Strong Linear Dependence and Unbiased Distribution of Non-propagative Vectors

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

[1] School of Comp & Info Tech, Monash University, McMahons Road, Frankston,
Melbourne, VIC 3199, Australia. E-mail: yuliang@pscit.monash.edu.au
URL: http://www.pscit.monash.edu.au/links/

[2] School of Info Tech & Comp Sci, the University of Wollongong, Wollongong
NSW 2522, Australia. E-mail: xianmo@cs.uow.edu.au

Abstract. This paper proves (i) in any $(n-1)$-dimensional linear subspace, the non-propagative vectors of a function with n variables are linearly dependent, (ii) for this function, there exists a non-propagative vector in any $(n-2)$-dimensional linear subspace and there exist three non-propagative vectors in any $(n-1)$-dimensional linear subspace, except for those functions whose nonlinearity takes special values.

Key Words:

Cryptography, Boolean Function, Propagation, Nonlinearity.

1 Introduction

In examining the nonlinearity properties of a function f with n variables, it is important to understand $\Re_f$, the set of so-called non-propagative vectors where f does not satisfy the propagation criterion. In this work, we are concerned with both $\#\Re_f$ (the number of non-propagative vectors in $\Re_f$) and the distribution of $\Re_f$. More specifically, we prove two properties of $\Re$. One is called the strong linear dependence and the other the unbiased distribution, of $\Re$.

The strong linear dependence property states that if W is a $(n-1)$-dimensional linear subspace satisfying $\#(\Re \cap W) \geq 4$, then the non-zero vectors in $\Re \cap W$ are linearly dependent. This improves a previously known result. The unbiased distribution property says that any function f with n variables, except for those whose nonlinearity takes the special value of $2^{n-1} - 2^{\frac{1}{2}(n-1)}$, $2^{n-1} - 2^{\frac{1}{2}n}$ or $2^{n-1} - 2^{\frac{1}{2}n-1}$, fulfills the condition that every $(n-2)$-dimensional linear subspace contains a non-zero vector in $\Re_f$ and every $(n-1)$-dimensional linear subspace contains at least three non-zero vectors in $\Re_f$. In special cases, $\#(\Re \cap W)$ may significantly effect other cryptographic properties of a function. The strong linear dependence and the unbiased distribution are helpful for the design of cryptographic functions as these conclusions provide more information on the number and the status of non-propagative vectors in any $(n-1)$-dimensional linear subspace.

2 Cryptographic Criteria of Boolean Functions

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

Given two sequences $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$, their *component-wise product* is defined by $\tilde{a} * \tilde{b} = (a_1 b_1, \cdots, a_m b_m)$. In particular, if $m = 2^n$ and $\tilde{a}$, $\tilde{b}$ are the sequences of functions f and g on V_n respectively, then $\tilde{a} * \tilde{b}$ is the sequence of $f \oplus g$ where $\oplus$ denotes the addition in $GF(2)$.

Let $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$ be two sequences or vectors, the *scalar product* of $\tilde{a}$ and $\tilde{b}$, denoted by $\langle \tilde{a}, \tilde{b} \rangle$, is defined as the sum of the component-wise multiplications. In particular, when $\tilde{a}$ and $\tilde{b}$ are from V_m, $\langle \tilde{a}, \tilde{b} \rangle = a_1 b_1 \oplus \cdots \oplus a_m b_m$, where the addition and multiplication are over $GF(2)$, and when $\tilde{a}$ and $\tilde{b}$ are $(1,-1)$-sequences, $\langle \tilde{a}, \tilde{b} \rangle = \sum_{i=1}^{m} a_i b_i$, where the addition and multiplication are over the reals.

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 $c = 0$.

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

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

Let ℓ_i, $0 \le i \le 2^n - 1$, be the i row of H_n. It is known that ℓ_i is the sequence of a linear function $\varphi_i(x)$ defined by the scalar product $\varphi_i(x) = \langle \alpha_i, x \rangle$, where α_i is the ith vector in V_n according to the ascending alphabetical order.

The *Hamming weight* of a $(0,1)$-sequence ξ, denoted by $W(\xi)$, 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 $x = (x_1, \ldots, x_n)$.

Definition 1. *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.*

The following characterisations of nonlinearity will be useful (for a proof see for instance [2]).

Lemma 1. *The nonlinearity of f on V_n can be expressed by*

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

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

Definition 2. *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*

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

the scalar product of $\xi(0)$ and $\xi(\alpha)$. $\varDelta(\alpha)$ is called the auto-correlation of f with a shift α. Write

$$\varDelta_M = \max\{|\varDelta(\alpha)||\alpha \in V_n, \alpha \ne 0\}$$

We omit the subscript of $\varDelta_f(\alpha)$ if no confusion occurs.

Definition 3. *Let f be a function on V_n. We say that f satisfies 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. Furthermore f is said to satisfy the* propagation criterion of degree k *if it satisfies the propagation criterion with respect to every non-zero vector α whose Hamming weight is not larger than k (see [3]).*

The *strict avalanche criterion (SAC)* [5] is the same as the propagation criterion of degree one.

