The Relationship Between Propagation Characteristic and Nonlinearity of Cryptographic Functions

Jennifer Seberry *Xian-Mo Zhang* *Yuliang Zheng*
Department of Computer Science
The University of Wollongong
Wollongong, NSW 2522, AUSTRALIA

E-mail: {jennie,xianmo,yuliang}@cs.uow.edu.au

June 2, 1994

Abstract

The nonlinearity of a Boolean function indicates the minimum distance between the function and all the affine functions, while the propagation characteristic of a Boolean function forecasts the avalanche behavior of the function when some input bits to the function are complemented. Both nonlinearity and propagation characteristic are regarded as critical indicators of the cryptographic strength of a Boolean function. A main contribution of this paper is to reveal the relationship of the two cryptographic criteria. In particular, we prove that

(i) if f, a Boolean function on V_n, satisfies the propagation criterion with respect to all but a subset $\Re$ of vectors in V_n, then the nonlinearity of f satisfies $N_f \geqq 2^{n-1} - 2^{\frac{1}{2}(n+t)-1}$, where t is the rank of $\Re$, and

(ii) When $|\Re| > 2$, the nonzero vectors in $\Re$ are linearly dependent.

Furthermore we show that

(iii) if $|\Re| = 2$ then n must be odd and the nonlinearity of f satisfies $N_f \geqq 2^{n-1} - 2^{\frac{1}{2}(n-1)}$, and if $|\Re| = 4$ then n must be even and the nonlinearity of f satisfies $N_f \geqq 2^{n-1} - 2^{\frac{1}{2}n}$. In both cases, the nonzero vector(s) in $\Re$ must be linear structure(s) of f.

(iv) there exists no function on V_n such that $|\Re| = 3$.

Combining (iii) with results presented in (Seberry *et al.*, 1994a), we conclude that $|\Re| = 2$ (or 4) if and only if f is a two-(or four-)repetition of a bent function on V_{n-1} (or V_{n-2}).

Key Words

Bent Functions, Boolean Functions, Cryptography, Data Security, Hadamard Matrices, Nonlinearity, Propagation Characteristic.

1 Basic Definitions

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

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

Definition 1 *The* Hamming weight *of a $(0,1)$-sequence s, denoted by $W(s)$, is the number of ones in the sequence. Given two functions f and g on V_n, the* Hamming distance *$d(f,g)$ between them is defined as the Hamming weight of the truth table of $f(x) \oplus g(x)$, where $x = (x_1,\ldots,x_n)$. The* nonlinearity *of f, denoted by N_f, is the 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.*

Now we introduce the definition of propagation criterion.

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

1. *the* propagation criterion with respect to α *if $f(x) \oplus f(x \oplus \alpha)$ is a balanced function, where $x = (x_1,\ldots,x_n)$ and α is a vector in V_n.*

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

The above definition for propagation criterion is from (Preneel *et al.*, 1991b). Further work on the topic can be found in (Preneel *et al.*, 1991a). Note that the strict avalanche criterion (SAC) introduced by Webster and Tavares (Webster, 1985; Webster & Tavares, 1986) is equivalent to the propagation criterion of degree 1 and that the perfect nonlinearity studied by Meier and Staffelbach (Meier & Staffelbach, 1990) is equivalent to the propagation criterion of degree n where n is the number of the coordinates of the function.

While the propagation characteristic measures the avalanche effect of a function, the linear structure is a concept that in a sense complements the former, namely, it indicates the straightness of a function.

Definition 3 *Let f be a function on V_n. A vector $\alpha \in V_n$ is called a* linear structure *of f if $f(x) \oplus f(x \oplus \alpha)$ is a constant.*

By definition, the zero vector in V_n is a linear structure of all functions on V_n. It is not hard to see that the linear structures of a function f form a linear subspace of V_n. The dimension of the subspace is called the *linearity dimension* of f. We note that it was Evertse who first introduced the notion of linear structure (in a sense broader than ours) and studied its implication on the security of encryption algorithms (Evertse, 1988).

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

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

Definition 4 *A function f on V_n is called a* bent *function if*

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

for all $\beta \in V_n$. Here $\langle \beta, x \rangle$ is the scalar product of β and x, namely, $\langle \beta, x \rangle = \sum_{i=1}^{n} b_i x_i$, and $f(x) \oplus \langle \beta, x \rangle$ is regarded as a real-valued function.

Bent functions can be characterized in various ways (Adams & Tavares, 1990; Dillon, 1972; Seberry *et al.*, 1994a; Yarlagadda & Hershey, 1989). In particular the following four statements are equivalent:

(i) f is bent.

(ii) $\langle \xi, \ell \rangle = \pm 2^{\frac{1}{2}n}$ for any affine sequence ℓ of length 2^n, where ξ is the sequence of f.

(iii) f satisfies the propagation criterion with respect to all non-zero vectors in V_n.

(iv) M, the matrix of f, is a Hadamard matrix.

Bent functions on V_n exist only when n is even. Another important property of bent functions is that they achieve the highest possible nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$.

