# Characterizing the Structures of Highly Nonlinear 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

July 15, 1994

**Abstract**

This paper studies the properties and constructions of nonlinear functions, which are a core component of cryptographic primitives including data encryption algorithms and one-way hash functions. A main contribution of this paper is to reveal the relationship between nonlinearity and propagation characteristic, two critical indicators of the cryptographic strength of a Boolean function. 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, the nonlinearity of $f$ satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$, and the nonzero vector in $\Re$ must be a linear structure of $f$.

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

(v) if $|\Re| = 4$ then $n$ must be even, the nonlinearity of $f$ satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}n}$, and the nonzero vectors in $\Re$ must be linear structures of $f$.

(vi) if $|\Re| = 5$ then $n$ must be odd, the nonlinearity of $f$ is $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$, the four nonzero vectors in $\Re$, denoted by $\beta_1$, $\beta_2$, $\beta_3$ and $\beta_4$, are related by the equation $\beta_1 \oplus \beta_2 \oplus \beta_3 \oplus \beta_4 = 0$, and *none* of the four vectors is a linear structure of $f$.

(vii) there exists no function on $V_n$ such that $|\Re| = 6$.

We also discuss the structures of functions with $|\Re| = 2, 4, 5$. In particular we show that these functions have close relationships with bent functions, and can be easily constructed from the latter.

# 1 Introduction

Cryptographic techniques for information authentication and data encryption require Boolean functions with a number of critical properties that distinguish them from linear (or affine) functions. Among the properties are high nonlinearity, high degree of propagation, few linear structures, high algebraic degree etc. These properties are often called *nonlinearity criteria*. An important topic is to investigate relationships among the various nonlinearity criteria. Progress in this direction has been made in [10], where connections have been revealed among the strict avalanche characteristic (SAC), differential characteristics, linear structures and nonlinearity, of *quadratic* functions.

In this paper we carry on the investigation initiated in [10] and bring together nonlinearity and propagation characteristic of a Boolean function (quadratic or non-quadratic). These two cryptographic criteria are seemly quite separate, in the sense that the former indicates the minimum distance between a Boolean function and all the affine functions whereas the latter forecasts the avalanche behavior of the function when some input bits to the function are complemented.

We further extend our investigation into the structures of cryptographic functions. The organization of the remaining part of this paper is as follows: After introducing basic definitions in Section 2, we show in Section 3 the relationship between propagation characteristic and nonlinearity. We further explore this result in Sections 4, 5, 6, 7, 8 and 9, and make explicit the structural forms of functions that satisfy the propagation criterion with respect to all but six or less vectors. We examine degrees of propagation of the functions in Section 10, and finally, close the paper with some remarks in Section 11.

# 2 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 $\varphi_1$, $\varphi_2$, ..., $\varphi_{2^{n+1}}$ 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 $\alpha$ *if* $f(x) \oplus f(x \oplus \alpha)$ *is a balanced function, where* $x = (x_1, \ldots, x_n)$ *and* $\alpha$ *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 [8]. Further work on the topic can be found in [7]. Note that the strict avalanche criterion (SAC) introduced by Webster and Tavares [11, 12] is equivalent to the propagation criterion of degree 1 and that the perfect nonlinearity studied by Meier and Staffelbach [5] 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 [3].

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* $\beta$ *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 [1, 2, 9, 13]. 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 $\ell$ of length $2^n$, where $\xi$ 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 $2^{n-1} - 2^{\frac{1}{2}n-1}$.

## 3 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 $\alpha$. On the other hand, if $|\Delta(\alpha)| = 2^n$, then $f(x) \oplus f(x \oplus \alpha)$ is a constant and hence $\alpha$ is a linear structure of $f$.

Let $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$ be the matrix of $f$ and $\xi$ be the sequence of $f$. Due to a very pretty result by R. L. McFarland (see Theorem 3.3 of [2]), $M$ 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 $\ell_i$ is the $i$th row of $H_n$, a Sylvester-Hadamard matrix of order $2^n$. By Lemma 2 of [9], $\ell_i$ is the sequence of a linear function defined by $\varphi_i(x) = \langle \alpha_i, x \rangle$, where $\alpha_i$ is the $i$th 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.

Lemma 6 of [9] 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 $\xi_{f_1}$ and $\xi_{f_2}$ are the sequences of $f_1$ and $f_2$ respectively. As an immediate consequence we have:

**Lemma 1** *The nonlinearity of a function $f$ on $V_n$ can be calculated by*

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

*where $\xi$ is the sequence of $f$ and $\ell_0$, ..., $\ell_{2^n-1}$ are the sequences of the linear functions on $V_n$.*

Now we prove a central result of this 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 $\alpha_j$ 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 in that $2^{-n} H_n H_n = I$, 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 the 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, [4]), 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 $j = 0, 1, \ldots, 2^n - 1$.

By Lemma 1, 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 [5] or Lemma 10 of [9]). 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 [6] (see also a detailed discussion in [10]) that knowing the linearity dimension, say $\ell$, 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 [6].

In the next section we discuss an interesting special case where $|\Re| = 2$. More general cases where $|\Re| > 2$, which need very different proof techniques, will be fully discussed in the later part of the paper.