Obviously, $\varDelta(\alpha) = 0$ if and only if $f(x) \oplus f(x \oplus \alpha)$ is balanced, i.e., f satisfies the propagation criterion with respect to α.

Definition 4. *Let f be a function on V_n. $\alpha \in V_n$ is called a* linear structure *of f if $|\varDelta(\alpha)| = 2^n$ (i.e., $f(x) \oplus f(x \oplus \alpha)$ is a constant).*

For any function f, $\varDelta(\alpha_0) = 2^n$, 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*. It is also well-known that if f has non-zero linear structures, then there exists a nonsingular $n \times n$ matrix B over $GF(2)$ such that $f(xB) = g(y) \oplus h(z)$, where $x = (y, z)$, $y \in V_p$, $z \in V_q$, g is a function on V_p that has no non-zero linear structures, and h is an affine function on V_q.

The following lemma is the re-statement of a relation proved in Section 2 of [1].

Lemma 2. *For every function f on V_n, we have*

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

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

The balance and the nonlinearity are necessary in most cases. The propagation or especially the SAC, is an important cryptographic criterion.

3 Introduction to $\Re$

Notation 1. *Let f be a function on V_n. Set $\Re_f = \{\alpha \mid \Delta(\alpha) \neq 0,\ \alpha \in V_n\}$, $\Delta_M = \max\{|\Delta(\alpha)| | \alpha \in V_n,\ \alpha \neq 0\}$.*

We simply write $\Re_f$ as $\Re$ if no confusion occurs. It is easy to verify that $\#\Re$ and Δ_M are invariant under any nonsingular linear transformation on the variables, where # denotes the cardinal number of a set.

$\#\Re$ and the distribution of $\Re$ reflects the propagation characteristics, while Δ_M forecasts the avalanche property of the function. Therefore information on $\Re$ and Δ_M is useful in determining important cryptographic characteristics of f. Usually, small $\#\Re$ and Δ_M are desirable.

Definition 5. *A function f on V_n is called a* bent function *[4] 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 highest possible nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$. The algebraic degree of bent functions on V_n is at most $\frac{1}{2}n$ [4]. From [4] and Parseval's equation, we have the following:

Theorem 1. *Let f be a function on V_n. Then the following statements are equivalent: (i) f is bent, (ii) $\#\Re = 1$, (iii) $\Delta_M = 0$, (iv) the nonlinearity of f, N_f, satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}n-1}$, (v) the matrix of f is an Hadamard matrix.*

The following result is called *the linear dependence theorem* that can be found in [7]

Theorem 2. *Let f be a function on V_n that satisfies the propagation criterion with respect to all but $k+1$ vectors $0, \beta_1, \ldots, \beta_k$ in V_n, where $k \geq 2$. 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 $c_1\beta_1 \oplus \cdots \oplus c_k\beta_k = 0$.*

Note that $n+1$ non-zero vectors in V_n must be linearly dependent. Hence if $\#\Re \geq n+2$ (i.e., $\#(\Re - \{0\}) \geq n+1$) then Theorem 2 is trivial. For this reason, we improve Theorem 2 in this paper. We prove two properties of $\Re$: the strong linear dependence and the unbiased distribution of $\Re$.

4 The Strong Linear Dependence Theorem

Note the ith (i.e., the α_ith) row of H_n, where $\alpha_i \in V_n$ is the binary representation of integer j, $j = 0, 1, \ldots, 2^n - 1$, is the sequence of linear function $\varphi_i(x) = \langle \alpha_i, x \rangle$. Lemma 4 of [7] can be restated as follows:

Lemma 3. *Let Q be the $2^n \times q$ that consists of the α_{j_1}th, ... , the α_{j_q}th rows of H_n, where each $\alpha_j \in V_n$ is the binary representation of integer j, $0 \leq j \leq 2^n - 1$. If $\alpha_{j_1}, \ldots, \alpha_{j_q}$ are linearly independent then each $(a_1, \ldots, a_q)^T$, where each $a_j = \pm 1$, appears as a column in Q precisely 2^{n-q} times.*

The following Lemma can be found in [7].

Lemma 4. *Let $n \geq 3$ be a positive integer and $2^n = \sum_{j=1}^{4} a_j^2$ where $a_1 \geq a_2 \geq a_3 \geq a_4 \geq 0$ and each a_j is an integer. We have the following statements:*

(i) if n is add, then $a_1^2 = a_2^2 = 2^{n-1}$, $a_3 = a_4 = 0$,
(ii) if n is even, then $a_1^2 = 2^n$, $a_2 = a_3 = a_4 = 0$ or $a_1^2 = a_2^2 = a_3^2 = a_4^2 = 2^{n-2}$.