In (Seberry *et al.*, 1994b) connections among various important cryptographic characteristics, including the SAC, differential characteristics, linear structures and nonlinearity, of *quadratic* functions have been presented. In Section 2 we carry on the investigation initiated in (Seberry *et al.*, 1994b) and bring together nonlinearity and propagation characteristic, two seemingly quite separate cryptographic criteria, of a Boolean function (quadratic or non-quadratic). In Sections 3, 4 and 5 we further explore this result to make explicit the structural forms of functions that satisfy the propagation criterion with respect to all but a small number of vectors.

2 Propagation Characteristic and Nonlinearity

Given two sequences $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_m)$, their component-wise product is defined by $a * b = (a_1 b_1, \ldots, a_m b_m)$. Let f be a function on V_n. For a vector $\alpha \in V_n$, denote by $\xi(\alpha)$ the sequence of $f(x \oplus \alpha)$. Thus $\xi(0)$ is the sequence of f itself and $\xi(0) * \xi(\alpha)$ is the sequence of $f(x) \oplus f(x \oplus \alpha)$.

Set

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

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

Let $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$ be the matrix of f and ξ be the sequence of f. Due to a very pretty result by R. L. McFarland (see Theorem 3.3 of (Dillon, 1972)), M can be decomposed into

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

where ℓ_i is the ith row of H_n, a Sylvester-Hadamard matrix of order 2^n. By Lemma 2 of (Seberry *et al.*, 1994a), ℓ_i is the sequence of a linear function defined by $\varphi_i(x) = \langle \alpha_i, x \rangle$, where α_i is the ith vector in V_n according to the ascending alphabetical order.

Clearly

$$MM^T = 2^{-n} H_n \operatorname{diag}(\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2) H_n. \tag{1}$$

On the other hand, we always have

$$MM^T = (\Delta(\alpha_{i+j})),$$

where $i, j = 0, 1, \ldots, 2^n - 1$.

Let S be a set of vectors in V_n. The *rank* of S is the maximum number of linearly independent vectors in S. Note that when S forms a linear subspace of V_n, its rank coincides with its dimension. Now we prove a central result of the paper:

Theorem 1 *Let f be a function on V_n that satisfies the propagation criterion with respect to all but a subset $\Re$ of vectors in V_n. Then the nonlinearity of f satisfies $N_f \geqq 2^{n-1} - 2^{\frac{1}{2}(n+t)-1}$, where t is the rank of $\Re$.*

Proof. First we consider the case where $\{\alpha_1, \ldots, \alpha_t\}$ are t linearly independent vectors in $\Re$, where each α_j is defined according to the ascending alphabetical order in V_n. Let W be the t-dimensional subspace with $\{\alpha_1, \ldots, \alpha_t\}$ as its basis. We have $\Re \subseteq W$.

From the discussions preceding the theorem, we have

$$MM^T = \begin{bmatrix} D & 0 & \cdots & 0 \\ 0 & D & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & D \end{bmatrix}$$

where 0 denotes the zero matrix and $D = (\Delta(\alpha_{i+j}))$, both of order 2^t, and $i, j = 0, 1, \ldots, 2^t - 1$. Now let $\lambda_1, \ldots, \lambda_{2^t}$ be the eigenvalues of D. Then the collection of the eigenvalues of MM^T consists of 2^{n-t} copies of $\lambda_1, \ldots, \lambda_{2^t}$.

An interpretation of (1) is that the two matrices MM^T and $\mathrm{diag}(\langle \xi, \ell_0 \rangle^2, \ldots, \langle \xi, \ell_{2^n-1} \rangle^2)$ are similar, since $2^{-n} H_n H_n = I$, where I denotes the identity matrix of order 2^n. In addition it is easy to see that $\{\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2\}$ is also the collection of eigenvalues of MM^T.

Thus $\lambda_i \geqq 0$ for all $1 \leqq i \leqq 2^t$. Also we have

$$2^{n-t}(\lambda_1 + \cdots + \lambda_{2^t}) = \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2.$$

By Parseval's equation (p. 416, (MacWilliams & Sloane, 1977)), we have

$$\sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2 = 2^{2n}.$$

Hence

$$\lambda_1 + \cdots + \lambda_{2^t} = 2^{n+t}.$$

Since each $\lambda_i \geqq 0$, we have

$$\lambda_i \leqq 2^{n+t}$$

for $i = 1, \ldots, 2^t$, or equivalently

$$\langle \xi, \ell_j \rangle^2 \leqq 2^{n+t}$$

for $j = 0, 1, \ldots, 2^n - 1$. Thus

$$|\langle \xi, \ell_j \rangle| \leqq 2^{\frac{1}{2}(n+t)}$$

for $j = 0, 1, \ldots, 2^n - 1$.

Lemma 6 of (Seberry *et al.*, 1994a) states that the distance between two functions f_1 and f_2 on V_n can be expressed as $d(f_1, f_2) = 2^{n-1} - \frac{1}{2}\langle \xi_{f_1}, \xi_{f_2} \rangle$, where ξ_{f_1} and ξ_{f_2} are the sequences of f_1 and f_2 respectively. ¿From this result it immediately follows that the nonlinearity of f satisfies $N_f \geqq 2^{n-1} - 2^{\frac{1}{2}(n+t)-1}$.