# 4 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 2** *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 $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.*

*Proof.* Let $\beta$ 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 $\alpha_1$. In addition, $\beta$ is a linear structure of $f$ if and only if $\alpha_1$ 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 $\alpha_j$ is the $j$th 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 2,

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

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

Since $n$ is odd, from (6) and Lemma 2 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, $\alpha_1$ is a linear structure of $g$. Thus $\beta = \alpha_1 B^{-1}$ is a linear structure of $f$. This proves (ii) of the theorem.

The above discussions for Cases 1 and 2, together with (3), imply that $\langle \xi, \ell_i \rangle^2 = 2^{n+1}$ or 0, i.e., $|\langle \xi, \ell_i \rangle| = 2^{\frac{1}{2}(n+1)}$ or 0, for all $0 \leqq i \leqq 2^n - 1$. Applying Lemma 1,

$$N_f = N_g = 2^{n-1} - 2^{\frac{1}{2}(n-1)}.$$

This completes the proof. □

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 $g(x) = f(xB)$ 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 [6], $N_g = 2N_h$. On the other hand, from (iii) of Theorem 2,

$$N_g = 2^{n-1} - 2^{\frac{1}{2}(n-1)}.$$

Thus

$$N_h = 2^{n-2} - 2^{\frac{1}{2}(n-1)-1}.$$

This indicates that $h$, a function on $V_{n-1}$, achieves the maximum nonlinearity and hence it is bent (see also [4] or Lemma 4 of [9]).

Conversely, suppose that $g$ can be expressed as (7). Since $h$ is a bent function on $V_{n-1}$, $\alpha_1 = (0, 0, \ldots, 0, 1)$ 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 (informally) 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.*

## 5 Linear Dependence in $\Re$

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

**Lemma 3** *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 $\sigma_i$ is the truth table and $\ell_i$ is the sequence of $\psi_i$, $i = 1, \ldots, k$. 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 [10]. □

Next we show the linear dependence of nonzero 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 $\xi$ be the sequence of $f$.

Let $P$ be a matrix that consists of the 0th, $\beta_1$th, ..., $\beta_k$th rows of $H_n$. Here we regard $beta_i$ as an integer. 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 $\alpha_0$ 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 $\beta_i$th 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 [9]). 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 3, 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 2, $a_j^2 = a_{j_0}^2 = 2^n$. 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 2). 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 2, $a_j^2 = 2^{n+1}$ 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 3, 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 criterion with respect to $\beta_1$, we have $\Delta(\beta_1) \neq 0$ and $c_j + c_{j_0} \neq 0$. This implies $c_j + c_{j_0} = \pm 2$, and hence $\Delta(\beta_1) = \pm 2^n$. 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 $b_j = \pm 1$. By Lemma 3, 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 following sections we examine the cases when $|\Re| = 3, 4, 5, 6$.

# 6 Functions with $|\Re| = 3$

When $|\Re| = 3$, the two distinct nonzero vectors in $\Re$ 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.*

## 7 Functions with $|\Re| = 4$

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, but not two, squares.

**Lemma 4** *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)* *$\beta_1, \beta_2$ and $\beta_3$ must be linear structures of $f$,*

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

*Proof.* By Lemma 3, $\beta_1, \beta_2$ and $\beta_3$ are linearly dependent. The only possibility is $\beta_1 \oplus \beta_2 \oplus \beta_3 = 0$. Since $\beta_1, \beta_2$ and $\beta_3$ 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 $\alpha_i$ is the $i$th 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, second, third and 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

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

It turns out that that $n$ must be even. Suppose that $n$ is odd. By Lemma 4, 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 $\alpha_1$. 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 4, 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 $\alpha_1$, $\alpha_2$ and $\alpha_3$ all are linear structures of $g$. Hence $\beta_1, \beta_2$ and $\beta_3$ must be linear structures of the original function $f$. This show that the part (iii) holds.

The above discussions also show that $\langle \xi, \ell_i \rangle^2 = 2^{n+2}$ or 0 for all $0 \leqq i \leqq 2^n - 1$. By Lemma 1, $N_f = N_g = 2^{n-1} - 2^{\frac{1}{2}n}$. Hence the part (iv) is true. □

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 $g(x) = f(xB)$ 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 [9], 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 [9], we conclude that *the methods of repeating bent functions presented in [9] generate all the functions that satisfy the propagation criterion with respect to all but two or four vectors.*

# 8 Functions with $|\Re| = 5$

Let $f$ be a function on $V_n$ with $|\Re| = 5$ and let $\Re = \{0, \beta_1, \beta_2, \beta_3, \beta_4\}$. First we discuss properties of and relationship among the four nonzero vectors. This is followed by a method showing how to construct functions with $|\Re| = 5$.

## 8.1 $\beta_1 \oplus \beta_2 \oplus \beta_3 \oplus \beta_4 = 0$

By Theorem 3, $\beta_1, \beta_2, \beta_3, \beta_4$ are linearly dependent. As $\beta_1, \beta_2, \beta_3, \beta_4$ are distinct nonzero vectors, the rank of $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ must be 3.

