonsingular, $N_g = N_f$. Hence $N_f \geqq 2^{n-2} - \frac{1}{4}|\Delta(\alpha_s)|$. As s is arbitrary, $N_f \geqq 2^{n-2} - \frac{1}{4}\Delta_{min}$. □

Theorem 7 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 nonzero 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 7 holds for such a function $f(y) = x_1\varphi(y) \oplus \psi(y)$.

6.2.2. The Second Lower Bound

By using a result in [4], the authors pointed out in [29] that if f, a function on V_n, satisfies the avalanche criterion with respect to all but a subset $\Re$ of vectors in V_n, then the nonlinearity of f satisfies

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

More recently, a further improvement has been made in [21]:

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

where ρ is the maximum dimension of the linear sub-spaces in $\{0\} \cup \Re^c$ and $\Re^c = V_n - \Re$. (see Theorem 11, [21]). 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 $n \geqq 4$. Now we construct a function f on V_n: $f(x) = g(x)$ if $x \neq 0$ and $f(0) = 1 \oplus g(0)$. Since $HW(g)$ is even, $HW(f)$ must be odd. Hence f does not satisfy the avalanche characteristics with respect to any vectors and hence $|\Re| = 2^n$. In this case both (6) and (7) give the trivial inequality $N_f \geqq 0$. This problem is addressed in the rest of this section. Let f, a function on V_n, satisfy the avalanche criterion with respect to all but a subset $\Re$ of vectors in V_n. For any integer t, $0 \leqq t \leqq n$, set

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

Recall $\alpha_0, \alpha_{2^t}, \alpha_{2\cdot 2^t}, \ldots, \alpha_{(2^{n-t}-1)2^t}$ form a $(n-t)$-dimensional linear subspace of V_n, and $\{\alpha_{2^t}, \alpha_{2^{t+1}}, \ldots, \alpha_{2^{n-1}}\}$ is a basis of this subspace. From (4),

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

where $\Delta_{max} = \max\{|\Delta(\alpha)||\alpha \in V_n, \alpha \neq 0\}$ and $\sigma_j = \sum_{k=0}^{2^t-1}\langle\xi, \ell_{j2^t+k}\rangle^2$, $j = 0, 1, \ldots, 2^{n-t} - 1$. Hence $\langle\xi, \ell_{j2^t+k}\rangle^2 \leqq 2^t(\Delta(\alpha_0) + (|\Re \cap \Omega| - 1)\Delta_{max})$, $j = 0, 1, \ldots, 2^{n-t} - 1$, $k = 0, 1, \ldots, 2^t - 1$.

Note that $\Delta(\alpha_0) = 2^n$. By using Lemma 7, the nonlinearity of f satisfies

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

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

Theorem 8 *Let f, a function on V_n, satisfy the avalanche criterion with respect to all but a subset $\Re$ of vectors in V_n. Let W be any r-dimensional linear subspace of V_n, $r = 0, 1, \ldots, n$. Then the nonlinearity of f satisfies*

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

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

Since $|\Delta(\alpha)| \leqq 2^n$ for each $\alpha \in V_n$, from Theorem 8, we have

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

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

Theorem 8 is more general and gives a better estimate of lower bound than all other known lower bounds. To see this, let $W = V_n$ i.e. $r = n$. Hence we have $N_f \geqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + (|\Re| - 1)\Delta_{max}}$. As $\Delta_{max} \leqq 2^n$, this estimate is clearly better than (6). On the other hand, if $\Re \cap W = \{\alpha_0 = 0\}$ then $N_f \geqq 2^{n-1} - 2^{n-\frac{1}{2}r-1}$, which is exactly (7).

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

7. Polynomials, Nonlinearity and The Number of Terms

7.1. Terms in A Polynomial

Notation 4 $(b_1, \ldots, b_n) \preceq (a_1, \ldots, a_n)$ means that $(b_1, \ldots, b_n)$ is covered by $(a_1, \ldots, a_n)$, namely if $b_j = 1$ then $a_j = 1$. In addition, $(b_1, \ldots, b_n) \prec (a_1, \ldots, a_n)$ means that $(b_1, \ldots, b_n)$ is properly covered by $(a_1, \ldots, a_n)$, namely $(b_1, \ldots, b_n) \preceq (a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n) \neq (a_1, \ldots, a_n)$.

Notation 5 Let W be a subspace of V_n. Denote the dimension of W by $dim(W)$.

Table 1. Upper and Lower Bounds on Nonlinearity

Upper Bounds	Theorem 5: $N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt[4]{2^{2n} + \sum_{j=1}^{2^n-1} \Delta^2(\alpha_j)}$
	Theorem 6: $N_f \leqq 2^{n-1} - \frac{1}{2}\sqrt{2^n + \Delta_{max}}$
Lower Bounds	Theorem 7: $N_f \geqq 2^{n-2} - \frac{1}{4}\lvert\Delta_{min}\rvert$
	Theorem 8: $N_f \geqq 2^{n-1} - 2^{\frac{1}{2}(n-r)-1}\sqrt{2^n + (\lvert\Re \cap W\rvert - 1)\Delta_{max}}$

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

Notation 6 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 9 *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 $s+1 \leqq i_1 < \cdots < i_{t'} \leqq s+t$, 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 $\chi(x) = x_{j_1} \cdots x_{j_{s'}} x_{i_1} \cdots x_{i_{t'}}$ in f, where $x = (x_1, \ldots, x_n)$, $1 \leqq j_1 < \cdots < j_{s'} \leqq s$ and $s+1 \leqq i_1 < \cdots < i_{t'} \leqq s+t$. Denote the set of such terms by Γ_1 if $s' < s$, and by Γ_2 if $s' = s$. 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 $\bigoplus_{\gamma \preceq \alpha} \chi(\gamma \oplus \beta) = 0$. For $s' = s$, there is only one vector in V_n, $\gamma = \alpha$, such that $\chi(\gamma \oplus \beta) = 1$. Hence $\bigoplus_{\gamma \preceq \alpha} \chi(\gamma \oplus \beta) = 1$. Now consider a term $\omega(x) = x_{j_1} \cdots x_{j_k}$ in f, where $x = (x_1, \ldots, x_n)$, $1 \leqq j_1 < \cdots < j_k$, and $j_k > s+t$. Denote the set of terms given in the form of $\omega(x)$ by Ω. Due to $j_k > s+t$, and the structures of α and β, we know that $\omega(\gamma \oplus \beta) = 0$ for each $\gamma \preceq \alpha$. We write f as $f = \bigoplus_{\chi \in \Gamma_1} \chi \oplus \bigoplus_{\chi \in \Gamma_2} \chi \oplus \bigoplus_{\omega \in \Omega} \omega$. Combing the above discussion, we have $\bigoplus_{\gamma \preceq \alpha} f(\gamma \oplus \beta) = \bigoplus_{\gamma \preceq \alpha} \bigoplus_{\chi \in \Gamma_2} \chi(\gamma \oplus \beta)$. 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 9 and reorder the variables, we obtain a result well-known to coding theorists (see p.372 of [10]):

Corollary 2 *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 21 *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) $f(x_1, \dots, x_n) = \bigoplus_{\alpha \in V_n} g(a_1, \dots, a_n) x_1^{a_1} \cdots x_n^{a_n}$ *where* $\alpha = (a_1, \dots, a_n)$,
(iv) $g(x_1, \dots, x_n) = \bigoplus_{\alpha \in V_n} f(a_1, \dots, a_n) x_1^{a_1} \cdots x_n^{a_n}$ *where* $\alpha = (a_1, \dots, a_n)$.

7.2. 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.