In the more general case where $\{\alpha_1, \ldots, \alpha_t\}$ are not t linearly independent vectors in $\Re$, we can apply a nonsingular linear transformation A on the input coordinates of f so that the resulting function $g(x) = f(xA)$ has $\{\alpha_1, \ldots, \alpha_t\}$ as t linearly independent vectors in the set $\Re$ associated with g. The nonlinearity of g satisfies $N_g \geqq 2^{n-1} - 2^{\frac{1}{2}(n+t)-1}$. It has been well-known that a nonsingular linear transformation on the input coordinates of a function does not alter its nonlinearity (see for instance (Meier & Staffelbach, 1990) or Lemma 10 of (Seberry *et al.*, 1994a)). Consequently $N_f = N_g \geqq 2^{n-1} - 2^{\frac{1}{2}(n+t)-1}$. This completes the proof. □

It was observed by Nyberg in Proposition 3 of (Nyberg, 1992) (see also a detailed discussion in (Seberry *et al.*, 1994b)) that knowing the linearity dimension, say ℓ, of a function f on V_n, the nonlinearity of the function can be expressed as $N_f = 2^\ell N_r$,

where N_r is the nonlinearity of a function obtained by restricting f on an $(n-\ell)$-dimensional subspace of V_n. Therefore, in a sense Theorem 1 is complementary to Proposition 3 of (Nyberg, 1992).

In the next section we discuss an interesting special case where $|\Re| = 2$. More general cases where $|\Re| > 2$, which need a very different proof technique, will be fully discussed in Sections 4 and 5.

3 Functions with $|\Re| = 2$

Since $\Re$ consists of two vectors, a zero and a nonzero, it forms a one-dimensional subspace of V_n. The following result on splitting a power of 2 into two squares will be used in later discussions.

Lemma 1 *Let $n \geqq 2$ be a positive integer and $2^n = p^2 + q^2$ where both $p \geqq 0$ and $q \geqq 0$ are integers. Then $p = 2^{\frac{1}{2}n}$ and $q = 0$ when n is even, and $p = q = 2^{\frac{1}{2}(n-1)}$ when n is odd.*

Proof. We first prove that if $n \geqq 2$ and $2^n = p^2 + q^2$ then both p and q are even. Assume for contradiction that $p = 2p_1 + 1$ and $q = 2q_1 + a$ where p_1 and q_1 are positive integers and a is 0 or 1. Then $2^n = p^2 + q^2$ can be written as $2^n = 4N + 1$ or $2^n = 4N + 2$ for a positive integer N. This contradicts to either the fact that 2^n is even or the fact that 2^n is divisible by 4.

We now prove the lemma by induction. It is easy to verify that the lemma is true for $n = 2, 3$. Suppose that the lemma is true for $3 \leqq n \leqq n_0$. Consider

$$2^{n_0+1} = p^2 + q^2.$$

Since both p and q are even, we can write $p = 2p_1$ and $q = 2q_1$. Thus

$$2^{n_0-1} = p_1^2 + q_1^2.$$

Note that $n_0 + 1$ is even (odd) if and only if $n_0 - 1$ is even (odd). By the induction assumption, the lemma is true for $n = n_0 + 1$. □

Now we prove

Theorem 2 *If f, a function on V_n, satisfies the propagation criterion with respect to all but two (a zero and a nonzero) vectors in V_n, then*

(i) n must be odd,

(ii) the nonzero vector where the propagation criterion is not satisfied must be a linear structure of f and

(iii) the nonlinearity of f satisfies $N_f \geqq 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.

Proof. Let β be the vector where the propagation criterion is not satisfied. We can always find a nonsingular matrix of order n over $GF(2)$, say B, such that $\beta B = \alpha_1$, where $\alpha_1 = (0, 0, \ldots, 1)$. The new function g, defined by $g(x) = f(xB)$, has the same nonlinearity as that of f, and satisfies the propagation criterion with respect to every nonzero vector except for α_1. In addition, β is a linear structure of f if and only if α_1 is a linear structure of g.

Compare the first row of the two sides of (1), we have

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

where α_j is the jth vector in V_n in the ascending alphabetical order. Equivalently we have

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

Note that $\Delta(\alpha_j) = 0$ if $j \neq 0, 1$. Thus (2) is specialized as

$$(\Delta(\alpha_0), \Delta(\alpha_1), 0, \ldots, 0) H_n = (\langle \xi, \ell_0 \rangle^2, \ldots, \langle \xi, \ell_{2^n-1} \rangle^2) \tag{3}$$

¿From the construction of H_n, the first and the second columns of H_n are $(1, 1, \ldots, 1)^T$ and $(1, -1, 1, -1, \ldots, 1, -1)^T$ respectively. From (3), we have

$$\Delta(\alpha_0) + \Delta(\alpha_1) = \langle \xi, \ell_0 \rangle^2$$

and

$$\Delta(\alpha_0) - \Delta(\alpha_1) = \langle \xi, \ell_1 \rangle^2.$$

Note that $\Delta(\alpha_0) = 2^n$. Hence

$$2^n + \Delta(\alpha_1) = \langle \xi, \ell_0 \rangle^2, \tag{4}$$

$$2^n - \Delta(\alpha_1) = \langle \xi, \ell_1 \rangle^2. \tag{5}$$

¿From (4) and (5), we have

$$2^{n+1} = \langle \xi, \ell_0 \rangle^2 + \langle \xi, \ell_1 \rangle^2. \tag{6}$$

We now prove that n must be odd. Suppose n is even. By Lemma 1,

$$\langle \xi, \ell_0 \rangle^2 = \langle \xi, \ell_1 \rangle^2 = 2^n.$$

¿From (4) or (5), $\Delta(\alpha_1) = 0$. This contradicts the fact that f does not satisfy the propagation characteristic with respect to α_1. Thus n must be odd, i.e. the part (i) of the theorem is true.