Without loss of generality, we assume that $\beta_1, \beta_2, \beta_3$ are linearly independent. As a nonsingular linear transformation on the input coordinates does not affect the total number of vectors where the propagation criterion is satisfied by $f$, we can further assume that

$\beta_1 = \alpha_1 = (0,\ldots,0,0,0,1)$, $\beta_2 = \alpha_2 = (0,\ldots,0,0,1,0)$ and $\beta_3 = \alpha_4 = (0,\ldots,0,1,0,0)$. Our goal is to prove that $\beta_1$, $\beta_2$, $\beta_3$ and $\beta_4$ are related by $\beta_1 \oplus \beta_2 \oplus \beta_3 \oplus \beta_4 = 0$; that is, $\beta_4 = \beta_1 \oplus \beta_2 \oplus \beta_3$. We achieve this by showing that there exist *no* "shorter" relations than $\beta_4 = \beta_1 \oplus \beta_2 \oplus \beta_3$, namely, *none* of the three shorter equations $\beta_4 = \beta_1 \oplus \beta_2$, $\beta_4 = \beta_2 \oplus \beta_3$ and $\beta_4 = \beta_1 \oplus \beta_3$ can hold.

We first show that $\beta_4 \neq \beta_1 \oplus \beta_2$. Assume for contradiction that $\beta_4 = \beta_1 \oplus \beta_2$. Thus $\beta_4 = \alpha_1 \oplus \alpha_2 = (0,\ldots,0,1,1) = \alpha_3$.

Rewrite (2) as

$$(\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1}))H_n = (a_0^2, a_1^2, \ldots, a_{2^n-1}^2) \tag{13}$$

where $a_j = \langle \xi, \ell_j \rangle^2$, $j = 0, 1, \ldots, 2^n - 1$, and $\xi$ is the sequence of $f$. Since $\beta_1 = \alpha_1$, $\beta_2 = \alpha_2$, $\beta_3 = \alpha_4$, $\beta_4 = \alpha_3$, and $\Delta(\alpha) = 0$ for $\alpha \neq 0, \alpha_1, \alpha_2, \alpha_3, \alpha_4$, (13) is specialized as

$$(\Delta(\alpha_0), \Delta(\alpha_1), \Delta(\alpha_2), \Delta(\alpha_3), \Delta(\alpha_4))P = (a_0^2, a_1^2, \ldots, a_{2^n-1}^2) \tag{14}$$

where $P$ is a matrix that consists of the 0th, 1st, 2nd, 3rd and 4th rows of $H_n$. The matrix $P$ can be viewed as

$$P = (P_0, P_1, \ldots, P_{2^{n-3}})$$

where each $P_j$ is a $5 \times 8$ matrix specified by:

$$P_j = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \end{bmatrix}.$$

Using the 0th, 1st, 6th and 7th columns of $P_j$, we obtain from (14) the following four equations:

$$\begin{aligned} \Delta(\alpha_0) + \Delta(\alpha_1) + \Delta(\alpha_2) + \Delta(\alpha_3) + \Delta(\alpha_4) &= a_0^2 \\ \Delta(\alpha_0) - \Delta(\alpha_1) + \Delta(\alpha_2) - \Delta(\alpha_3) + \Delta(\alpha_4) &= a_1^2 \\ \Delta(\alpha_0) + \Delta(\alpha_1) - \Delta(\alpha_2) - \Delta(\alpha_3) - \Delta(\alpha_4) &= a_6^2 \\ \Delta(\alpha_0) - \Delta(\alpha_1) - \Delta(\alpha_2) + \Delta(\alpha_3) - \Delta(\alpha_4) &= a_7^2 \end{aligned}$$

Since $\Delta(\alpha_0) = 2^n$ we have

$$\begin{aligned} \Delta(\alpha_1) + \Delta(\alpha_2) + \Delta(\alpha_3) + \Delta(\alpha_4) &= a_0^2 - 2^n \\ -\Delta(\alpha_1) + \Delta(\alpha_2) - \Delta(\alpha_3) + \Delta(\alpha_4) &= a_1^2 - 2^n \\ \Delta(\alpha_1) - \Delta(\alpha_2) - \Delta(\alpha_3) - \Delta(\alpha_4) &= a_6^2 - 2^n \\ -\Delta(\alpha_1) - \Delta(\alpha_2) + \Delta(\alpha_3) - \Delta(\alpha_4) &= a_7^2 - 2^n \end{aligned} \tag{15}$$

Thus

$$a_0^2 + a_1^2 + a_6^2 + a_7^2 = 2^{n+2}, \tag{16}$$

$$\Delta(\alpha_1) = \frac{1}{4}(a_0^2 - a_1^2 + a_6^2 - a_7^2), \tag{17}$$

$$\Delta(\alpha_2) + \Delta(\alpha_4) = \frac{1}{4}(a_0^2 + a_1^2 - a_6^2 - a_7^2). \tag{18}$$