Lemma 5. *For every function f on V_n, we have*

$$\begin{aligned}&2(\varDelta(\alpha_0), \varDelta(\alpha_2), \ldots, \varDelta(\alpha_{2^n-2}))H_{n-1}\\&= (\langle\xi, \ell_0\rangle^2 + \langle\xi, \ell_1\rangle^2, \langle\xi, \ell_2\rangle^2 + \langle\xi, \ell_3\rangle^2, \ldots, \langle\xi, \ell_{2^n-2}\rangle^2 + \langle\xi, \ell_{2^n-1}\rangle^2)\end{aligned}$$

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

Proof. From Lemma 2,

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

Comparing the 0th, the 2nd, ..., the $(2^n - 2)$th terms in the two sides of equality (1), we obtain

$$\begin{aligned}&2^n(\varDelta(\alpha_0), \varDelta(\alpha_2), \ldots, \varDelta(\alpha_{2^n-2}))\\&= (\langle\xi, \ell_0\rangle^2 + \langle\xi, \ell_1\rangle^2, (\langle\xi, \ell_2\rangle^2 + \langle\xi, \ell_3\rangle^2, \ldots, \langle\xi, \ell_{2^n-2}\rangle^2 + \langle\xi, \ell_{2^n-1}\rangle^2)H_{n-1}\end{aligned}$$

This proves the lemma. □

The following theorem is called *the strong linearly dependence theorem* which is an improvement on Theorem 2 (the linearly dependence theorem).

Theorem 3. *Let f be a function on V_n, and W be a $(n-1)$-dimensional linear subspace satisfying $\Re \cap W = \{0, \beta_1, \ldots, \beta_k\}$ $(k \geq 3)$. Then $\beta_1, \ldots, \beta_k$ are linearly dependent, namely, there exist k constants $c_1, \ldots, c_k \in GF(2)$ with $(c_1, \ldots, c_k) \neq (0, \ldots, 0)$, 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 $k \leq n$. We only need to prove the lemma in the special case when W is composed of $\alpha_0, \alpha_2, \ldots, \alpha_{2^n-2}$, where $\alpha_{2j} \in V_n$ is the binary representation of an even number $2j$, $j = 0, 1, \ldots, 2^{n-1} - 1$. In other words, W is composed of all the vectors in V_n, that can be expressed in the form $(a_1, \ldots, a_{n-1}, 0)$, where each $a_j \in GF(2)$. In the general case, we can use a nonsingular linear transformation on the variables so as to change W into the special case. Let ξ be the sequence of f.

Since $\beta_j \in W$, $j = 1, \ldots, k$, β_j can be expressed as $\beta_j = (\gamma_j, 0)$ where $\gamma_j \in V_{n-1}$, $j = 1, \ldots, k$, and $0 \in GF(2)$.

Let P be a $(k+1)\times 2^{n-1}$ matrix composed of the 0th, the γ_1th, ..., the γ_kth rows of H_{n-1}. Set $a_j^2 = \langle \xi, \ell_j\rangle^2$, $j = 0, 1, \dots, 2^n - 1$. Note that $\Delta(\alpha) = 0$ if $\alpha \notin \{0, \beta_1, \dots, \beta_k\}$. Hence the equality in Lemma 5 can be specialized as

$$2(\Delta(0), \Delta(\beta_1), \dots, \Delta(\beta_k))P = (a_0^2 + a_1^2, a_2^2 + a_3^2, \dots, a_{2^n-2}^2 + a_{2^n-1}^2) \qquad (2)$$

where $\Delta(0)$ is identical to $\Delta(\alpha_0)$ where $\alpha_0 = 0$.

Write $P = (p_{ij})$, $i = 0, 1, \dots k$, $j = 0, 1, \dots, 2^{n-1} - 1$. As the top row of P is $(1, 1, \dots, 1)$, from (2),

$$2(\Delta(0) + \sum_{i=1}^{k} p_{ij}\Delta(\beta_i)) = a_{2j}^2 + a_{2j+1}^2 \qquad (3)$$

$j = 0, 1, \dots, 2^{n-1} - 1$. Let P^* be the submatrix of P obtained by removing the top row from P.

We now prove the theorem by contradiction. Suppose k vectors in V_n, β_1, ..., β_k, are linearly independent. Hence k vectors in V_{n-1}, $\gamma_1, \dots, \gamma_k$, are also linearly independent and hence $k \leq n - 1$.

Applying Lemma 3 to matrix P^*, we conclude that each k-dimensional $(1, -1)$-vector appears in P^*, as a column vector of P^* precisely 2^{n-1-k} times. Thus for each fixed j there exists a number j_0, $0 \leq j_0 \leq 2^{n-1} - 1$, such that $(p_{1j_0}, \dots, p_{kj_0}) = -(p_{1j}, \dots, p_{kj})$ and hence

$$2(\Delta(0) - \sum_{i=1}^{k} p_{ij_0}\Delta(\beta_i)) = a_{j_0}^2 + a_{2j_0+1}^2 \qquad (4)$$

Adding (3) and (4) together, we have $4\Delta(0) = a_j^2 + a_{2j+1}^2 + a_{j_0}^2 + a_{2j_0+1}^2$. Hence $a_j^2 + a_{2j+1}^2 + a_{j_0}^2 + a_{2j_0+1}^2 = 2^{n+2}$. There are two cases to be considered: even n and odd n.