Since n is odd, from (6) and Lemma 1 we have $\langle \xi, \ell_0 \rangle^2 = 2^{n+1}$ or 0.

Case 1: $\langle \xi, \ell_0 \rangle^2 = 2^{n+1}$ and hence $\langle \xi, \ell_1 \rangle^2 = 0$. ¿From (4) or (5), we have $\Delta(\alpha_1) = 2^n$.

Case 2: $\langle \xi, \ell_0 \rangle^2 = 0$ and hence $\langle \xi, \ell_1 \rangle^2 = 2^{n+1}$. Again from (4) or (5), we have $\Delta(\alpha_1) = -2^n$.

In both cases, α_1 is a linear structure of g. Thus $\beta = \alpha_1 B^{-1}$ is a linear structure of f. This proves (ii) of the theorem.

Using Theorem 1 with $t = 1$, we obtain $N_f = N_g \geqq 2^{n-1} - 2^{\frac{1}{2}(n-1)}$, i.e. the part (iii) of the theorem. □

A further examination of the proof for Theorem 2 reveals that a function with $|\Re| = 2$ has a very simple structure as described below.

Corollary 1 *A function f on V_n satisfies the propagation criterion with respect to all but two (a zero and a nonzero) vectors in V_n, if and only if there exists a nonsingular linear matrix of order n over $GF(2)$, say B, such that $g(x) = f(Bx)$ can be written as*

$$g(x) = cx_n \oplus h(x_1, \ldots, x_{n-1})$$

where h is a bent function on V_{n-1} and c is a constant in $GF(2)$.

Proof. ¿From the proof of Theorem 2, one can see that $g(x) = f(xB)$ has an unique nonzero linear structure $\alpha_1 = (0, 0, \ldots, 1)$ and hence it can be written as

$$g(x) = cx_n \oplus h(x_1, \ldots, x_{n-1}), \tag{7}$$

where c is a constant from $GF(2)$. By Proposition 3 of (Nyberg, 1992), $N_g \geqq 2N_h$. On the other hand, by the part (iii) of Theorem 2, $N_g \geqq 2^{n-1} - 2^{\frac{1}{2}(n-1)}$. Thus $N_h \geqq 2^{n-2} - 2^{\frac{1}{2}(n-1)-1}$. This proves that h, a function on V_{n-1}, achieves the maximum nonlinearity and hence it is bent (see also (MacWilliams & Sloane, 1977) or Lemma 4 of (Seberry *et al.*, 1994a)).

Conversely, suppose that g can be expressed as (7). Since h is a bent function on V_{n-1}, $\alpha_1 = (0, 0, \ldots, 1)$ is the only nonzero linear structure of g, and hence $\beta = \alpha_1 B^{-1}$ is the only nonzero linear structure of the original function f. □

By Theorem 2 and Corollary 1, functions on V_n that satisfy the propagation criterion with respect to all but two vectors in V_n exist only if n is odd, and such a function can always be viewed as being obtained by repeating twice a bent function on V_{n-1} (subject to a nonsingular linear transformation on the input coordinates).

When $\Re$ has more than two vectors, it does not necessarily form a linear subspace of V_n. Therefore discussions presented in this section do not directly apply to the more general case. Nevertheless, using a different technique, we show in the next section a *significant* result on the structure of $\Re$, namely, *the nonzero vectors in $\Re$ with $|\Re| > 2$ are linearly dependent.*

4 Linear Dependence in $\Re$

The following result on vectors will be used in the proof of the main result in this section.

Lemma 2 *Let $\psi_1, \ldots, \psi_k$ be linear functions on V_n which are linearly independent. Set*

$$Q = \begin{bmatrix} \sigma_1 \\ \vdots \\ \sigma_k \end{bmatrix} \quad \text{and} \quad P = \begin{bmatrix} \ell_1 \\ \vdots \\ \ell_k \end{bmatrix}$$

where σ_i is the truth table and ℓ_i is the sequence of ψ_i, $i = 1, \ldots, k$. Then

(i) each vector in V_k appears as a column in Q precisely 2^{n-k} times and

(ii) each k-dimensional $(1, -1)$-vector appears as a column in P precisely 2^{n-k} times.

Proof. Note that (i) and (ii) are equivalent. Clearly, any nonzero linear combination of $\varphi_1, \ldots, \varphi_k$ is a nonzero linear function and thus it is balanced. Consequently, this lemma is equivalent to Lemma 7 of (Seberry *et al.*, 1994b). □

Next we show the linear dependence of vectors in $\Re$.