Similarly, using the 2nd, 3rd, 4th and 5th columns of $P_j$, we have

$$\begin{aligned}
\Delta(\alpha_1) - \Delta(\alpha_2) - \Delta(\alpha_3) + \Delta(\alpha_4) &= a_2^2 - 2^n \\
-\Delta(\alpha_1) - \Delta(\alpha_2) + \Delta(\alpha_3) + \Delta(\alpha_4) &= a_3^2 - 2^n \\
\Delta(\alpha_1) + \Delta(\alpha_2) + \Delta(\alpha_3) - \Delta(\alpha_4) &= a_4^2 - 2^n \\
-\Delta(\alpha_1) + \Delta(\alpha_2) - \Delta(\alpha_3) - \Delta(\alpha_4) &= a_5^2 - 2^n \qquad (19)
\end{aligned}$$

and

$$a_2^2 + a_3^3 + a_4^2 + a_5^2 = 2^{n+2}, \qquad (20)$$

$$\Delta(\alpha_1) = \frac{1}{4}(a_2^2 - a_3^2 + a_4^2 - a_5^2), \qquad (21)$$

$$\Delta(\alpha_2) - \Delta(\alpha_4) = \frac{1}{4}(-a_2^2 - a_3^2 + a_4^2 + a_5^2). \qquad (22)$$

We continue our discussions with the cases $n$ odd and $n$ even. In both cases we present a contradiction by showing that $f$ satisfies the propagation criterion with respect to at least one of the four vectors $\beta_1$, $\beta_2$, $\beta_3$ and $\beta_4$.

The 0th,1st, 6th and 7th columns of $P_j$ provide us with enough information for the case when $n$ is odd. To repeat the equation (17), we have $\Delta(\alpha_1) = \frac{1}{4}(a_0^2 - a_1^2 + a_6^2 - a_7^2)$. We can obtain one more equation from (15):

$$\Delta(\alpha_3) = \frac{1}{4}(a_0^2 - a_1^2 - a_6^2 + a_7^2). \qquad (23)$$

According to (16), the sum of the squares of $a_0$, $a_1$, $a_6$ and $a_7$ is $2^{n+2}$. As $n$ is odd, by Lemma 4, $a_{j_1}^2 = a_{j_2}^2 = 2^{n+1}$, for some $j_1$ and $j_2 \in \{0,1,6,7\}$, and $a_j = 0$, for the other two $j$s. Comparing (17) with (23), we can see that at least one of $\Delta(\alpha_1)$ and $\Delta(\alpha_3)$ must be zero, which contradicts the fact that $f$ does not satisfy the propagation criterion with respect to $\beta_j$, $j = 1,2,3,4$. Hence $\beta_4 = \beta_1 \oplus \beta_2$ does not hold for $n$ odd.

Next we consider the case when $n$ is even. In this case, by Lemma 4, (16) implies

$$a_0^2 = a_1^2 = a_6^2 = a_7^2 = 2^n, \qquad (24)$$

or

$$a_{j_0}^2 = 2^{n+2}, \text{for a } j_0 \in \{0,1,6,7\}, \text{and } a_j = 0, \text{ for the other three } j\text{s}, \qquad (25)$$

while (20) implies

$$a_2^2 = a_3^2 = a_4^2 = a_5^2 = 2^n, \qquad (26)$$

or

$$a_{k_0}^2 = 2^{n+2}, \text{for an } k_0 \in \{2,3,4,5\}, \text{and } a_k = 0, \text{ for the other three } k\text{s}. \qquad (27)$$

(24) or (26), together with (17), causes $\Delta(\alpha_1) = 0$, a contradiction. This leaves us with (25) and (27).

When (25) and (27) hold, (18) results in $\Delta(\alpha_2) + \Delta(\alpha_4) = \pm 2^n$, while (22) gives us $\Delta(\alpha_2) - \Delta(\alpha_4) = \pm 2^n$. Thus we have

$$\Delta(\alpha_2) + \Delta(\alpha_4) = \pm(\Delta(\alpha_2) - \Delta(\alpha_4)).$$

This causes $\Delta(\alpha_2) = 0$ or $\Delta(\alpha_4) = 0$. In either case it contradicts the fact that $f$ does not satisfy the propagation criterion with respect to $\beta_j$, $j = 1, 2, 3, 4$. Hence $\beta_4 = \beta_1 \oplus \beta_2$ does not hold for $n$ even.

In summary, $\beta_4 \neq \beta_1 \oplus \beta_2$ both for $n$ odd and for $n$ even. The other two cases, $\beta_4 \neq \beta_2 \oplus \beta_3$ and $\beta_4 \neq \beta_1 \oplus \beta_3$, can be proved in the same way. Hence we have proved the following result:

**Lemma 5** *Let $f$ be a function on $V_n$ that satisfies the propagation criterion with respect to all but five vectors 0, $\beta_1, \beta_2, \beta_3, \beta_4$ in $V_n$. Then $\beta_1 \oplus \beta_2 \oplus \beta_3 \oplus \beta_4 = 0$.*

### 8.2 $\beta_1$, $\beta_2$, $\beta_3$ and $\beta_4$ Are Not Linear Structures

We have proved that $\beta_1 = \alpha_1$, $\beta_2 = \alpha_2$, $\beta_3 = \alpha_4$ and $\beta_4 = \beta_1 \oplus \beta_2 \oplus \beta_3 = (0, \ldots, 0, 1, 1, 1) = \alpha_7$. The next topic is to find out the value of $\Delta(\beta_i)$, $i = 1, 2, 3, 4$.