Case 1: n is odd. By using Lemma 4,

$$\{a_j^2, a_{2j+1}^2, a_{j_0}^2, a_{2j_0+1}^2\} = \{2^{n+1}, 2^{n+1}, 0, 0\}, j = 0, 1, \dots, 2^{n-1} \qquad (5)$$

Hence from (3), we have $\Delta(0) + \sum_{i=1}^{k} p_{ij}\Delta(\beta_i) = 2^{n+1}, 2^n, 0$ and hence

$$\sum_{i=1}^{k} p_{ij}\Delta(\beta_i) = 2^n, 0, -2^n, j = 0, 1, \dots, 2^n - 1 \qquad (6)$$

For each fixed j, rewrite (6) as

$$p_{1j}\Delta(\beta_1) + \sum_{i=2}^{k} p_{ij}\Delta(\beta_i) = 2^n, 0, -2^n \qquad (7)$$

By using Lemma 3, there exists a number j_1, $0 \leq j_1 \leq 2^{n-1} - 1$, such that $(p_{1j_1}, p_{2j_1}, \dots, p_{kj_i}) = (p_{1j}, -p_{2j}, \dots, -p_{kj})$.

Hence

$$p_{1j_1}\Delta(\beta_1)-\sum_{i=2}^{k}p_{ij_1}\Delta(\beta_i)=2^n,0,-2^n \tag{8}$$

Adding (7) and (8) together, we have

$$p_{1j}\Delta(\beta_1)=\pm 2^n,\pm 2^{n-1},0$$

Since $\Delta(\beta_1)\neq 0$, we conclude $\Delta(\beta_1)=\pm 2^n,\pm 2^{n-1}$. By the same reasoning we can prove

$$\Delta(\beta_j)=\pm 2^n,\pm 2^{n-1},j=1,2,\ldots,k \tag{9}$$

Thus we can write

$$(\Delta(\beta_1),\ldots,\Delta(\beta_k))=2^{n-1}(b_1,\ldots,b_k) \tag{10}$$

where each $b_j=\pm 1,\pm 2$. By using Lemma 3, there exists a number s, $0\leq s\leq 2^{n-1}-1$, such that

$$(p_{1s},\ldots,p_{ks})=(\frac{b_1}{|b_1|},\ldots,\frac{b_k}{|b_j|}). \tag{11}$$

Due to (10) and (11),

$$\sum_{i=1}^{k}p_{is}\Delta(\beta_i)=\sum_{i=1}^{k}\frac{b_i}{|b_i|}\Delta(\beta_i)=\sum_{i=1}^{k}\frac{b_i^2}{|b_i|}2^{n-1}=2^{n-1}\sum_{i=1}^{k}|b_i|\geq k2^{n-1}. \tag{12}$$

Since $k\geq 3$, (12) contradicts (6).

Case 2: n is even. By using Lemma 4,

$$\begin{aligned}&\{a_j^2,a_{2j+1}^2,a_{j_0}^2,a_{2j_0+1}^2\}=\{2^{n+2},0,0,0\}\text{ or}\\&\{a_j^2,a_{2j+1}^2,a_{j_0}^2,a_{2j_0+1}^2\}=\{2^n,2^n,2^n,2^n\},j=0,1,\ldots,2^{n-1}\end{aligned} \tag{13}$$

Hence from (3), we have $\Delta(0)+\sum_{i=1}^{k}p_{ij}\Delta(\beta_i)=2^{n+1},2^n,0$, and hence

$$\sum_{i=1}^{k}p_{ij}\Delta(\beta_i)=2^n,0,-2^n$$

Repeating the same deduction as in Case 1, we obtain a contradiction in Case 2.

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. □

Theorem 3 shows that $\Re$ is subject to crucial restrictions. We now compare Theorem 3 with Theorem 2. Since $n+1$ non-zero vectors in V_n must be linearly dependent, Theorem 2 is trivial when $\#\Re\geq n+2$ (i.e., $\#(\Re-\{0\})\geq n+1$). In contrast, in Theorem 3 the linear dependence of vectors takes place in each $\Re\cap W$ not only in $\Re$.

We notice that there exist $n-1$ $(n-1)$-dimensional linear subspaces. Hence Theorem 3 is more profound than Theorem 2.

5 The Unbiased Distribution of $\Re$

In this section we focus on the distribution of $\Re$ for the functions on V_n, whose nonlinearity does not take the special value $2^{n-1}-2^{\frac{1}{2}(n-1)}$ or $2^{n-1}-2^{\frac{1}{2}n}$ or $2^{n-1}-2^{\frac{1}{2}n-1}$.

The next result is from [6] (Theorem 18).

Lemma 6. *Let f be a function on V_n $(n \geq 2)$, ξ be the sequence of f, and p is an integer, $2 \leq p \leq n$. 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 $p-1$.*

Lemma 7. *For every function f on V_n, we have*

$$4(\varDelta(\alpha_0), \varDelta(\alpha_4), \ldots, \varDelta(\alpha_{2^n-4}))H_{n-2}$$
$$= (\sum_{j=0}^{3}\langle \xi, \ell_j\rangle^2, \sum_{j=4}^{7}\langle \xi, \ell_j\rangle^2, \ldots, \sum_{j=2^n-4}^{2^n-1}\langle \xi, \ell_j\rangle^2)$$