Theorem 3 *Suppose that f, a function on V_n, satisfies the propagation criterion with respect to all but $k+1$ vectors $0, \beta_1, \ldots, \beta_k$ in V_n, where $k > 1$. Then $\beta_1, \ldots, \beta_k$ are linearly dependent, namely, there exist k constants $c_1, \ldots, c_k \in GF(2)$, not all of which are zeros, such that $c_1\beta_1 \oplus \cdots \oplus c_k\beta_k = 0$.*

Proof. The theorem is obviously true if $k > n$. Now we prove the theorem for $k \leqq n$ by contradiction. Assume that $\beta_1, \ldots, \beta_k$ are linearly independent. Let ξ be the sequence of f.

Let P be a submatrix that consists of the 0th, β_1th, ..., β_kth rows of H_n. Set $a_j^2 = \langle \xi, \ell_j \rangle^2$, $j = 0, 1, \ldots, 2^n - 1$. Note that $\Delta(\alpha) = 0$ if $\alpha \notin \{0, \beta_1, \ldots, \beta_k\}$. Hence (2) can be written as

$$(\Delta(0), \Delta(\beta_1), \ldots, \Delta(\beta_k))P = (a_0^2, a_1^2, \ldots, a_{2^n-1}^2) \tag{8}$$

where 0 in (8) is identical to α_0 in (2).

Write $P = (p_{ij})$, $i = 0, 1, \ldots k$, $j = 0, 1, \ldots, 2^n - 1$. As the top row of P is $(1, 1, \ldots, 1)$, a_j^2 in (8) can be expressed as

$$\Delta(0) + \sum_{i=1}^{k} p_{ij}\Delta(\beta_i) = a_j^2$$

$j = 0, 1, \ldots, 2^n - 1$. Let P^* be the submatrix of P obtained by removing the top row from P. As was mentioned earlier, the β_ith row of H_n is the sequence of a

linear function defined by $\psi_i(x) = \langle \beta_i, x \rangle$ (see Lemma 2 of (Seberry *et al.*, 1994a)). The linear independence of the vectors $\beta_1, \ldots, \beta_k$ implies the linear independence of the linear functions $\psi_1(x) = \langle \beta_1, x \rangle, \ldots, \psi_k(x) = \langle \beta_k, x \rangle$. By Lemma 2, each k-dimensional $(1, -1)$-vector appears in P^*, as a column vector, precisely 2^{n-k} times. Thus for each fixed j there exists a j_0 such that $(p_{1j}, \ldots, p_{kj}) = -(p_{1j_0}, \ldots, p_{kj_0})$ and hence

$$\Delta(0) + \sum_{i=1}^{k} p_{ij_0} \Delta(\beta_i) = a_{j_0}^2.$$

Adding together both sides of the above two equations, we have $2\Delta(0) = a_j^2 + a_{j_0}^2$. Hence $a_j^2 + a_{j_0}^2 = 2^{n+1}$. There are two cases to be considered: n even and n odd.

Case 1: n is even. By Lemma 1, $a_j^2 = a_{j_0}^2 = 2^n$. This implies that $\langle \xi, \ell_j \rangle = 2^n$ for any fixed j, which in turn implies that f is bent and that it satisfies the propagation criterion with respect to every nonzero vector in V_n (see also the equivalent statements about bent functions in Section 1). This clearly contradicts the fact that f does not satisfy the propagation criterion with respect to $\beta_1, \ldots, \beta_k$.

Case 2: n is odd. Again by Lemma 1, $a_j^2 = 2^{n+1}$ or 0. If $a_j^2 = 2^{n+1}$, then $\sum_{i=1}^{k} p_{ij} \Delta(\beta_i) = 2^n$. Otherwise if $a_j^2 = 0$, then $\sum_{i=1}^{k} p_{ij} \Delta(\beta_i) = -2^n$. Thus we can write

$$\sum_{i=1}^{k} p_{ij} \Delta(\beta_i) = c_j 2^n \tag{9}$$

where $c_j = \pm 1$, $j = 0, 1, \ldots, 2^n - 1$. For each fixed j rewrite (9) as

$$p_{1j} \Delta(\beta_1) + \sum_{i=2}^{k} p_{ij} \Delta(\beta_i) = c_j 2^n.$$

From Lemma 2, there exists a j_1 such that $p_{ij_1} = p_{1j}$ and $p_{ij_1} = -p_{ij}$, $i = 2, \ldots, k$. Note that

$$p_{1j_1} \Delta(\beta_1) + \sum_{i=2}^{k} p_{ij_1} \Delta(\beta_i) = c_{j_1} 2^n.$$

Adding the above two equations together, we have

$$2p_{1j} \Delta(\beta_1) = (c_j + c_{j_1}) 2^n.$$

As f does not satisfy the propagation with respect to β_1, we have $\Delta(\beta_1) \neq 0$ and $c_j + c_{j_0} \neq 0$. This implies $c_j + c_{j_0} = \pm 2$, which proves that $\Delta(\beta_1) = \pm 2^n$. By the same reasoning, we can prove that $\Delta(\beta_j) = \pm 2^n$, $j = 2, \ldots, k$. Thus we can write

$$(\Delta(\beta_1), \ldots, \Delta(\beta_k)) = 2^n (b_1, \ldots, b_k)$$

where each $b_j = \pm 1$. Using Lemma 2, there exists an s such that

$$(p_{1s}, \ldots, p_{ks}) = (b_1, \ldots, b_k).$$

This gives us

$$\sum_{i=1}^{k} p_{is}\Delta(\beta_i) = \sum_{i=1}^{k} b_i\Delta(\beta_i) = \sum_{i=1}^{k} b_i b_i 2^n = k2^n. \tag{10}$$

Since $k > 1$, (10) contradicts (9).