Since $\Delta(\alpha) = 0$ for $\alpha \neq 0, \alpha_1, \alpha_2, \alpha_4, \alpha_7$, (13) is simplified as

$$(\Delta(\alpha_0), \Delta(\alpha_1), \Delta(\alpha_2), \Delta(\alpha_4), \Delta(\alpha_7))Q = (a_0^2, a_1^2, \ldots, a_{2^n-1}^2) \tag{28}$$

where $Q$ is a matrix that consists of the 0th, 1st, 2nd, 4th and 7th rows of $H_n$. In other words, we have

$$P = (Q_0, Q_1, \ldots, Q_{2^{n-3}})$$

where each $Q_j$ is defined by

$$Q_j = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

Thus from (28), we have

$$\begin{aligned} \Delta(\alpha_0) + \Delta(\alpha_1) + \Delta(\alpha_2) + \Delta(\alpha_4) + \Delta(\alpha_7) &= a_0^2 \\ \Delta(\alpha_0) - \Delta(\alpha_1) - \Delta(\alpha_2) - \Delta(\alpha_4) - \Delta(\alpha_7) &= a_7^2 \end{aligned} \tag{29}$$

which correspond to the first and last columns of $Q_j$ respectively. Hence

$$a_0^2 + a_7^2 = 2\Delta(\alpha_0) = 2^{n+1}. \tag{30}$$

We distinguish two cases: $n$ even and $n$ odd.

When $n$ is even, by Lemma 2, we have $a_0^2 = a_7^2 = 2^n$. Similarly we have $a_1^2 = a_6^2 = 2^n$, $a_2^2 = a_5^2 = 2^n$ and $a_3^2 = a_4^2 = 2^n$. Hence $a_i^2 = 2^n$ for all $0 \leqq i \leqq 7$.

On the other hand, from (28),

$$\begin{aligned} \Delta(\alpha_0) + \Delta(\alpha_1) + \Delta(\alpha_2) + \Delta(\alpha_4) + \Delta(\alpha_7) &= a_0^2 \\ \Delta(\alpha_0) - \Delta(\alpha_1) + \Delta(\alpha_2) + \Delta(\alpha_4) - \Delta(\alpha_7) &= a_1^2 \end{aligned}$$

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

$$\Delta(\alpha_2) + \Delta(\alpha_4) = 0. \tag{31}$$

Again, from (28),

$$\begin{aligned}\Delta(\alpha_0)+\Delta(\alpha_1)-\Delta(\alpha_2)+\Delta(\alpha_4)-\Delta(\alpha_7) &= a_2^2\\ \Delta(\alpha_0)-\Delta(\alpha_1)-\Delta(\alpha_2)+\Delta(\alpha_4)+\Delta(\alpha_7) &= a_3^2\end{aligned}$$

hence

$$-\Delta(\alpha_2)+\Delta(\alpha_4)=0. \tag{32}$$

Compare (31) with (32), $\Delta(\alpha_2)=\Delta(\alpha_4)=0$. This contradicts the fact that $f$ does not satisfy the propagation criterion with respect to $\beta_j$, $j=1,2,3,4$. Thus we have the following conclusion:

**Lemma 6** *Let $f$ be a function on $V_n$ that satisfies the propagation criterion with respect to all but five vectors 0, $\beta_1, \beta_2$, $\beta_3$, $\beta_4$ in $V_n$. Then $n$ is odd.*

Now we know that $n$ must be odd. ¿From (30) and Lemma 2, we have

$$a_0^2 = 2^{n+1} \text{ or } 0,\ (a_7^2 = 0 \text{ or } 2^{n+1}).$$

By the same reasoning,

$$\begin{aligned}&a_0^2 = 2^{n+1} \text{ or } 0\ (a_7^2 = 0 \text{ or } 2^{n+1}), a_1^2 = 2^{n+1} \text{ or } 0\ (a_6^2 = 0 \text{ or } 2^{n+1}),\\ &a_2^2 = 2^{n+1} \text{ or } 0\ (a_5^2 = 0 \text{ or } 2^{n+1}), a_3^2 = 2^{n+1} \text{ or } 0\ (a_4^2 = 0 \text{ or } 2^{n+1}).\end{aligned} \tag{33}$$

The first four columns of $Q_j$, together with (28), yield,

$$\begin{aligned}\Delta(\alpha_0)+\Delta(\alpha_1)+\Delta(\alpha_2)+\Delta(\alpha_4)+\Delta(\alpha_7) &= a_0^2\\ \Delta(\alpha_0)-\Delta(\alpha_1)+\Delta(\alpha_2)+\Delta(\alpha_4)-\Delta(\alpha_7) &= a_1^2\\ \Delta(\alpha_0)+\Delta(\alpha_1)-\Delta(\alpha_2)+\Delta(\alpha_4)-\Delta(\alpha_7) &= a_2^2\\ \Delta(\alpha_0)-\Delta(\alpha_1)-\Delta(\alpha_2)+\Delta(\alpha_4)+\Delta(\alpha_7) &= a_3^2\end{aligned}$$