Definition 9 *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 $U' \supset U$.*

7.2.1. A Lower Bound on Nonlinearity

In this section 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 10 *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 $\{j_1, \dots, j_t\}$ is a subset of $\{i_1, \dots i_s\}$, and $x_{j_1} \cdots x_{j_t}$ is said to be* properly covered *by $x_{i_1} \cdots x_{i_s}$ if $\{j_1, \dots, j_t\}$ is a proper subset of $\{i_1, \dots i_s\}$.*

Theorem 10 *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

$$V_n = \Pi_0 \cup \Pi_1 \cup \cdots \cup \Pi_{2^{n-s}-1} \tag{8}$$

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 (8), $j = 0, 1, \dots, 2^{s-1}$. Since $\Pi_0 = U$, N_0 is odd. Note that $\Pi_0 \cup \Pi_j$ is a $(s+1)$-dimensional subspace of V_n, $j = 1, \dots, 2^{n-s} - 1$. 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, $j = 1, \dots, 2^{n-s} - 1$. Hence $N_0 + N_1 + \cdots + N_{2^{n-s}-1} \geqq 2^{n-s}$, namely, the Hamming weight of f is at least 2^{n-s}. □

Theorem 11 *Let f be a function on V_n and U be a maximal odd weighting subspace of f. Let $dim(U) = s$ ($s \geqq 2$). Then the nonlinearity N_f of f satisfies $N_f \geqq 2^{n-s}$.*

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 10, 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 12 *Let $t \geqq 2$. 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 10) by any other term in the same function, then the nonlinearity N_f of f satisfies $N_f \geqq 2^{n-t}$.*

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 2, $\bigoplus_{\gamma \preceq \alpha} f(\gamma) = 1$ 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: $W = U \cup (\beta_1 \oplus U) \cup \cdots \cup (\beta_{2^{s-t}-1} \oplus U)$ 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 $\beta_k \oplus U$, $1 \leqq k \leqq 2^{s-t} - 1$, such that the Hamming weight of $f_{\beta_k \oplus U}$ is even, i.e. $\bigoplus_{\gamma \preceq \alpha} f(\beta_k \oplus \gamma) = 0$. Applying Theorem 9 to this formula, 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 11, the proof is completed. □

We note that the lower bound in Theorem 11 is tight:

Corollary 3 *For any n and any s with $2 \leqq s \leqq n$, 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} ($s \geqq 2$), $d(f, h) \geqq 2^{n-s}$ 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. □

7.2.2. 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 13 *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 4. Then f has at least 2^{n-t} terms, where t denotes the Hamming weight of α.*

Proof. First we note that Theorem 10 can be equivalently stated as follows: Let f be a function on V_n and g be the Mӧbius transform of f defined in (1). 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 4. Then the Hamming weight of f is at least 2^{n-t}. The equivalence between (iii) and (iv) in Lemma 21 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 (1). 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 13, it is not hard to verify

Corollary 4 *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 4. 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.*

The lower bounds on the number of terms given by Theorem 13 and Corollary 4 are tight, due to Corollary 3 and Lemma 21.

7.3. 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.

Lemma 22 *Let f be a function on V_n ($n \geqq 2$). 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 2, then the Hamming weight of f is also even.*

7.3.1. Nonlinearity of the Restriction of a Function to a Coset

Theorem 14 *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*

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

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 $0 \leqq q \leqq k-1$. 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

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

Again, by using the assumption,

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

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 5 *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 $N_f - N_{f_\Pi} \leqq 2^{n-1} - 2^{p-1}$.*

Corollary 6 *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 $N_f \leqq 2^{n-1} - 2^{p-1}$.*

7.3.2. Relating Nonlinearity to Terms in Algebraic Normal Form

The following result is an application of Corollary 6.

Theorem 15 *Let f be a function on V_n and J be a subset of $\{1, \dots, n\}$ such that f does not contain any term $x_{j_1} \cdots x_{j_t}$ where $j_1, \dots, j_t \in J$. Then the nonlinearity N_f of f satisfies $N_f \leqq 2^{n-1} - 2^{s-1}$ 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 21, $f(\alpha) = \bigoplus_{\beta \preceq \alpha} g(\beta)$. Hence $f(\alpha) = 0$ for all $\alpha \in U$. That is, $f_U = 0$. By using Corollary 6, we have proved that $N_f \leqq 2^{n-1} - 2^{s-1}$. □

The following statement can be viewed as an improvement on Theorem 15.

Theorem 16 *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 $N_f \leqq 2^{n-1} - 2^{s-1}$ 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 15, we have $N_{f^*} \leqq 2^{n-1} - 2^{s-1}$. □

The next two statements can be obtained from Theorems 15 and 16 respectively, by setting $J = \{1, \ldots, n\} - P$.

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

Note that bent functions on V_n have nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$. By using Theorem 16 we conclude

Corollary 7 *Let f be a function on V_n satisfying $N_f \geqq 2^{n-1} - 2^{s-1}$. 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 $\#P \leqq q$. Hence we have $N_f \leqq 2^{n-1} - 2^{n-\#P-1} \leqq 2^{n-1} - 2^{n-q-1} < 2^{n-1} - 2^{s-1}$. This contradicts the condition that $N_f \geqq 2^{n-1} - 2^{s-1}$. □

7.4. Hypergraph of a Boolean Function

7.4.1. 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, $1 \leqq j \leqq p$, 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 [8]:

$$\tau(\Gamma) + \kappa(\Gamma) = n, \;\; \nu(\Gamma) \leqq \tau(\Gamma). \tag{9}$$

Γ is said to satisfy the *König Property* if $\nu(\Gamma) = \tau(\Gamma)$. The following lemma can be deduced from Theorem 3.5 of [8], established by Berge and Las Vergnas in 1970.

Lemma 23 *If a hypergraph Γ has no cycle with odd length, then Γ satisfies the* König Property.

Definition 11 *Let f be a function on V_n. If $f(0) = 0$, i.e., the constant term of f is zero, 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. If $f(0) = 1$, i.e., the constant term of f is one, we do the same for $1 \oplus f$ and then obtain a hypergraph that is called the the* hypergraph of *f denoted by $\Gamma(f)$. 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 $\nu(f)$.*

Without loss of generality, in this section, we only study $\Gamma(f)$ 2ith $f(0) = 0$.

7.4.2. Applications to Nonlinearity

Corollary 8 *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 $N_f \leqq 2^{n-1} - 2^{\kappa(f^*)-1}$ or equivalently $\kappa(f^*) \leqq 1 + log_2(2^{n-1} - N_f)$. In particular, if f is a bent function, then $\kappa(f^*) \leqq \frac{1}{2}n$ and $\tau(f^*) \geqq \frac{1}{2}n$.*

To prove the corollary, we note that $N_{f^*} = N_f$. Then applying Theorem 16, we have $N_{f^*} \leqq 2^{n-1} - 2^{\kappa(f^*)-1}$. Next we introduce a key result of this section.

Theorem 17 *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 23, we have $\tau(f^*) = \nu(f^*)$. From Corollary 8, $\nu(f^*) \geqq \frac{1}{2}n$. Hence there exists a matching B of $\Gamma(f^*)$. Without loss of generality, let $B = \{E_1, \ldots, E_\nu\}$, where each E_j is an edge of $\Gamma(f^*)$, $\nu = \nu(f^*) = \tau(f^*) \geqq \frac{1}{2}n$ and $E_j \cap E_i = \emptyset$, for $j \neq i$. Note that $\#E_1 + \cdots + \#E_\nu = \#(E_1 \cup \cdots \cup E_\nu) \leqq n$. On the other hand, since $\Gamma(f^*)$ has no isolated vertex, each E_j has at least two elements. Hence $\#E_1 + \cdots + \#E_\nu \geqq 2\nu \geqq n$. From the two inequalities, we have $\#E_1 + \cdots + \#E_\nu = n$. Note that $\nu \geqq \frac{1}{2}n$ 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 18 *Let f be a function on V_n, whose nonlinearity N_f satisfies*

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

where t is real with $1 \leqq t \leqq \frac{1}{6}n$. 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 23, $\tau(f^*) = \nu(f^*)$. From Corollary 8, $\nu(f^*) \geqq n - (\frac{2}{3}n - t) = \frac{1}{3}n + t$. 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 $\Gamma(f^*)$, $\nu = \nu(f^*) = \tau(f^*) \geqq \frac{1}{3}n + t$ and $E_j \cap E_i = \emptyset$, for $j \neq i$.