Summarizing Cases 1 and 2, we conclude that the assumption that $\beta_1, \ldots, \beta_k$ are linearly independent is wrong. This proves the theorem. □

We believe that Theorem 3 is of significant importance, as it reveals for the first time the interdependence among the vectors where the propagation criterion is not satisfied by f. Of particular interest is the case when $\Re = \{0, \beta_1, \ldots, \beta_k\}$ forms a linear subspace of V_n. Recall that linear structures form a linear subspace. Therefore, when $\Re$ is a subspace, a nonzero vector in $\Re$ is a linear structure if and only if all other nonzero vectors are linear structures of f.

In the next section we examine the case when $|\Re| = 3$ or 4.

5 Functions with $|\Re| = 3$ or 4

First we consider the case when $|\Re| = 3$. Note that $\Re$ contains two nonzero vectors. Since two distinct nonzero vectors can not be linearly dependent, by Theorem 3 we have

Theorem 4 *There exists no function that does not satisfy the propagation criterion with respect to only three vectors.*

Next we consider the case when $|\Re| = 4$. Similarly to the case of $|\Re| = 2$, the first step we take is to introduce a result on splitting a power of 2 into four squares.

Lemma 3 *Let $n \geqq 3$ be a positive integer and $2^n = \sum_{j=1}^{4} p_j^2$ where each $p_j \geqq 0$ is an integer. Then*

(i) $p_1^2 = p_2^2 = 2^{n-1}$, $p_3 = p_4 = 0$, *if n is odd;*

(ii) $p_1^2 = 2^n$, $p_2 = p_3 = p_4 = 0$ *or* $p_1^2 = p_2^2 = p_3^2 = p_4^2 = 2^{n-2}$, *if n is even.*

Proof. We first prove that if $n \geqq 3$ and $2^n = \sum_{j=1}^{4} p_j^2$ then each p_j must be even. Write $p_j = 2t_j + a_j$, where $a_j = 0$ or 1, $j = 1, 2, 3, 4$. Then we have $2^n = \sum_{j=1}^{4}(4t_j^2 + 4t_j a_j + a_j^2)$ or equivalently

$$2^n = \sum_{j=1}^{4} a_j^2 + 4\sum_{j=1}^{4} t_j(t_j + a_j). \tag{11}$$

Note that the left hand side of (11) is always even. If $\{a_1, a_2, a_3, a_4\}$ contains one or three ones, then the right hand side of (11) is odd, which is something that can not stand in parallel with the left hand side of (11). Otherwise, if $\{a_1, a_2, a_3, a_4\}$ contains

two or four ones, then by dividing both sides of (11) by 2 or 4, and also noting that $t(t+a)$ is even for $a=1$, we obtain the same contradiction. Hence none of the four numbers a_1, a_2, a_3, a_4 can take the value one, i.e., p_1, p_2, p_3, p_4 must be even.

Next we prove the lemma by induction. It is easy to verify the lemma for $n = 3, 4$. Suppose that the lemma is true for $3 \leqq n \leqq n_0$. Consider

$$2^{n_0+1} = \sum_{j=1}^{4} p_j^2.$$

Since p_j is even, we can write $p_j = 2t_j$. Thus

$$2^{n_0-1} = \sum_{j=1}^{4} t_j^2.$$

Note that $n_0 + 1$ is even (odd) if and only if $n_0 - 1$ is even (odd). By the induction assumption, the lemma is true for $n = n_0 + 1$. □

Now we can prove a key result on the case of $|\Re| = 4$.

Theorem 5 *If f, a function on V_n, satisfies the propagation criterion with respect to all but four vectors (0, $\beta_1, \beta_2, \beta_3$) in V_n, Then*

(i) $\Re = \{0, \beta_1, \beta_2, \beta_3\}$ *forms a two-dimensional linear subspace of* V_n,

(ii) n *must be even,*

(iii) β_1, β_2 *and* β_3 *must be linear structures of* f,

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

Proof. By Lemma 3, β_1, β_2 and β_3 are linearly dependent. The only possibility is $\beta_1 \oplus \beta_2 \oplus \beta_3 = 0$. Since β_1, β_2 and β_3 are mutually distinct, $\Re$ is a two-dimensional linear subspace of V_n. This proves the part (i).