Using (33), they can be rewritten as

$$\begin{aligned}\Delta(\alpha_1)+\Delta(\alpha_2)+\Delta(\alpha_4)+\Delta(\alpha_7) &= c_1 2^n\\ -\Delta(\alpha_1)+\Delta(\alpha_2)+\Delta(\alpha_4)-\Delta(\alpha_7) &= c_2 2^n\\ \Delta(\alpha_1)-\Delta(\alpha_2)+\Delta(\alpha_4)-\Delta(\alpha_7) &= c_3 2^n\\ -\Delta(\alpha_1)-\Delta(\alpha_2)+\Delta(\alpha_4)+\Delta(\alpha_7) &= c_4 2^n\end{aligned}$$

where $c_j=\pm 1$, $j=1,2,3,4$. Hence

$$\begin{aligned}\Delta(\alpha_1) &= (c_1-c_2+c_3-c_4)2^{n-2}\\ \Delta(\alpha_2) &= (c_1+c_2-c_3-c_4)2^{n-2}\\ \Delta(\alpha_3) &= (c_1+c_2+c_3+c_4)2^{n-2}\\ \Delta(\alpha_4) &= (c_1-c_2-c_3+c_4)2^{n-2}.\end{aligned} \tag{34}$$

Since $\Delta(\alpha_j)\neq 0$, $j=1,2,3,4$, we have $(c_1,c_2,c_3,c_4)\neq \pm(1,1,1,1)$, $\pm(1,1,-1,-1)$, $(1,-1,1,-1)$ or $\pm(1,-1,-1,1)$. Hence $(c_1,c_2,c_3,c_4)$ can come only from $\pm(1,1,1,-1)$, $\pm(1,1,-1,1)$, $(1,-1,1,1)$ and $\pm(-1,1,1,1)$.

Without loss of generality, suppose that $(c_1,c_2,c_3,c_4)=\pm(1,1,1,-1)$. ¿From (34), we have

$$\Delta(\alpha_1)=2^{n-1}, \Delta(\alpha_2)=2^{n-1}, \Delta(\alpha_4)=2^{n-1}, \Delta(\alpha_7)=-2^{n-1}.$$

This proves the result shown below.

**Lemma 7** *Let $f$ be a function on $V_n$ that satisfies the propagation criterion with respect to all but five vectors 0, $\beta_1, \beta_2, \beta_3, \beta_4$ in $V_n$. Then $|\Delta(\beta_j)| = 2^{n-1}$, $j = 1,2,3,4$. Furthermore, among the four values $\Delta(\beta_j)$, $j = 1,2,3,4$, three have the same sign while the remaining one has a different sign.*

Finally we examine the nonlinearity of $f$. Clearly, from (33) we have $a_j = \langle \xi, \ell_j \rangle^2 = 2^{n+1}$ or 0, namely $\langle \xi, \ell_j \rangle = \pm 2^{\frac{1}{2}(n+1)}$ or 0, for all $j = 0, 1, \ldots, 2^n - 1$. By Lemma 1, the nonlinearity of $f$ with $|\Re| = 5$ is $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.

**Lemma 8** *Let $f$ be a function on $V_n$ that satisfies the propagation criterion with respect to all but five vectors 0, $\beta_1, \beta_2, \beta_3, \beta_4$ in $V_n$. Then the nonlinearity of $f$ is $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.*

Combining together Lemmas 5, 6, 7 and 8, we have the following conclusion

**Theorem 6** *Let $f$ be a Boolean function on $V_n$ that satisfies the propagation criterion with respect to all but a subset $\Re = \{0, \beta_1, \beta_2, \beta_3, \beta_4\}$. Then*

*(i) $n$ is odd,*

*(ii) $\beta_1 \oplus \beta_2 \oplus \beta_3 \oplus \beta_4 = 0$,*

*(iii) $|\Delta(\beta_j)| = 2^{n-1}$, $j = 1,2,3,4$, and three $\Delta(\beta_j)$ have the same sign while the remaining has a different sign, and*

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

Recall that when $|\Re| = 2$ or 4, all nonzero vectors in $\Re$ are linear structures of $f$, and the structure of $f$ is very simple — it can be (informally) viewed as the two- or four-repetition of a bent function on $V_{n-1}$ or $V_{n-2}$. In contrast, when $|\Re| = 5$, none of the nonzero vectors in $\Re$ is a linear structure of $f$. Thus if a non-bent function does *not* possess linear structures, then $|\Re|$ must be at least 5. In this sense, functions with $|\Re| = 5$ occupy a very special position in our understanding of the structures of functions.

### 8.3 Constructing Functions with $|\Re| = 5$

The structure of a function with $|\Re| = 5$ is not as simple as the cases when $|\Re| < 5$. Unlike the case with $|\Re| = 2$ or 4, there seem to be a number of different ways to construct functions with $|\Re| = 5$. The purpose of this section is to demonstrate one of such construction methods.