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

Proof. Comparing the $4j$th terms, $j = 0, 1, \ldots, 2^{n-2}-1$, in the two sides of equality (1), we obtain

$$2^n(\varDelta(\alpha_0), \varDelta(\alpha_4), \ldots, \varDelta(\alpha_{2^n-4}))$$
$$= (\sum_{j=0}^{3}\langle \xi, \ell_j\rangle^2, \sum_{j=4}^{7}\langle \xi, \ell_j\rangle^2, \ldots, \sum_{j=2^n-4}^{2^n-1}\langle \xi, \ell_j\rangle^2)H_{n-2}$$

This proves the lemma. □

Theorem 4. *Let f be a function on V_n, and U be a $(n-2)$-dimensional linear subspace satisfying $\#(\Re \cap U) = 1$ (i.e., $\Re \cap U = \{0\}$). Then we have*

(i) if n is odd, then the nonlinearity of f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$ and the algebraic degree of f is at most $2^{\frac{1}{2}(n+1)}$,

(ii) if n is even, then f is bent or the nonlinearity of f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}n}$ and the algebraic degree of f is at most $2^{\frac{1}{2}n+1}$.

Proof. We only need to prove the theorem in the special case when U is composed of $\alpha_0, \alpha_4, \alpha_8, \ldots, \alpha_{2^n-4}$, where $\alpha_{4j} \in V_n$ is the binary representation of even number $4j$, $j = 0, 1, 2, \ldots, 2^{n-2}-1$. In other words, U is composed of all the vectors in V_n, that can be expressed in the form $(a_1, \ldots, a_{n-2}, 0, 0)$, where each $a_j \in GF(2)$. For U in general case, we can use a nonsingular linear transformation on the variables so as to change U into the special case. Let ξ be the sequence of f. Set $a_j^2 = \langle \xi, \ell_j \rangle^2$, $j = 0, 1, \ldots, 2^n-1$.

Since $\varDelta(0) = 2^n$ and $\varDelta(\alpha_{4j}) = 0$, $j = 1, 2, \ldots, 2^{n-2}-1$, the equality in Lemma 7 is specialized as

$$2^{n+2}(1,\ldots,1)=(\sum_{j=0}^{3}a_j^2,\sum_{j=4}^{7}a_j^2,\ldots,\sum_{j=2^n-4}^{2^n-1}a_j^2) \tag{14}$$

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

(i) When n is odd, by using Lemma 4,

$$\{a_{4j}^2,a_{4j+1}^2,a_{4j+3}^2,a_{4j+3}^2\}=\{2^{n+1},2^{n+1},0,0\},j=0,1,\ldots,2^{n-2}$$

By using Lemma 1, we have proved the nonlinearity of f satisfies $N_f=2^{n-1}-2^{\frac{1}{2}(n-1)}$, and by using Lemma 6, we have proved that the algebraic degree of f is at most $2^{\frac{1}{2}(n+1)}$.

(ii) When n is even. By using Lemma 4,

$$\{a_{4j}^2,a_{4j+1}^2,a_{4j+3}^2,a_{4j+3}^2\}=\{2^n,2^n,2^n,2^n\} \text{ or } \{2^{n+2},0,0,0\},$$

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

If there exists a number j_0, $0\le j_0\le 2^{n-2}-1$, such that

$$\{a_{4j_0}^2,a_{4j_0+1}^2,a_{4j_0+2}^2,a_{4j_0+3}^2\}=\{2^{n+2},0,0,0\}$$

then by using Lemma 1, we have proved that the nonlinearity of f satisfies $N_f=2^{n-1}-2^{\frac{1}{2}n}$, and by using Lemma 6, we have proved that the algebraic degree of f is at most $2^{\frac{1}{2}(n+1)}$.

If there exists no such j_0, mentioned as above, i.e., $\{a_{4j}^2,a_{4j+1}^2,a_{4j+3}^2,a_{4j+3}^2\}=\{2^n,2^n,2^n,2^n\}$, $j=0,1,\ldots,2^{n-2}-1$. Then f is bent.

□

To emphasise the distribution of $\Re$ we modify Theorem 4 as follows:

Theorem 5. *Let f be a function on V_n. If the nonlinearity of f does not take the special value $2^{n-1}-2^{\frac{1}{2}(n-1)}$ or $2^{n-1}-2^{\frac{1}{2}n}$ or $2^{n-1}-2^{\frac{1}{2}n-1}$, then $\#(\Re\cap U)\ge 2$ where U is any $(n-2)$-dimensional linear subspace, in other words, every $(n-2)$-dimensional linear subspace U contains a non-zero vector in $\Re$.*

There exist many methods to locate all the $(n-1)$-dimensional linear subspaces and all the $(n-2)$-dimensional linear subspaces in V_n. For example, let φ_α denote the linear function on V_n, where $\alpha\in V_n$, such that $\varphi_\alpha(x)=\langle\alpha,x\rangle$. Hence $W=\{\gamma|\alpha\in V_n,\ \varphi_\alpha(\gamma)=0\}$ is a $(n-1)$-dimensional linear subspace and each $(n-1)$-dimensional linear subspace can be expressed in this form.

Also for any $\alpha,\alpha'\in V_n$ with $\alpha\ne\alpha'$, $U=\{\gamma|\alpha\in V_n,\ \varphi_\alpha(\gamma)=0,\ \varphi_{\alpha'}(\gamma)=0\}$ is a $(n-2)$-dimensional linear subspace and each $(n-2)$-dimensional linear subspace can be expressed in this form.