Note that

$$\#E_1 + \cdots + \#E_\nu = \#(E_1 \cup \cdots \cup E_\nu) \leqq n. \tag{10}$$

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

$$\#(E_1 + \cdots + E_\nu) \geqq 2k + 3(\nu - k) \geqq 2k + 3(\frac{1}{3}n + t - k). \tag{11}$$

Comparing (10) and (11), we have $k \geqq 3t$. □

Corollary 9 *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, $0 < t \leqq \frac{1}{6}n$, such that $N_f \geqq 2^{n-1} - 2^{\frac{2}{3}n-t-1} > 2^{n-1} - 2^{\frac{2}{3}n-1}$. By using Theorem 18, the proof is completed. □

Theorems 17, 18 and Corollary 9 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. $\Gamma(f)$ is also useful in algebraic attacks [27].

8. Plateaued Functions

Now we introduce a new class of functions called plateaued functions [32,30]. Here is the definition.

Definition 12 *Let f be a function on V_n and ξ denote the sequence of f. If there exists an even number r, $0 \leqq r \leqq n$, such that $\#\Im = 2^r$ and each $\langle \xi, \ell_j \rangle^2$ takes the value of 2^{2n-r} or 0 only, where ℓ_j denotes the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$, then f is called a* rth-order plateaued function *on V_n. f is also simply called a* plateaued function *on V_n if we ignore the particular order r.*

Due to Parseval's equation (Lemma 4), the condition $\#\Im = 2^r$ can be obtained from the condition "each $\langle \xi, \ell_j \rangle^2$ takes the value of 2^{2n-r} or 0 only, where ℓ_j denotes the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$". For the sake of convenience, however, we have mentioned both conditions in Definition 12. The following result can be obtained immediately from Definition 12.

Proposition 3 *Let f be a function on V_n. Then we have (i) if f is a rth-order plateaued function then r must be even, (ii) f is an nth-order plateaued function if and only if f is bent, (iii) f is a 0th-order plateaued function if and only if f is affine.*

The following is a consequence of Theorem 3 of [25].

Proposition 4 *Every partially-bent function is a plateaued function.*

An interesting question naturally arises from Proposition 4: is a plateaued function also partially-bent ? In the coming sections we characterize plateaued functions and disprove the converse of the proposition.

8.1. Characterizations of Plateaued Functions

First we introduce Hölder's Inequality [6]. It states that for real numbers $a_j \geqq 0$, $b_j \geqq 0$, $j = 1, \ldots, k$, p and q with $p > 1$ and $\frac{1}{p} + \frac{1}{q} = 1$, the following is true:

$$(\sum_{j=1}^{k} a_j^p)^{1/p} (\sum_{j=1}^{k} b_j^q)^{1/q} \geqq \sum_{j=1}^{k} a_j b_j$$

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

We are particularly interested in the case when $p = q = 2$ in Hölder's Inequality. In this case we have

$$\sum_{j=1}^{k} a_j b_j \leqq \sqrt{(\sum_{j=1}^{k} a_j^2)(\sum_{j=1}^{k} b_j^2)} \qquad (12)$$

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

Notation 7 *Let f be a function on V_n and ξ denote the sequence of f. Let χ denote the real valued $(0,1)$-sequence defined as $\chi = (c_0, c_1, \ldots, c_{2^n-1})$ where $c_j = \begin{cases} 1 \text{ if } j \in \Im \\ 0 \text{ otherwise} \end{cases}$ and $\alpha_j \in V_n$, that is the binary representation of integer j. Write*

$$\chi H_n = (s_0, s_1, \ldots, s_{2^n-1}) \tag{13}$$

where each s_j is an integer.

We note that $\chi \begin{bmatrix} \langle \xi, \ell_0 \rangle^2 \\ \langle \xi, \ell_1 \rangle^2 \\ \vdots \\ \langle \xi, \ell_{2^n-1} \rangle^2 \end{bmatrix} = \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2 = 2^{2n}$ where the second equality holds thanks to Parseval's equation (Lemma 4). By using Lemma 3, we have $\chi H_n \begin{bmatrix} \Delta(\alpha_0) \\ \Delta(\alpha_1) \\ \vdots \\ \Delta(\alpha_{2^n-1}) \end{bmatrix} = 2^{2n}$. Noticing $\Delta(\alpha_0) = 2^n$, we obtain $s_0 2^n + \sum_{j=1}^{2^n-1} s_j \Delta(\alpha_j) = 2^{2n}$. Since

$$\Delta(\alpha_j) = 0 \text{ if } \alpha_j \notin \Re \tag{14}$$

we have $s_0 2^n + \sum_{\alpha_j \in \Re, j>0} s_j \Delta(\alpha_j) = 2^{2n}$. As $s_0 = \#\Im$, where $\#$ denotes the cardinal number of a set, we have $\sum_{\alpha_j \in \Re, j>0} s_j \Delta(\alpha_j) = 2^n(2^n - \#\Im)$. Note that

$$\begin{aligned} &2^n(2^n - \#\Im) = \textstyle\sum_{\alpha_j \in \Re, j>0} s_j \Delta(\alpha_j) \\ &\leqq \textstyle\sum_{\alpha_j \in \Re, j>0} |s_j \Delta(\alpha_j)| \leqq s_M \Delta_M (\#\Re - 1) \end{aligned} \tag{15}$$

Hence the following inequality holds.

$$s_M \Delta_M (\#\Re - 1) \geqq 2^n(2^n - \#\Im) \tag{16}$$

From (13), we obtain

$$\#\Im \cdot 2^n = \sum_{j=0}^{2^n-1} s_j^2 \text{ or } \#\Im(2^n - \#\Im) = \sum_{j=1}^{2^n-1} s_j^2 \tag{17}$$

Now we prove the first inequality that helps us understand properties of plateaued functions.

Theorem 19 *Let f be a function on V_n and ξ denote the sequence of f. Then*

$$\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) \geqq \frac{2^{3n}}{\#\Im}$$

where the equality holds if and only if f is a plateaued function.

Proof. By using (15), (12) and (17), we obtain

$$2^{2n} \leqq \sum_{\alpha_j \in \Re} s_j \Delta(\alpha_j) \leqq \sum_{\alpha_j \in \Re} |s_j \Delta(\alpha_j)| \leqq \sqrt{(\sum_{\alpha_j \in \Re} s_j^2)(\sum_{\alpha_j \in \Re} \Delta^2(\alpha_j))}$$
$$\leqq \sqrt{(\sum_{j=0}^{2^n-1} s_j^2)(\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j))} \leqq \sqrt{\#\Im 2^n \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)} \tag{18}$$

Hence $\frac{2^{3n}}{\#\Im} \leqq \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)$. We have proved the inequality in the theorem.