Let B be a nonsingular matrix of order n on $GF(2)$ such that $\beta_i B = \alpha_i$, where $i = 1, 2, 3$ and α_i is the ith vector in V_n according to the ascending alphabetical order. Let $g(x) = f(xB)$. Then g has the same nonlinearity as f and the only vectors where the propagation criterion is not satisfied by g are $\{\alpha_0, \alpha_1, \alpha_2, \alpha_3\}$.

For g, the matrix D in the proof of Theorem 1 has the following form:

$$D = \begin{bmatrix} \Delta(\alpha_0) & \Delta(\alpha_1) & \Delta(\alpha_2) & \Delta(\alpha_3) \\ \Delta(\alpha_1) & \Delta(\alpha_2) & \Delta(\alpha_3) & \Delta(\alpha_0) \\ \Delta(\alpha_2) & \Delta(\alpha_3) & \Delta(\alpha_0) & \Delta(\alpha_1) \\ \Delta(\alpha_3) & \Delta(\alpha_0) & \Delta(\alpha_1) & \Delta(\alpha_2) \end{bmatrix}$$

Compare the first row of the two sides of (1), we have

$$(\Delta(\alpha_0), \Delta(\alpha_1), \Delta(\alpha_2), \Delta(\alpha_3), 0, \ldots, 0) = 2^{-n}(\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2) H_n$$

and hence

$$(\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2) = (\Delta(\alpha_0), \Delta(\alpha_1), \Delta(\alpha_2), \Delta(\alpha_3), 0, \ldots, 0) H_n. \tag{12}$$

Recall that the first, the second, the third and the fourth columns of H_n have the following forms:

$$\begin{aligned}
&(1,1,1,1,\ldots,1,1,1,1)^T,\\
&(1,-1,1,-1,\ldots,1,-1,1,-1)^T,\\
&(1,1,-1,-1,\ldots,1,1,-1,-1)^T,\\
&(1,-1,-1,1,\ldots,1,-1,-1,1)^T
\end{aligned}$$

By noting the first four elements of each of the four columns, we have

$$\begin{aligned}
\langle \xi, \ell_0 \rangle^2 &= \Delta(\alpha_0) + \Delta(\alpha_1) + \Delta(\alpha_2) + \Delta(\alpha_3),\\
\langle \xi, \ell_1 \rangle^2 &= \Delta(\alpha_0) - \Delta(\alpha_1) + \Delta(\alpha_2) - \Delta(\alpha_3),\\
\langle \xi, \ell_2 \rangle^2 &= \Delta(\alpha_0) + \Delta(\alpha_1) - \Delta(\alpha_2) - \Delta(\alpha_3),\\
\langle \xi, \ell_3 \rangle^2 &= \Delta(\alpha_0) - \Delta(\alpha_1) - \Delta(\alpha_2) + \Delta(\alpha_3).
\end{aligned}$$

This can be translated into

$$\begin{aligned}
\Delta(\alpha_0) &= \frac{1}{4}(\langle \xi, \ell_0 \rangle^2 + \langle \xi, \ell_1 \rangle^2 + \langle \xi, \ell_2 \rangle^2 + \langle \xi, \ell_3 \rangle^2),\\
\Delta(\alpha_1) &= \frac{1}{4}(\langle \xi, \ell_0 \rangle^2 - \langle \xi, \ell_1 \rangle^2 + \langle \xi, \ell_2 \rangle^2 - \langle \xi, \ell_3 \rangle^2),\\
\Delta(\alpha_2) &= \frac{1}{4}(\langle \xi, \ell_0 \rangle^2 + \langle \xi, \ell_1 \rangle^2 - \langle \xi, \ell_2 \rangle^2 - \langle \xi, \ell_3 \rangle^2),\\
\Delta(\alpha_3) &= \frac{1}{4}(\langle \xi, \ell_0 \rangle^2 - \langle \xi, \ell_1 \rangle^2 - \langle \xi, \ell_2 \rangle^2 + \langle \xi, \ell_3 \rangle^2).
\end{aligned}$$

Note that $\Delta(\alpha_0) = 2^n$. Hence

$$\langle \xi, \ell_0 \rangle^2 + \langle \xi, \ell_1 \rangle^2 + \langle \xi, \ell_2 \rangle^2 + \langle \xi, \ell_3 \rangle^2 = 2^{n+2}.$$

Now we show that n is even. Suppose that n is odd. By Lemma 3, we have $\langle \xi, \ell_0 \rangle^2 = \langle \xi, \ell_1 \rangle^2 = 2^{n+1}$, $\langle \xi, \ell_2 \rangle^2 = \langle \xi, \ell_3 \rangle^2 = 0$. Thus $\Delta(\alpha_1) = 0$. This contradicts the fact that g does not satisfies the propagation criterion with respect to α_1. This proves the part (ii), namely, n must be even.

Next we show that the part (iii) is true. Since n is even, by Lemma 3, we need to consider the following two cases.

Case 1: $\langle \xi, \ell_j \rangle^2 = 2^n$, $j = 0, 1, 2, 3$. In this case we have $\Delta(\alpha_j) = 0$, $j = 0, 1, 2, 3$, contradicting the fact that g does not satisfies the propagation criterion with respect to the four vectors.