Lemma 8. *Let Ω be a subset of V_k with $0\notin\Omega$. If there exists a positive integer p such that $\#(\Omega\cap U)\ge p$ holds for every $(k-1)$-dimensional linear subspace U, then $\#\Omega\ge 2p+1$.*

Proof. Note that each non-zero vector is included in precisely $2^{k-1}-1$ $(k-1)$-dimensional linear subspaces, on the other hand, there exist exactly 2^k-1 $(k-1)$-dimensional linear subspaces. Hence $(2^{k-1}-1)\#\Omega = \sum_U \#(\Omega \cap U)$. From $\#(\Omega \cap U) \geq p$, we conclude that $(2^{k-1}-1)\#\Omega \geq (2^k-1)p$. Since $\frac{2^k-1}{2^{k-1}-1} > 2$, $\#\Omega > 2p$ or $\#\Omega \geq 2p+1$. □

Theorem 6. *Let f be a function on V_n. If the nonlinearity of f does not take the special values $2^{n-1}-2^{\frac{1}{2}(n-1)}$ or $2^{n-1}-2^{\frac{1}{2}n}$ or $2^{n-1}-2^{\frac{1}{2}n-1}$, then $\#(\Re \cap W) \geq 4$ for every $(n-1)$-dimensional linear subspace W, in other words, every $(n-1)$-dimensional linear subspace W contains at least three non-zero vectors in $\Re$.*

Proof. Let W be an arbitrary $(n-1)$-dimensional linear subspace and U be an arbitrary $(n-2)$-dimensional linear subspace with $U \subset W$. Note that the inequality in Theorem 5 can be rewritten as

$$\#((\Re - \{0\}) \cap U) \geq 1 \tag{15}$$

and $((\Re - \{0\}) \cap W) \cap U = (\Re - \{0\}) \cap U$. Applying Lemma 8, we have proved $\#((\Re - \{0\}) \cap W) \geq 3$. Since $0 \in \Re \cap W$, $\#(\Re \cap W) \geq 4$. □

Theorems 5 and 6 are helpful to locate the non-propagative vectors.

The properties mentioned together in Theorems 5 and 6 are called *the unbiased distribution of* $\Re$, with respect to every $(n-2)$-dimensional linear subspace and every $(n-1)$-dimensional linear subspace.

6 Distribution of $\Re$ in Special Cases

We now turn to the case $\#(\Re_f \cap W) \leq 3$ where W is an $(n-1)$-dimensional linear subspace. The following Lemma can be found in [7]:

Lemma 9. *Let $n \geq 2$ be a positive integer and $2^n = a^2 + b^2$ where $a \geq b \geq 0$ and both a and b are integers. Then $a^2 = 2^n$ and $b = 0$ when n is even, and $a^2 = b^2 = 2^{n-1}$ when n is odd.*

Theorem 7. *Let f be a function on V_n, and W be an $(n-1)$-dimensional linear subspace satisfying $\#(\Re \cap W) = 1$ (i.e., $\Re \cap W = \{0\}$). We have*

(i) f has at most one non-zero linear structure,
(ii) if n is odd, then the nonlinearity of f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$ and the algebraic degree of f is at most $2^{\frac{1}{2}(n+1)}$,
(iii) if n is even, then f is bent.

Proof. (i) Let $\alpha^* \in V_n$ and $\alpha^* \notin W$, From linear algebra, $V_n = W \cup (\alpha^* \oplus W)$, where $\alpha^* \oplus W = \{\alpha^* \oplus \alpha | \alpha \in W\}$, W and $\alpha^* \oplus W$ are disjoint. We now prove that f has at most one non-zero linear structure by contradiction. Suppose f has two non-zero linear structures, β_1 and β_2 with $\beta_1 \neq \beta_2$. Since all linear structures of f form a linear subspace of V_n, $\beta_1 \oplus \beta_2$ is also a non-zero linear structures of f and hence $\beta_1 \oplus \beta_2 \in \Re$. Since $\Re \cap W = \{0\}$, $\beta_1, \beta_2 \in \alpha^* \oplus W$. Obviously $\beta_1 \oplus \beta_2 \in W$ and hence $\beta_1 \oplus \beta_2 \in \Re \cap W$. This contradicts the condition $\Re \cap W = \{0\}$. The contradiction proves that f has at most one non-zero linear structure.

Recall the proof of Theorem 3, (3) can be specialized as $2\Delta(0) = a_{2j}^2 + a_{2j+1}^2$ and hence $a_{2j}^2 + a_{2j+1}^2 = 2^{n+1}$, where $j = 0, 1, \ldots, 2^{n-1} - 1$.

(ii) If n be odd, from Lemma 9, $\{a_{2j}^2, a_{2j+1}^2\} = \{2^{n+1}, 0\}$, where $j = 0, 1, \ldots$, $2^{n-1} - 1$. From Lemma 1, the nonlinearity of f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$. By using Lemma 6 we conclude that the algebraic degree of f is at most $2^{\frac{1}{2}(n+1)}$.