Assume that the equality in the theorem holds i.e., $\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = \frac{2^{3n}}{\#\Im}$. This implies that all the equalities in (18) hold. Hence

$$2^{2n} = \sum_{\alpha_j \in \Re} s_j \Delta(\alpha_j) = \sum_{\alpha_j \in \Re} |s_j \Delta(\alpha_j)| = \sqrt{(\sum_{\alpha_j \in \Re} s_j^2)(\sum_{\alpha_j \in \Re} \Delta^2(\alpha_j))}$$
$$= \sqrt{(\sum_{j=0}^{2^n-1} s_j^2)(\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j))} = \sqrt{\#\Im 2^n \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)} \tag{19}$$

Applying the property of Hölder's Inequality to (19), we conclude that

$$|\Delta(\alpha_j)| = \nu |s_j|, \alpha_j \in \Re \tag{20}$$

where $\nu > 0$ is a constant. Applying (20) and (17) to (19), we have

$$2^{2n} = \sum_{\alpha_j \in \Re} |s_j \Delta(\alpha_j)| = \sqrt{\#\Im 2^n \nu^2 \sum_{j=0}^{2^n-1} s_j^2} = \nu \#\Im 2^n \tag{21}$$

From (19), we have $\sum_{\alpha_j \in \Re} s_j \Delta(\alpha_j) = \sum_{\alpha_j \in \Re} |s_j \Delta(\alpha_j)|$. Hence (20) can be expressed more accurately as follows

$$\Delta(\alpha_j) = \nu s_j, \alpha_j \in \Re \tag{22}$$

where $\nu > 0$ is a constant. From (19), it is easy to see that $\sum_{\alpha_j \in \Re} s_j^2 = \sum_{j=0}^{2^n-1} s_j^2$. Hence

$$s_j = 0 \text{ if } \alpha_j \notin \Re \tag{23}$$

Combining (22), (23) and (14), we have

$$\nu(s_0, s_1, \ldots, s_{2^n-1}) = (\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1})) \tag{24}$$

Comparing (24) and (13), we obtain

$$\nu \chi H_n = (\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1})) \tag{25}$$

Further comparing (25) and the equation in Lemma 3, we obtain

$$2^n\nu\chi = (\langle\xi, \ell_0\rangle^2, \dots, \langle\xi, \ell_{2^n-1}\rangle^2) \tag{26}$$

Note that χ is a real valued $(0,1)$-sequence, containing $\#\Im$ ones. By using Parseval's equation (Lemma 4), we obtain $2^n\nu(\#\Im) = 2^{2n}$. Hence $\nu(\#\Im) = 2^n$, and there exists an integer r with $0 \leqq r \leqq n$ such that $\#\Im = 2^r$ and $\nu = 2^{n-r}$. From (26) it is easy to see that $\langle\xi, \ell_j\rangle^2 = 2^{2n-r}$ or 0. Hence r must be even. This proves that f is a plateaued function. Conversely assume that f is a plateaued function. Then there exists an even number r, $0 \leqq r \leqq n$, such that $\#\Im = 2^r$ and $\langle\xi, \ell_j\rangle^2 = 2^{2n-r}$ or 0, Due to Lemma 3, we have $\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = 2^{-n}\sum_{j=0}^{2^n-1}\langle\xi, \ell_j\rangle^4 = 2^{-n} \cdot 2^r \cdot 2^{4n-2r} = 2^{3n-r}$. Hence we have proved $\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = \frac{2^{3n}}{\#\Im}$. □

Lemma 24 *Let f be a function on V_n and ξ denote the sequence of f. Then the nonlinearity N_f of f satisfies $N_f \leqq 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$, where the equality holds if and only if f is a plateaued function.*

Proof. Set $p_M = \max\{|\langle\xi, \ell_j\rangle| \mid j = 0, 1, \dots, 2^n - 1\}$, where ℓ_j is the jth row of H_n, $0 \leqq j \leqq 2^n - 1$. Using Parseval's equation (Lemma 4), we obtain $p_M^2\#\Im \geqq 2^{2n}$. Due to Lemma 7, $N_f \leqq 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$. Assume that f is a plateaued function. Then there exists an even number r, $0 \leqq r \leqq n$, such that $\#\Im = 2^r$ and each $\langle\xi, \ell_j\rangle^2$ takes either the value of 2^{2n-r} or 0 only, where ℓ_j denotes the jth row of H_n, $j = 0, 1, \dots, 2^n - 1$. Hence $p_M = 2^{n-\frac{1}{2}r}$. By using Lemma 7, we have $N_f = 2^{n-1} - 2^{n-\frac{1}{2}r-1} = 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$. Conversely assume that $N_f = 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$. From Lemma 7, we have also $N_f = 2^{n-1} - \frac{1}{2}p_M$. Hence $p_M\sqrt{\#\Im} = 2^n$. Since both p_M and $\sqrt{\#\Im}$ are integers and powers of two, we can let $\#\Im = 2^r$, where r is an integer with $0 \leqq r \leqq n$. Hence $p_M = 2^{n-\frac{r}{2}}$. Obviously r is even. From Parseval's equation (Lemma 4), $\sum_{j\in\Im}\langle\xi, \ell_j\rangle^2 = 2^{2n}$, and the fact that $p_M^2\#\Im = 2^{2n}$, we conclude that $\langle\xi, \ell_j\rangle^2 = 2^{2n-r}$ for all $j \in \Im$. This proves that f is a plateaued function. □

From the proof of Lemma 24, we can see that Lemma 24 can be stated in a different way as follows.

Lemma 25 *Let f be a function f on V_n and ξ denote the sequence of f. Set $p_M = \max\{|\langle\xi, \ell_j\rangle| \mid j = 0, 1, \dots, 2^n - 1\}$, where ℓ_j is the jth row of H_n, $0 \leqq j \leqq 2^n - 1$. Then $p_M\sqrt{\#\Im} \geqq 2^n$ where the equality holds if and only if f is a plateaued function.*

Summarizing Theorem 19, Lemmas 24 and 25, we conclude

Theorem 20 *Let f be a function on V_n and ξ denote the sequence of f. Set $p_M = \max\{|\langle\xi, \ell_j\rangle| \mid j = 0, 1, \dots, 2^n - 1\}$, where ℓ_j is the jth row of H_n, $0 \leqq j \leqq 2^n - 1$. Then the following statements are equivalent: (i) f is a plateaued function on V_n, (ii) there exists an even number r, $0 \leqq r \leqq 2^n$, such that $\#\Im = 2^r$ and each $\langle\xi, \ell_j\rangle^2$ takes the value of 2^{2n-r} or 0 only, where ℓ_j denotes the jth row of H_n, $j = 0, 1, \dots, 2^n - 1$, (iii) $\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = \frac{2^{3n}}{\#\Im}$, (iv) the nonlinearity of f, N_f, satisfies $N_f = 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$, (v) $p_M\sqrt{\#\Im} = 2^n$, (vi) $N_f = 2^{n-1} - 2^{-\frac{n}{2}-1}\sqrt{\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)}$.*

Proof. Due to Definition 12, Theorem 19, Lemmas 24 and 25, (i), (ii), (iii), (iv) and (v) hold. (vi) follows from (iii) and (iv). □

We now proceed to prove the second inequality that relates $\Delta(\alpha_j)$ to nonlinearity.

Theorem 21 *Let f be a function on V_n and ξ denote the sequence of f. Then the nonlinearity N_f of f satisfies*

$$N_f \leqq 2^{n-1} - 2^{-\frac{n}{2}-1}\sqrt{\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)}$$

where the equality holds if and only if f is a plateaued function on V_n.

Proof. Set $p_M = \max\{|\langle \xi, \ell_j \rangle|| \ j = 0, 1, \ldots, 2^n - 1\}$. Multiplying the equality in Lemma 3 by itself, we have $2^n \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^4 \leqq p_M^2 \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2$. Applying Parseval's equation (Lemma 4) to the above equality, we have $\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) \leqq 2^n p_M^2$. Hence $p_M \geqq 2^{-\frac{n}{2}} \sqrt{\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)}$. By using Lemma 7, we have proved the inequality
$N_f \leqq 2^{n-1} - 2^{-\frac{n}{2}-1} \sqrt{\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)}$. The rest part of the theorem can be proved by using Theorem 20. □

Theorem 19, Lemmas 24 and 25 and Theorem 20 represent characterizations of plateaued functions.

To close this section, let us note that since $\Delta(\alpha_0) = 2^n$ and $\#\Im \leqq 2^n$, we have $2^{n-1} - 2^{-\frac{n}{2}-1} \sqrt{\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)} \leqq 2^{n-1} - 2^{\frac{n}{2}-1}$ and $2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}} \leqq 2^{n-1} - 2^{\frac{n}{2}-1}$. Hence both inequalities $N_f \leqq 2^{n-1} - 2^{-\frac{n}{2}-1} \sqrt{\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)}$ and $N_f \leqq 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$ are improvements on a more commonly used inequality $N_f \leqq 2^{n-1} - 2^{\frac{n}{2}-1}$.