So we are left with Case 2: one of the four quantities $\langle \xi, \ell_0 \rangle^2$, $\langle \xi, \ell_1 \rangle^2$, $\langle \xi, \ell_2 \rangle^2$ and $\langle \xi, \ell_3 \rangle^2$ is 2^{n+2}, and the other three are all zero. Without loss of generality, suppose that $\langle \xi, \ell_1 \rangle^2 = 2^{n+2}$ and $\langle \xi, \ell_j \rangle^2 = 0$, $j = 0, 2, 3$. Then we have $\Delta(\alpha_0) = \Delta(\alpha_2) = 2^n$, $\Delta(\alpha_1) = \Delta(\alpha_3) = -2^n$. This implies that α_1, α_2 and α_3 all are linear structures of g.

Hence β_1, β_2 and β_3 must be linear structures of the original function f. This show that the part (iii) holds.

Using Theorem 1 with $t = 2$ we have $N_f = N_g \geqq 2^{n-1} - 2^{\frac{1}{2}n}$. □

As a result we have

Corollary 2 *A function f on V_n satisfies the propagation criterion with respect to all but four vectors in V_n if and only if there exists a nonsingular linear matrix of order n over $GF(2)$, say B, such that $g(x) = f(Bx)$ can be written as*

$$g(x) = c_1 x_{n-1} \oplus c_2 x_n \oplus h(x_1, \ldots, x_{n-2})$$

where c_1 and c_2 are constants in $GF(2)$, and h is a bent function on V_{n-2}.

The proof of Corollary 2 is similar to that of Corollary 1.

In (Seberry *et al.*, 1994a), it has been shown that repeating twice or four times a bent function on V_n, n even, results in a function on V_{n-1} or V_{n-2} that satisfies the propagation criterion with respect to all but two or four vectors in V_{n-1} or V_{n-2}. Combining Corollaries 2 and 1 with results shown in (Seberry *et al.*, 1994a), we conclude that *the methods of repeating bent functions presented in (Seberry* et al., *1994a) generate all the functions that satisfy the propagation criterion with respect to all but two or four vectors.*

6 Final Remarks

We have presented a quantitative relationship between propagation characteristic and nonlinearity. We have also completely decided the structures and construction methods of cryptographic functions that satisfy the propagation criterion with respect to all but two or four vectors.

An implication of Theorems 2 and 5 is that if a function satisfies the propagation criterion with respect to almost all vectors, then the function might have very bad avalanche effect at the rest of the vectors in the space. This property may be undesirable in designing cryptographic functions including S-boxes or substitution boxes. This subject will be treated in a forthcoming paper.

Acknowledgments

The first author was supported in part by the Australian Research Council under the reference numbers A49130102, A49131885 and A49232172, the second author by A49130102, and the third author by A49232172. All authors were supported by a University of Wollongong Research Program grant and the first two by ATERB C010/058.

References

Adams, C. M., & Tavares, S. E. 1990. Generating and Counting binary bent sequences. *IEEE Transactions on Information Theory*, **IT-36 No. 5**, 1170–1173.

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

Evertse, J.-H. 1988. Linear Structures in Blockciphers. *Pages 249–266 of: Advances in Cryptology - EUROCRYPT'87*, vol. 304, Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, New York.

MacWilliams, F. J., & Sloane, N. J. A. 1977. *The Theory of Error-Correcting Codes*. New York: North-Holland.

Meier, W., & Staffelbach, O. 1990. Nonlinearity Criteria For Cryptographic Functions. *Pages 549–562 of: Advances in Cryptology - EUROCRYPT'89*, vol. 434, Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, New York.

Nyberg, K. 1992. On the construction of highly nonlinear permutations. *In: Advances in Cryptology - EUROCRYPT'92*. Springer-Verlag, Berlin, Heidelberg, New York. to appear.

Preneel, B., Govaerts, R., & Vandewalle, J. 1991a. Boolean Functions Satisfying Higher Order Propagation Criteria. *Pages 141–152 of: Advances in Cryptology - EUROCRYPT'91*, vol. 547, Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, New York.

Preneel, B., Leekwick, W. V., Linden, L. V., Govaerts, R., & Vandewalle, J. 1991b. Propagation Characteristics of Boolean Functions. *Pages 155–165 of: Advances in Cryptology - EUROCRYPT'90*, vol. 437, Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, New York.

Seberry, J., Zhang, X. M., & Zheng, Y. 1994a. *Nonlinearity and Propagation Characteristics of Balanced Boolean Functions*. To appear in *Information and Computation*.

Seberry, J., Zhang, X. M., & Zheng, Y. 1994b. *Relationships among Nonlinearity Criteria*. Presented at *EUROCRYPT'94*.

Webster, A. F. 1985. *Plaintext/Ciphertext Bit Dependencies in Cryptographic System*. Master's Thesis, Department of Electrical Engineering, Queen's University, Ontario, Cannada.

Webster, A. F., & Tavares, S. E. 1986. On the Designs of S-Boxes. *Pages 523–534 of: Advances in Cryptology - CRYPTO'85*, vol. 219, Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, New York.

Yarlagadda, R., & Hershey, J. E. 1989. Analysis and synthesis of bent sequences. *IEE Proceeding (Part E)*, **136**, 112–123.