(iii) If n is even, due to Lemma 9, $a_{2j}^2 = a_{2j+1}^2 = 2^n$, where $j = 0, 1, \ldots, 2^{n-1} - 1$. This proves that f is bent.

□

Example 1. Let n be a positive odd number and $f(x_1, \ldots, x_n) = x_1 \oplus g(x_2, \ldots, x_n)$ where g is a bent function in V_{n-1}. Let W be an $(n-1)$-dimensional linear subspace of V_n, composed of all the vectors in V_n, that can be expressed in the form $(0, a_2, \ldots, a_n)$, where each $a_j \in GF(2)$. It is easy to see $\alpha^* = (1, 0, \ldots, 0) \in V_n$ is a non-zero linear structure of f and $\Re \cap W = \{0\}$. Due to (ii) of Theorem 7, $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.

We can restate (iii) of Theorem 7 as follows:

Proposition 1. *Let f be a function on V_n where n is even. If there exists an $(n-1)$-dimensional linear subspace W_0 satisfying $\#(\Re \cap W_0) = 1$ (i.e., $\Re \cap W_0 = \{0\}$), then f satisfies $\Re \cap W = \{0\}$, for every $(n-1)$-dimensional linear subspace W.*

Next we examine the case of $\#(\Re \cap W) = 2$.

Theorem 8. *Let f be a function on V_n. If there exists a $(n-1)$-dimensional linear subspace W satisfying $\Re \cap W = \{0, \beta_1\}$, then we have*

(i) β_1 is a non-zero linear structure of f,
(ii) if n is odd, then the nonlinearity of f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$ and the algebraic degree of f is at most $2^{\frac{1}{2}(n+1)}$,
(iii) if n is even, then $N_f = 2^{n-1} - 2^{\frac{1}{2}n}$ and the algebraic degree of f is at most $2^{\frac{1}{2}n+1}$.

Proof. Since any single non-zero vector is linearly independent, we can keep the deduction in the proof of Theorem 3 until inequality (12) where we need the condition $k \geq 3$.

(i) Recall the proof of Theorem 3, (6) can be specialized as $p_{1j}\Delta(\beta_1) = 2^n, 0, -2^n$, $j = 0, 1, \ldots, 2^n - 1$. Since $\beta_1 \in \Re$, $\Delta(\beta_1) \neq 0$. Hence $\Delta(\beta_1) = \pm 2^n$. This proves that β_1 is a non-zero linear structure.

(ii) If n is odd, from (5) we conclude that $\langle\xi,\ell_i\rangle^2 = 2^{n+1}, 0, i = 0, 1, \ldots, 2^n-1$, and hence by using Lemma 1, we have proved $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$. By using Lemma 6 we conclude that the algebraic degree of f is at most $2^{\frac{1}{2}(n+1)}$.

(iii) If n is even, from (13), $\langle\xi,\ell_i\rangle^2 = 2^{n+2}, 0, 2^n$. Since $\#\Re > 1$, f is not bent. Hence $\langle\xi,\ell_i\rangle^2 = 2^n$ cannot hold for all i and hence there exists a number i_0, $0 \le i_0 \le 2^n-1$, such that $\langle\xi,\ell_i\rangle^2 = 2^{n+2}$. By using Lemma 1, we have proved $N_f = 2^{n-1} - 2^{\frac{1}{2}n}$, if n is even. By using Lemma 6 we conclude that the algebraic degree of f is at most $2^{\frac{1}{2}n+1}$.

□

Example 2. Let n be a positive odd number and $f(x_1,\ldots,x_n)$ be the same with that in Example 1. Let W be an $(n-1)$-dimensional linear subspace of V_n, composed of all the vectors in V_n, that can be expressed in the form $(a_1,\ldots,a_{n-1},0)$, where each $a_j \in GF(2)$. It is easy to see $\alpha^* = (1,0,\ldots,0) \in V_n$ is a non-zero linear structure of f and $\Re \cap W = \{0, \alpha^*\}$. Due to (ii) of Theorem 8, $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.

Let k be a positive even number with $k \ge 4$ and $h(x_1,\ldots,x_k) = x_1 \oplus x_2 \oplus q(x_3,\ldots,x_k)$ where q is a bent function on V_{k-2}. Let U be an $(n-1)$-dimensional linear subspace of V_n, composed of all the vectors in V_n, that can be expressed in the form $(0,a_2,\ldots,a_k)$, where each $a_j \in GF(2)$. It is easy to see $\alpha_1^* = (0,1,0,\ldots,0)$ is a non-zero linear structures of h and $\Re \cap U = \{0, \alpha_1^*\}$. Due to (iii) of Theorem 8, $N_h = 2^{k-1} - 2^{\frac{1}{2}k}$.

It is interesting that by using Theorem 8, we have determined N_h only from the condition $\#(\Re \cap U) = 2$ for an $(n-1)$-dimensional linear subspace U although we do not search other vectors in $\Re$.

Finally, we consider the case when $\#(\Re \cap W) = 3$.