8.2. Other Cryptographic Properties of Plateaued Functions

By using Lemma 7, we conclude

Proposition 5 *Let f be a rth-order plateaued function on V_n. Then the nonlinearity N_f of f satisfies $N_f = 2^{n-1} - 2^{n-\frac{r}{2}-1}$.*

The following result is the same as Theorem 18 of [31].

Lemma 26 *Let f be a function on V_n ($n \geqq 2$), ξ be the sequence of f, and p is an integer, $2 \leqq p \leqq n$. If $\langle \xi, \ell_j \rangle \equiv 0 \pmod{2^{n-p+2}}$, where ℓ_j is the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$, then the algebraic degree of f is at most $p - 1$.*

Using Lemma 26, we obtain

Proposition 6 *Let f be a rth-order plateaued function on V_n. Then the algebraic degree of f, denoted by $deg(f)$, satisfies $deg(f) \leqq \frac{r}{2} + 1$.*

We note that the upper bound on algebraic degree in Proposition 6 is tight for $r < n$. For the case of $r = n$, any nth-order plateaued function is a bent function on V_n. [16] gives a better upper bound on the algebraic degree of a bent function on V_n. That bound is $\frac{n}{2}$. The following property of plateaued functions can be verified by noting their definition.

Proposition 7 *Let f be a rth-order plateaued function on V_n, B be any nonsingular $n \times n$ matrix over $GF(2)$ and α be any vector in V_n. Then $f(xB \oplus \alpha)$ is also a rth-order plateaued function on V_n.*

Theorem 22 *Let f be a rth-order plateaued function on V_n. Then the linearity of f, denoted by q, satisfies $q \leqq n - r$, where the equality holds if and only if f is partially-bent.*

Proof. There exists a nonsingular $n \times n$ matrix B over $GF(2)$ such that $f(xB) = g(y) \oplus h(z)$, where $x = (y, z)$, $y \in V_p$, $z \in V_q$, $p + q = n$, g is a function on V_p and g does not have nonzero linear structures, h is a linear function on V_q. Hence q is equal to the linearity of f. Set $f^*(x) = f(xB)$. Let ξ, η and ζ denote the sequences of f^*, g and h respectively. Then $\xi = \eta \times \zeta$, where $\times$ denotes the Kronecker product, defined in 1. From the structure of H_n, each row of H_n, L, can be expressed as $L = \ell \times e$, where ℓ is a row of H_p and e is a row of H_q. Then we have $\langle \xi, L \rangle = \langle \eta, \ell \rangle \langle \zeta, e \rangle$. Since h is linear, ζ is a row of H_q. Replace e by ζ, we have $\langle \xi, L' \rangle = \langle \eta, \ell \rangle \langle \zeta, \zeta \rangle = 2^q \langle \eta, \ell \rangle$ where $L' = \ell \times \zeta$ is still a row of H_n. Note that f^* is also a rth-order plateaued function on V_n. Hence $\langle \xi, L \rangle$ takes the value of $\pm 2^{n-\frac{1}{2}r}$ or zero only. Therefore $\langle \eta, \ell \rangle$ must take the value of $\pm 2^{n-\frac{1}{2}r-q} = \pm 2^{p-\frac{1}{2}r}$ or zero only. This proves that g is a rth-order plateaued function on V_p. Hence $r \leqq p$ and $r \leqq n - q$, i.e., $q \leqq n - r$.

Assume that $q = n - r$. Then $p = r$. Then each $\langle \eta, \ell \rangle$ takes the value of $\pm 2^{\frac{r}{2}} = \pm 2^{\frac{p}{2}}$ or zero only, where ℓ is any row of H_p. Hence applying Parseval's equation (Lemma 4) to g, we can conclude that for each row ℓ of H_p, $\langle \eta, \ell \rangle$ cannot take the value of zero. In other words, for each row ℓ of H_p, $\langle \eta, \ell \rangle$ takes the value of $\pm 2^{\frac{p}{2}}$ only. Hence we have proved that g is a bent function on V_p. Due to Theorem 2, f is partially-bent. Conversely, assume that f is partially-bent. Due to Theorem 2, g is a bent function on V_p. Hence each $\langle \eta, \ell \rangle$ takes the value of $\pm 2^{\frac{p}{2}}$ only, where ℓ is any row of H_p. As both ζ and e are rows of H_q, $\langle \zeta, e \rangle$ takes the value 2^q or zero only. We then conclude that $\langle \xi, L \rangle$ takes the value $\pm 2^{q+\frac{p}{2}}$ or zero only. Recall that f is a rth-order plateaued function on V_n. Hence $q + \frac{p}{2} = n - \frac{r}{2}$. This implies that $r = p$, i.e., $q = n - r$. □

8.3. Relationships between Partially-bent Functions and Plateaued Functions

To examine more profound relationships between partially-bent functions and plateaued functions, we introduce one more characterization of partially-bent functions as follows.

Theorem 23 *For every function f on V_n, we have $\frac{2^n - \#\Im}{\#\Im} \leqq \frac{\Delta_M}{2^n}(\#\Re - 1)$ where the equality holds if and only if f is partially-bent.*

Proof. From Notation 7, we have $s_M \leqq s_0 = \#\Im$. As a consequence of (16), we obtain the inequality in the theorem. Next we consider the equality in the theorem. Assume that the equality holds, i.e., $\Delta_M(\#\Re - 1)\#\Im = 2^n(2^n - \#\Im)$. From (15),

$$\begin{aligned} &2^n(2^n - \#\Im) \leqq \textstyle\sum_{\alpha_j \in \Re, j>0} |s_j \Delta(\alpha_j)| \\ &\leqq \Delta_M \textstyle\sum_{\alpha_j \in \Re, j>0} |s_j| \leqq \Delta_M(\#\Re - 1)\#\Im \end{aligned} \tag{27}$$

We can see that all the equalities in (27) hold. Hence $\Delta_M(\#\Re-1)\#\Im = \sum_{\alpha_j \in \Re, j>0} |s_j \Delta(\alpha_j)|$. Note that $|s_j| \leqq \#\Im$ and $|\Delta(\alpha_j)| \leqq \Delta_M$, for $j > 0$. Hence we obtain

$$|s_j| = \#\Im \text{ whenever } \alpha_j \in \Re \text{ and } j > 0 \tag{28}$$

and $|\Delta(\alpha_j)| = \Delta_M$ for all $\alpha_j \in \Re$ with $j > 0$. Applying (28) to (17), and noticing that $s_0 = \#\Im$, we obtain $\#\Im \cdot 2^n = \sum_{j=0}^{2^n-1} s_j^2 \geqq \sum_{\alpha_j \in \Re} s_j^2 = (\#\Re)(\#\Im)^2$. This results in $2^n \geqq (\#\Re)(\#\Im)$. Together with the inequality in Theorem 2, it proves that $(\#\Re)(\#\Im) = 2^n$, i.e., f is a partially-bent function.

Conversely assume that f is a partially-bent function, i.e., $(\#\Im)(\#\Re) = 2^n$. Then the inequality in the theorem is specialized as

$$\Delta_M(2^n - \#\Im) \geqq 2^n(2^n - \#\Im) \tag{29}$$

We need to examine two cases. Case 1: $\#\Im = 2^n$. Obviously the equality in (29) holds. Case 2: $\#\Im \neq 2^n$. From (29), we have $\Delta_M \geqq 2^n$. Thus $\Delta_M = 2^n$. This completes the proof. □

Next we consider a non-bent function f. With such a function we have $\Delta_M \neq 0$. Thus from Theorem 23, we have the following result.