We start with $n = 5$. Let $\omega(y)$ be a mapping from $V_2$ into $V_3$, defined as follows

$$\omega(0,0) = (1,0,0), \omega(0,1) = (0,1,0), \omega(1,0) = (1,1,0), \omega(1,1) = (0,1,1).$$

Set

$$f_5(z) = f_5(y,x) = \langle \omega(y), x \rangle \tag{35}$$

where $y \in V_2$ and $x \in V_3$, $z = (y,x)$. Obviously $f_5$ is a function on $V_5$ and

$$\begin{aligned} f_5(0,0,x_1,x_2,x_3) &= x_1, \\ f_5(0,1,x_1,x_2,x_3) &= x_2, \\ f_5(1,0,x_1,x_2,x_3) &= x_1 \oplus x_2, \\ f_5(1,1,x_1,x_2,x_3) &= x_2 \oplus x_3. \end{aligned}$$

Hence $f_5$ can be explicitly expressed as

$$\begin{aligned} f_5(y_1,y_2,x_1,x_2,x_3) &= (1\oplus y_1)(1\oplus y_2)x_1 \oplus (1\oplus y_1)y_2x_2 \oplus \\ & \quad y_1(1\oplus y_2)(x_1\oplus x_2)\oplus y_1y_2(x_2\oplus x_3) \end{aligned} \tag{36}$$

Let $\ell_{100}$, $\ell_{010}$, $\ell_{110}$, $\ell_{011}$ denote the sequences of $\varphi_{100}(x_1,x_2,x_3)=x_1$, $\varphi_{010}(x_1,x_2,x_3)=x_2$, $\varphi_{110}(x_1,x_2,x_3)=x_1\oplus x_2$, $\varphi_{011}(x_1,x_2,x_3)=x_2\oplus x_3$ respectively, where each $\varphi$ is regarded as a linear function on $V_3$. By Lemma 1 of [9], $\ell_{100}$, $\ell_{010}$, $\ell_{110}$, $\ell_{011}$ are four different rows of $H_3$. By Lemma 2 of [9], the sequence of $f_5$ is

$$\xi = (\ell_{100},\ \ell_{010},\ \ell_{110},\ \ell_{011}).$$

Let $\xi(\gamma)$ denote the sequence of

$$f_5(z\oplus\gamma) = \langle \omega(y\oplus\beta), x\oplus\alpha\rangle$$

where $\beta\in V_2$ and $\alpha\in V_3$, $\gamma=(\beta,\alpha)$. We now consider $\Delta(\gamma)=\langle\xi,\xi(\gamma)\rangle$.

Case 1: $\beta\neq 0$. In this case we have

$$f_5(z)\oplus f_5(z\oplus\gamma) = \langle\omega(y)\oplus\omega(y\oplus\beta),x\rangle\oplus\langle\omega(y\oplus\beta),\alpha\rangle.$$

Note that $\omega(y)\oplus\omega(y\oplus\beta)$ is a nonzero constant vector in $V_3$ for any fixed $y\in V_2$. Thus $f_5(z)\oplus f_5(z\oplus\gamma)$ is a nonzero linear function on $V_3$ for any fixed $y\in V_2$ and hence it is balanced. This proves that $\Delta(\gamma)=0$ with $\gamma=(\beta,\alpha)$ and $\beta\neq 0$.

Case 2: $\beta=0$. In this case

$$f_5(z)\oplus f_5(z\oplus\gamma) = \langle\omega(y),\alpha\rangle$$

is balanced for $\alpha=(0,1,1)$, $(1,0,0)$ and $(1,1,1)$. In other words, $\Delta(\gamma)=0$, if $\gamma=(0,\alpha)$ and $\alpha=(0,1,1)$, $(1,0,0)$ or $(1,1,1)$. It is straightforward to verify that $\Delta(\gamma)=2^4$, $-2^4$, $-2^4$ and $-2^4$ with $\gamma=(0,\alpha)$ and $\alpha=(0,0,1)$, $(0,1,0)$, $(1,0,1)$ and $(1,1,0)$ respectively. Obviously $\Delta(0)=2^5$. Thus $f_5$ satisfies the propagation criterion with respect to all but five vectors in $V_5$.

With $f_5$ as a basis, we now construct functions with $|\Re|=5$ over higher dimensional spaces. Let $t\geqq 5$ be odd and $s$ be even. And let $g$ be a function on $V_t$ that satisfies the propagation criterion with respect to all but five vectors in $V_t$, and $h$ be a bent function on $V_s$. Set

$$f(w) = g(v)\oplus h(u) \tag{37}$$

where $w=(v,u)$, $v\in V_t$ and $u\in V_s$. Then we have

**Lemma 9** *A function constructed by (37) satisfies* $|\Re|=5$.

*Proof.* Let $\xi(\beta)$ and $\eta(\alpha)$ be the sequences of $g(v\oplus\beta)$ and $h(u\oplus\alpha)$ respectively. Write $\zeta(\gamma)$ as the sequence of $f(w\oplus\gamma)=g(v\oplus\beta)\oplus h(u\oplus\alpha)$, where $\gamma=(\beta,\alpha)$. By definition, $\zeta(\gamma)=\xi(\beta)\times\eta(\alpha)$, where $\times$ is the *Kronecker product*. Hence we have

$$\begin{aligned} \Delta_f(\gamma) &= \langle\zeta(0),\zeta(\gamma)\rangle = \langle\xi(0)\times\eta(0),\xi(\beta)\times\eta(\alpha)\rangle \\ &= \langle\xi(0),\xi(\beta)\rangle\langle\eta(0),\eta(\alpha)\rangle \\ &= \Delta_h(\beta)\Delta_g(\alpha) \end{aligned}$$

where $\Delta_f$, $\Delta_g$ and $\Delta_h$ are well defined and the subscripts are used to distinguish the three different functions $f$, $g$ and $h$.