Theorem 9. *Let f be a function on V_n. If there exists a $(n-1)$-dimensional linear subspace W satisfying $\Re \cap W = \{0, \beta_1, \beta_2\}$, then the following statements hold:*

(i) $\Delta(\beta_j) = \pm 2^{n-1}$, $j = 1, 2$,

(ii) if n is odd, then the nonlinearity of f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$ and the algebraic degree of f is at most $2^{\frac{1}{2}(n+1)}$,

(iii) if n is even, then $N_f = 2^{n-1} - 2^{\frac{1}{2}n}$ and the algebraic degree of f is at most $2^{\frac{1}{2}n+1}$.

Proof. Since any two non-zero vectors are linearly independent, we can keep the deduction in the proof of Theorem 3 until inequality (12) where we need the condition $k \ge 3$.

Recall the proof of Theorem 3, (9) can be specialized as $\Delta(\beta_j) = \pm 2^n, \pm 2^{n-1}$, $j = 1, 2$.

On the other hand, (10), (11) and (12) can be rewritten as $(\Delta(\beta_1), \Delta(\beta_2)) = 2^{n-1}(b_1, b_2)$ where each $b_j = \pm 1, \pm 2$, $(p_{1s}, p_{2s}) = (\frac{b_1}{|b_1|}, \frac{b_2}{|b_2|})$. and

$$p_{1s}\Delta(\beta_1) + p_{2s}\Delta(\beta_2) = (|b_1| + |b_2|)2^{n-1} \tag{16}$$

respectively. It is easy to prove $b_1, b_2 = \pm 1$. Otherwise, for example, $b_1 = \pm 2$, from (16), $p_{1s}\Delta(\beta_1)+p_{2s}\Delta(\beta_2) \geq 3\cdot 2^{n-1}$. This contradicts (6). Since $b_1, b_2 = \pm 1$, $\Delta(\beta_1), \Delta(\beta_2) = \pm 2^{n-1}$. This proves (i).

The rest proof is the same with the proof of Theorem 8. □

Example 3. Let n be a positive odd number with $n \geq 7$, $h(x_1, x_2, x_3, x_4, x_5) = (x_1 \oplus x_2 \oplus x_3)x_4x_5 \oplus x_1x_5 \oplus x_2x_4 \oplus x_1 \oplus x_2 \oplus x_3$ and $g(x_6, \ldots, x_n)$ be a bent function on V_{n-5}. Set $f(x_1, \ldots, x_n) = h(x_1, x_2, x_3, x_4, x_5) \oplus g(x_6, \ldots, x_n)$.

Let W be an $(n-1)$-dimensional linear subspace of V_n, composed of all the vectors in V_n, that can be expressed in the form $(0, a_2, \ldots, a_n)$, where each $a_j \in GF(2)$. Write $\alpha_1^* = (0,0,1,0,\ldots,0)$, $\alpha_2^* = (0,1,0,\ldots,0) \in V_n$, It is easy to verify $\alpha_1^*, \alpha_2^* \in \Re$ and $\Re \cap W = \{0, \alpha_1^*, \alpha_2^*\}$. Due to (i) and (ii) of Theorem 9, we conclude $\Delta(\alpha_1^*) = \pm 2^{n-1}$, $\Delta(\alpha_2^*) = \pm 2^{n-1}$ and $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.

We notice that by using Theorem 9, we have determined N_h, $\Delta(\alpha_1^*)$ and $\Delta(\alpha_2^*)$ only from the information about $\#(\Re \cap W)$ for an $(n-1)$-dimensional linear subspace W although we do not search other the vectors in $\Re$.

We can also find an example corresponding to (iii) of Theorem 9. All Theorems 7, 8 and 9 and Examples 1, 2 and 3 show that we can determine the nonlinearity of a function only from some information about $\#(\Re \cap W)$, where W is an $(n-1)$-dimensional linear subspace. It is interesting that [7] has proved that there exists no a function with $\#\Re = 3$ while Example 3 gives a function satisfying $\#(\Re \cap W) = 3$ for an $(n-1)$-dimensional linear subspace W.

7 Conclusions

The strong linear dependence is an improvement on a previously known result. The unbiased distribution of non-propagation vectors is valid for most functions. These results provide more information on the non-propagative vectors in any $(n-1)$-dimensional linear subspace of V_n, and hence they are helpful for designing cryptographic functions.

8 Acknowledgement

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

References

1. Claude Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, 3:135–145, 1993.
2. W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89*, volume 434, Lecture Notes in Computer Science, pages 549–562. Springer-Verlag, Berlin, Heidelberg, New York, 1990.

3. 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, Lecture Notes in Computer Science, pages 155–165. Springer-Verlag, Berlin, Heidelberg, New York, 1991.
4. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.
5. A. F. Webster and S. E. Tavares. On the design of S-boxes. In *Advances in Cryptology - CRYPTO'85*, volume 219, Lecture Notes in Computer Science, pages 523–534. Springer-Verlag, Berlin, Heidelberg, New York, 1986.
6. Y. Zheng X. M. Zhang and Hideki Imai. Duality of boolean functions and its cryptographic significance. In *Advances in Cryptology - ICICS'97*, volume 1334, Lecture Notes in Computer Science, pages 159–169. Springer-Verlag, Berlin, Heidelberg, New York, 1997.
7. 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.