Corollary 10 *For every non-bent function f on V_n, we have $(\#\Im)(\#\Re) \geqq \frac{2^n(2^n-\#\Im)}{\Delta_M} + \#\Im$ where the equality holds if and only if f is partially-bent (but not bent).*

Proposition 8 *For every non-bent function f, we have $\frac{2^n(2^n-\#\Im)}{\Delta_M} + \#\Im \geqq 2^n$ where the equality holds if and only if $\#\Im = 2^n$ or f has a nonzero linear structure.*

Proof. Since $\Delta_M \leqq 2^n$, the inequality is obvious. On the other hand, it is easy to see that the equality holds if and only if $(2^n - \Delta_M)(2^n - \#\Im) = 0$. □

From Proposition 8, one observes that for any non-bent function f, Corollary 10 implies Theorem 2.

Theorem 24 *Let f be a rth-order plateaued function. Then the following statements are equivalent: (i) f is a partially-bent function, (ii) $\#\Re = 2^{n-r}$, (iii) $\Delta_M(\#\Re - 1) = 2^{2n-r} - 2^n$, (iv) the linearity q of f satisfies $q = n - r$.*

Proof. (i) $\Longrightarrow$ (ii). Since f is a partially-bent function, we have $(\#\Im)(\#\Re) = 2^n$. As f is a rth-order plateaued function, $\#\Im = 2^r$ and hence $\#\Re = 2^{n-r}$.

(ii) $\Longrightarrow$ (iii). It is obviously true when $r = n$. For the case of $r < n$. Using Theorem 23, we have $\frac{2^n-\#\Im}{\#\Im} \leqq \frac{\Delta_M}{2^n}(\#\Re - 1)$ which is specialized as

$$2^{n-r} - 1 \leqq \frac{\Delta_M}{2^n}(2^{n-r} - 1) \tag{30}$$

From (30) and the fact that $\Delta_M \leqq 2^n$, we obtain $2^{n-r}-1 \leqq \frac{\Delta_M}{2^n}(2^{n-r}-1) \leqq 2^{n-r}-1$. Hence $\Delta_M = 2^n$ or $r = n$. (iii) obviously holds when $\Delta_M = 2^n$. When $r = n$, we have $\#\Re = 1$ and hence (iii) also holds.

(iii) $\Longrightarrow$ (i). Note that (iii) implies $\frac{2^n - \#\Im}{\#\Im} = \frac{\Delta_M}{2^n}(\#\Re - 1)$ where $\#\Im = 2^r$. By Theorem 23, f is partially-bent. Due to Theorem 22, (iv) $\Longleftrightarrow$ (i). □

8.4. Constructing Plateaued Functions and Disproof of the Converse of Proposition 4

8.4.1. Disproof of The Converse of Proposition 4

Lemma 27 *For any positive integers t and k with $k < 2^t < 2^k$, there exist $k+1$ nonzero vectors in V_k, say $\gamma_0, \gamma_1, \ldots, \gamma_k$, such that for any nonzero vector $\gamma \in V_k$, we have $(\langle\gamma_0,\gamma\rangle, \langle\gamma_1,\gamma\rangle, \ldots, \langle\gamma_k,\gamma\rangle) \neq (0,0,\ldots,0)$ and $(\langle\gamma_0,\gamma\rangle, \langle\gamma_1,\gamma\rangle, \ldots, \langle\gamma_k,\gamma\rangle) \neq (1,1,\ldots,1)$.*

Proof. We choose k linearly independent vectors in V_k, say $\gamma_1, \ldots, \gamma_k$. From linear algebra, $(\langle\gamma_1,\gamma\rangle, \ldots, \langle\gamma_k,\gamma\rangle)$ goes through all the nonzero vectors in V_k exactly once while γ goes through all the nonzero vectors in V_k. Hence there exists a unique γ^* satisfying $(\langle\gamma_1,\gamma^*\rangle, \ldots, \langle\gamma_k,\gamma^*\rangle) = (1,\ldots,1)$ and hence for any nonzero vector $\gamma \in V_k$ with $\gamma \neq \gamma^*$, $\{\langle\gamma_1,\gamma\rangle, \ldots, \langle\gamma_k,\gamma\rangle\}$ contains both one and zero. Let γ_0 be a nonzero vector in V_k, such that $\langle\gamma_0,\gamma^*\rangle = 0$. Obviously $\gamma_0 \notin \{\gamma_1,\ldots,\gamma_k\}$. It is easy to see that $\gamma_0, \gamma_1, \ldots, \gamma_k$ satisfy the property in the lemma. □

Let t and k be positive integers with $k < 2^t < 2^k$. Set $n = t+k$ and $r = 2n-2k = 2t$. We now prove the existence of balanced rth-order plateaued functions on V_n and disproves the converse of Proposition 4. We will not discuss nth-order and 0th-order plateaued function on V_n as they are simply bent and affine functions respectively.

Since $t < k$, there exists a mapping P from V_t to V_k satisfying

(i) $P(\beta) \neq P(\beta')$ if $\beta \neq \beta'$,
(ii) $\gamma_0, \gamma_1, \ldots, \gamma_k \in P(V_t)$, where $P(V_t) = \{P(\beta) | \beta \in V_t\}$,
(iii) $0 \notin P(V_t)$ where 0 denotes the zero vector in V_k.

We define a function f on V_{t+k} as $f(x) = f(y,z) = P(y)z^T$. where $x = (y,z)$, $y \in V_t$ and $z \in V_k$. Denote the sequence of f by ξ. Let L be a row of H_{t+k}. Hence $L = e \times \ell$ where e is a row of H_t and ℓ is a row of H_k. Once again from the properties of Sylvester-Hadamard matrices, L is the sequence of a linear function V_{t+k}, denoted by ψ, $\psi(x) = \langle\alpha,x\rangle$, $\alpha = (\beta,\gamma)$ and $x = (y,z)$ where $y,\beta \in V_t$ and $z,\gamma \in V_k$. Hence $\psi(x) = \langle\beta,y\rangle \oplus \langle\gamma,z\rangle$. Note that

$$\begin{aligned}\langle\xi, L\rangle &= \sum_{y\in V_t, z\in V_k} (-1)^{P(y)z^T \oplus \langle\beta,y\rangle \oplus \langle\gamma,z\rangle} \\ &= \sum_{y\in V_t} (-1)^{\langle\beta,y\rangle} \sum_{z\in V_k} (-1)^{(P(y)\oplus\gamma)z^T} \\ &= \begin{cases} 2^k \sum_{P(y)=\gamma} (-1)^{\langle\beta,y\rangle} \\ = 2^k(-1)^{\langle\beta,P^{-1}(\gamma)\rangle}, \text{ if } P^{-1}(\gamma) \text{ exists} \\ 0, \text{ otherwise} \end{cases} \end{aligned} \tag{31}$$

Thus f is a rth-order plateaued function on V_n. Next we prove that f has no nonzero linear structures. Let $\alpha = (\beta, \gamma)$ be a nonzero vector in V_{t+k} where $\beta \in V_t$ and $\gamma \in V_k$.

$$\Delta(\alpha) = \langle \xi, \xi(\alpha) \rangle = \sum_{y \in V_t, z \in V_k} (-1)^{P(y)z^T \oplus P(y \oplus \beta)(z \oplus \gamma)^T}$$

$$= \sum_{y \in V_t} (-1)^{P(y\oplus\beta)\gamma^T} \sum_{z \in V_k} (-1)^{(P(y)\oplus P(y\oplus\beta))z^T} \tag{32}$$

There exist two cases to be considered: $\beta \neq 0$ and $\beta = 0$. When $\beta \neq 0$, due to the property (i) of P, we have $P(y) \neq P(y \oplus \beta)$. Hence we have $\sum_{z \in V_k} (-1)^{(P(y)\oplus P(y\oplus\beta))z^T} = 0$ from which it follows that $\Delta(\alpha) = 0$. On the other hand, when $\beta = 0$, we have $\Delta(\alpha) = 2^k \sum_{y \in V_t} (-1)^{P(y)\gamma^T}$. Due to Lemma 27, $P(y)\gamma^T$ cannot be a constant. Hence $\sum_{y \in V_t} (-1)^{P(y)\gamma^T} \neq \pm 2^t$ which implies that $\Delta(\alpha) \neq 2^{t+k}$. Thus we can conclude that f has no nonzero linear structures. Finally, due to the property (iii) of P, f must be balanced. Therefore we have

Lemma 28 *Let k, t be possible integers with $k < 2^t < 2^k$, $n = t + k$ and $r = 2t$. Then there exists a balanced rth-order plateaued function on V_n that does not have a nonzero linear structure.*

Lemma 28 not only indicates the existence of balanced plateaued function of any order r with $0 < r < n$, but also shows that the converse of Proposition 4 is not true. f has some other interesting properties. In particular, due to Proposition 5, the nonlinearity N_f of f satisfies $N_f = 2^{n-1} - 2^{n-\frac{r}{2}-1}$. Since f is not partially-bent, Theorem 2 tells us that $(\#\Im)(\#\Re) > 2^n$. This proves that $\#\Re > 2^{n-r}$.

Now we summaries the relationships among bent, partially-bent and plateaued functions. Let $\mathbf{B_n}$ denote the set of bent functions on V_n, $\mathbf{P_n}$ denote the set of partially-bent functions on V_n and $\mathbf{F_n}$ denote the set of plateaued functions on V_n. Then the above results imply that $\mathbf{B_n} \subset \mathbf{P_n} \subset \mathbf{F_n}$, where $\subset$ denotes the relationship of proper subset. We further let $\mathbf{G_n}$ denote the set of plateaued functions on V_n that do *not* have nonzero linear structures and are not bent functions. Lemma 28 ensures that $\mathbf{G_n}$ is non-empty.

8.4.2. Constructing Balanced rth-order Plateaued Functions Satisfying SAC

Next we consider how to improve the function in the proof of Lemma 28 so as to obtain a rth-order plateaued function on V_n satisfying the strictly avalanche criterion (SAC), in addition to all the properties mentioned in Section 8.4.1. Note that if $r > 2$, i.e., $t > 1$, then from Section 8.4.1, we have $\#\Re \leqq 2^{n-\frac{1}{2}r} < 2^{n-1}$. In other words, $\#\Re^c > 2^{n-1}$ where $\Re^c$ denotes the complementary set of $\Re$. Hence there exist n linearly independent vectors in $\Re^c$. In other words, there exist n linearly independent vectors with respect to which f satisfies the avalanche criterion. Hence we can choose a nonsingular $n \times n$ matrix A over $GF(2)$ such that $g(x) = f(xA)$ satisfies the SAC (see [19]). The nonsingular linear transformation A does not alter any of the properties of f discussed in Section 8.4.1. Thus we have

Theorem 25 *Let n be a positive number and r be any even number with $0 < r < n$. Then there exists a balanced rth-order plateaued function on V_n that does not have a nonzero linear structure and satisfies the SAC.*

8.4.3. Constructing Balanced rth-order Plateaued Functions Satisfying SAC and Having Maximum Algebraic Degree

We can further improve the function described in Section 8.4.2 so as to obtain a rth-order plateaued functions on V_n that have the highest algebraic degree and satisfy all the properties mentioned in Section 8.4.2. Theorem 1 in Chapter 13 of [10] allows us to verify that the following lemma is true.

Theorem 26 *Let k, t be possible integers with $k < 2^t < 2^k$, $n = t + k$ and $r = 2t$. Then there exists a balanced rth-order plateaued function on V_n that does not have a nonzero linear structure, satisfies the SAC and has the highest possible algebraic degree $\frac{r}{2} + 1$.*

8.4.4. Constructing Balanced rth-order Plateaued and Correlation Immune Functions

Let f be a function on V_n, ξ be the sequence of f and ℓ_i denote the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$. Recall that in Notation 3, we defined $\Im_f = \{i \mid 0 \leqq i \leqq 2^n - 1,\ \langle \xi, \ell_i \rangle \neq 0\}$. Now let $\Im_f^* = \{\alpha_i \mid 0 \leqq i \leqq 2^n - 1,\ i \in \Im_f\}$. $\Im_f^*$ will be used in the following description of constructing plateaued functions that are correlation immune.

Lemma 29 *Let f be a function on V_n, ξ be the sequence of f, and ℓ_i denote the ith row of H_n. Also let W be an r-dimensional linear subspace of V_n such that $\Im_f^* \subseteq W$, and $s = \lfloor \frac{n}{r} \rfloor$ where $\lfloor \frac{n}{r} \rfloor$ denotes the maximum integer not larger than $\frac{n}{r}$. Then there exists a nonsingular $n \times n$ matrix B on $GF(2)$ such that $h(y) = g(yB)$ is an $(s-1)$th-order correlation immune function.*

Theorem 27 *Let t and k be positive integers with $k < 2^t < 2^k$. Let $n = k + t$ and $r = 2t$. Then there exists a rth-order plateaued function on V_n that is also an $(s-1)$th-order correlation immune function, where $s = \lfloor \frac{n}{r+1} \rfloor$ or $s = \lfloor \frac{t+k}{2t+1} \rfloor$, and does not have a nonzero linear structure.*

Other constructions of plateaued functions can be found in [3].

9. Relationships among Avalanche, Nonlinearity and Correlation Immunity

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

Lemma 30 *Let $(a_0, a_1, \ldots, a_{2^n-1})$ and $(b_0, b_1, \ldots, b_{2^n-1})$ be two real-valued sequences of length 2^n, satisfying $(a_0, a_1, \ldots, a_{2^n-1})H_n = (b_0, b_1, \ldots, b_{2^n-1})$. Let p be an integer with $1 \leqq p \leqq n-1$. For any fixed i with $0 \leqq i \leqq 2^{n-p}-1$ and any fixed j with $0 \leqq j \leqq 2^p - 1$, let $\chi_i = (a_{i \cdot 2^p}, a_{1+i \cdot 2^p}, \ldots, a_{2^p-1+i \cdot 2^p})$ and $\lambda_j = (b_j, b_{j+2^p}, b_{j+2 \cdot 2^p}, \ldots, b_{j+(2^{n-p}-1)2^p})$. Then we have*

$$2^{n-p}\langle \chi_i, e_j \rangle = \langle \lambda_j, \ell_i \rangle,\ i = 0, 1, \ldots, 2^{n-p} - 1,\ j = 0, 1, \ldots, 2^p - 1 \qquad (33)$$

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

Lemma 30 can be viewed as a refined version of the Hadamard transformation $(a_0, a_1, \ldots, a_{2^n-1})H_n = (b_0, b_1, \ldots, b_{2^n-1})$ and it will be a useful mathematical tool in proving the following two lemmas. These two lemmas will then play a significant role in proving the main results of this paper.

Lemma 31 *Let f be a non-bent function on V_n, satisfying the avalanche criterion of degree p. Denote the sequence of f by ξ. If there exists a row L^* of H_n such that $|\langle \xi, L^* \rangle| = 2^{n-\frac{1}{2}p}$, then $\alpha_{2^{t+p}+2^p-1}$ is a nonzero linear structure of f, where $\alpha_{2^{t+p}+2^p-1}$ is the vector in V_n corresponding to the integer $2^{t+p} + 2^p - 1$, $t = 0, 1, \ldots, n-p-1$.*

Lemma 32 *Let f be a non-bent function on V_n, satisfying the avalanche criterion of degree p. Denote the sequence of f by ξ. If there exists a row L^* of H_n, such that $|\langle \xi, L^* \rangle| = 2^{n-\frac{1}{2}p}$, then $p = n-1$ and n is odd.*

Theorem 28 *Let f be a function on V_n, satisfying the avalanche criterion of degree p. Then*

(i) *the nonlinearity N_f of f satisfies $N_f \geqq 2^{n-1} - 2^{n-1-\frac{1}{2}p}$,*

(ii) *the equality in (i) holds if and only if one of the following two conditions holds:*

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

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

9.2. Relationships between Avalanche and Correlation Immunity

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

Lemma 33 *Let f be a function on V_n. Then*

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

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

9.2.1. The Case of Balanced Functions

Theorem 29 *Let f be a balanced qth-order correlation immune function on V_n, satisfying the avalanche criterion of degree p. Then we have $p + q \leqq n-2$.*

9.2.2. The Case of Unbalanced Functions

We turn our attention to unbalanced functions. A direct proof of the following Lemma can be found in [29].

Lemma 34 *Let $k \geqq 2$ be a positive integer and $2^k = a^2 + b^2$, where both a and b are integers with $a \geqq b \geqq 0$. Then $a = 2^{\frac{1}{2}k}$ and $b = 0$ when k is even, and $a = b = 2^{\frac{1}{2}(k-1)}$ otherwise.*

Theorem 30 *Let f be an unbalanced qth-order correlation immune function on V_n, satisfying the avalanche criterion of degree p. Then*

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

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

Theorem 31 *Let f be an unbalanced qth-order correlation immune function on V_n, satisfying the avalanche criterion of degree p. If $p + q = n - 1$, then f also satisfies the avalanche criterion of degree $p + 1$, n is odd and f must take the form mentioned in (ii) of Theorem 30.*

From Theorems 30 and 31, we conclude

Corollary 11 *Let f be an unbalanced qth-order correlation immune function on V_n, satisfying the avalanche criterion of degree p. Then*

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

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

When a correlation immune function is balanced, it is said to be cryptographically resilient. Analogous to order of correlation immunity, we can define order of resiliency for a cryptographically resilient function. Further results on relationships between nonlinearity and correlation immunity can be found in [11], [18], [23], [33] and [24]. In addition, authors of [17] presented new construction methods for balanced Boolean functions with such desirable cryptographic properties as balance, hight nonlinearity, good avalanche characteristics and correlation immunity.

10. Concluding Remarks

Cryptographic Boolean functions remain a fascinating area of research both to theoreticians and practitioners. Recent progress in cryptanalysis made by Xiaoyun Wang and co-workers [26] indicated that sometimes a cryptographic algorithm may still be vulnerable even though the algorithm employs Boolean functions with highly desirable nonlinear properties. This, however, should not be interpreted as an indication that nonlinear Boolean functions are irrelevant to cryptographic algorithms. A more prudent view is that nonlinear Boolean functions need to be applied in an appropriate way that enhances the security of a cryptographic algorithm. Identifying methods or best practices for applying nonlinear Boolean functions that strengthen the security of cryptographic algorithms is an important area worth further research.

References

[1] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, Vol. 4, No. 1:3–72, 1991.

[2] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In *Advances in Cryptology - CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 87–100. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[3] C. Carlet and E. Prouff. On plateaued functions and their constructions. In *Fast Software Encryption 2003*, volume 2887 of *Lecture Notes in Computer Science*, pages 54–73. Springer-Verlag, Berlin, Heidelberg, New York, 2003.

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

[5] D. Coppersmith. The development of DES, 2000. (Invited talk at CRYPTO2000).

[6] Friedhelm Erwe. *Differential And Integral Calculus*. Oliver And Boyd Ltd, Edinburgh And London, 1967.

[7] H. Feistel. Cryptography and computer privacy. *Scientific American*, 228(5):15–23, 1973.

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

[9] Xiao Guo-Zhen and J. L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Transactions on Information Theory*, 34(3):569–571, 1988.

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

[11] S. Maitra and P. Sarkar. Highly nonlinear resilient functions optimizing siegenthaler's inequality. In *Advances in Cryptology - CRYPTO 1999*, volume 1666 of *Lecture Notes in Computer Science*, pages 198–215. Springer-Verlag, Berlin, Heidelberg, New York, 1999.

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

[13] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89*, volume 434 of *Lecture Notes in Computer Science*, pages 549–562. Springer-Verlag, Berlin, Heidelberg, New York, 1990.

[14] N. J. Patterson and D. H. Wiedemann. The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-29(3):354–356, 1983.

[15] B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, volume 437 of *Lecture Notes in Computer Science*, pages 155–165. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

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

[17] P. Sarkar and S. Maitra. Constructions of highly nonlinear balanced boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 485–506. Springer-Verlag, Berlin, Heidelberg, New York, 2000.

[18] P. Sarkar and S. Maitra. Nonlinearity bounds and constructions of resilient boolean functions. In *Advances in Cryptology - CRYPTO2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 515–532. Springer-Verlag, Berlin, Heidelberg, New York, 2000.

[19] J. Seberry, X. M. Zhang, and Y. Zheng. Improving the strict avalanche characteristics of cryptographic functions. *Information Processing Letters*, 50:37–41, 1994.

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

[21] J. Seberry, X. M. Zhang, and Y. Zheng. The relationship between propagation characteristics and nonlinearity of cryptographic functions. *Journal of Universal Computer Science*, 1(2):136–150, 1995. (`http://www.jucs.org/`).

[22] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30 No. 5:776–779, 1984.

[23] Y. Tarannikov. On resilient boolean functions with maximal possible nonlinearity. In *Proceedings of Indocrypt 2000*, volume 1977 of *Lecture Notes in Computer Science*, pages 19–30. Springer-Verlag, Berlin, Heidelberg, New York, 2000.

[24] Y. Tarannikov, P. Korolev, and A. Botev. Autocorrelation coefficients and correlation immunity of boolean functionstions. In *Proceedings of ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 460–479. Springer-Verlag, Berlin, Heidelberg, New York, 2001.

[25] J. Wang. The linear kernel of boolean functions and partially-bent functions. *System Science and Mathematical Science*, 10:6–11, 1997.

[26] Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu. Finding Collisions in the Full SHA-1. In *Proceedings of CRYPT 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 17-36. Springer-Verlag, Berlin, Heidelberg, New York, 2005.

[27] X. M. Zhang, J. Pieprzyk, and Y. Zheng. Algebraic immunity and annihilators. In *The 9th International Conference on Information Security and Cryptology (ICISC 2006), Busan, Korea*, volume 4296 of *Lecture Notes in Computer Science*, pages 65–80. Springer-Verlag, Berlin, Heidelberg, New York, 2006.

[28] X. M. Zhang and Y. Zheng. GAC — the criterion for global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science*, 1(5):316–333, 1995. (`http://www.jucs.org/`).

[29] X. M. Zhang and Y. Zheng. Characterizing the structures of cryptographic functions satisfying the propagation criterion for almost all vectors. *Design, Codes and Cryptography*, 7(1/2):111–134, 1996. special issue dedicated to Gus Simmons.

[30] X. M. Zhang and Y. Zheng. On plateaued functions. *IEEE Transactions on Information Theory*, IT-47 No. 3:1215–1223, 2001.

[31] X. M. Zhang, Y. Zheng, and Hideki Imai. Duality of boolean functions and its cryptographic significance. In *Advances in Cryptology - ICICS'97*, volume 1334 of *Lecture Notes in Computer Science*, pages 159–169. Springer-Verlag, Berlin, Heidelberg, New York, 1997.

[32] Y. Zheng and X. M. Zhang. Plateaued functions. In *Advances in Cryptology - ICICS'99*, volume 1726 of *Lecture Notes in Computer Science*, pages 284–300. Springer-Verlag, Berlin, Heidelberg, New York, 1999.

[33] Y. Zheng and X. M. Zhang. Improved upper bound on the nonlinearity of high order correlation immune functions. In *Selected Areas in Cryptography, 7th Annual International Workshop, SAC2000*, volume 2012 of *Lecture Notes in Computer Science*, pages 264–274. Springer-Verlag, Berlin, Heidelberg, New York, 2001.