Since $h(u)$ is a bent function, $\Delta_h(\alpha) \neq 0$ if and only if $\alpha = 0$. On the other hand, since $g$ satisfies the propagation criterion with respect to all but five vectors 0, $\beta_1, \beta_2, \beta_3$ and $\beta_4$ in $V_t$, $\Delta_h(\beta) = 0$ if and only if $\beta \in \{0, \beta_1, \beta_2, \beta_3, \beta_4\}$. Thus $\Delta_g(\gamma) = 0$ if and only if $\gamma = (\beta, \alpha)$ with $\alpha = 0$ and $\beta \in \{0, \beta_1, \beta_2, \beta_3, \beta_4\}$. This proves that $f$ satisfies the propagation criterion with respect to all but five vectors in $V_{t+s}$. □

A function $f$ constructed by (37) is balanced if $g$ is balanced. As the function $f_5$ on $V_5$ defined in (36) is balanced, we have

**Theorem 7** *For any odd $n \geqq 5$, there exists a balanced function satisfying the propagation criterion with respect to all but five vectors in $V_n$.*

As an example, set $h(x_6, x_7) = x_6 x_7$ and

$$f_7(x_1, x_2, x_3, x_4, x_5, x_6, x_7) = f_5(x_1, x_2, x_3, x_4, x_5) \oplus h(x_6, x_7)$$

where $f_5$ is defined in (36). Note that $h(x_6, x_7)$ is a bent function on $V_2$, by Theorem 7, $f_7$ is a balanced function on $V_7$ that satisfies $|\Re| = 5$.

To close this section we note that one can also start with constructing a function $f_7$ on $V_7$ with $|\Re| = 5$ by using the same method as that for designing $f_5$.

# 9 Functions with $|\Re| = 6$

This section proves that there is *no* function with $|\Re| = 6$. Throughout this section $f$ is a function on $V_n$ satisfying the propagation criterion with respect to all but six vectors 0, $\beta_1, \beta_2$, $\beta_3$, $\beta_4$ and $\beta_5$ in $V_n$. As $\beta_1, \beta_2$, $\beta_3$, $\beta_4$ and $\beta_5$ are linearly dependent, the rank of $\{\beta_1, \beta_2, \beta_3, \beta_4, \beta_5\}$ can only be 3 or 4.

## 9.1 Rank = 3

Without loss of generality, we suppose that $\beta_1, \beta_2, \beta_3$ are linearly independent and are a basis of $\{\beta_1, \beta_2, \beta_3, \beta_4, \beta_5\}$. We can further assume that $\beta_1 = \alpha_1 = (0, \ldots, 0, 0, 0, 1)$, $\beta_2 = \alpha_2 = (0, \ldots, 0, 0, 1, 0)$, $\beta_3 = \alpha_4 = (0, \ldots, 0, 1, 0, 0)$. We distinguish two cases:

Case 1: $\beta_4 = \beta_1 \oplus \beta_2 = \alpha_1 \oplus \alpha_2 = \alpha_3$, and $\beta_5 = \beta_1 \oplus \beta_3 = \alpha_1 \oplus \alpha_4 = \alpha_5$.

Case 2: $\beta_4 = \beta_1 \oplus \beta_2 = \alpha_1 \oplus \alpha_2 = \alpha_3$, and $\beta_5 = \beta_1 \oplus \beta_2 \oplus \beta_3 = \alpha_1 \oplus \alpha_2 \oplus \alpha_4 = \alpha_7$.

We note that other cases can all be reduced to either Case 1 or Case 2. In both cases, a contradiction can be derived. The proofs are similar to that for the proof of Lemma 5. The main difference is that in Case 1, the matrix $P$ consists of the 0th, 1st, 2nd, 3rd, 4th and 5th rows, while in Case 2, it consists of the 0th, 1st, 2nd, 3rd, 4th and 7th rows of $H_n$. Hence in both cases, $P_j$ is a $6 \times 8$ matrix, and, as we did with the proof of Lemma 5, we use the 0th, 1st, 6th and 7th columns of $P_j$ to obtain the first set of four equations, and the 2nd, 3rd, 4th and 5th columns of $P_j$ to generate the second set of four equations.

## 9.2 Rank = 4

In this case, we suppose that $\beta_1, \beta_2, \beta_3, \beta_4$ are linearly independent and are a basis of $\{\beta_1, \beta_2, \beta_3, \beta_4, \beta_5\}$. We also assume that $\beta_1 = \alpha_1 = (0, \ldots, 0, 0, 0, 0, 1)$, $\beta_2 = \alpha_2 =$

$(0,\ldots,0,0,0,1,0)$, $\beta_3 = \alpha_4 = (0,\ldots,0,0,1,0,0)$, and $\beta_4 = \alpha_8 = (0,\ldots,0,1,0,0,0)$. Unlike the situation where the rank is 3, this time we distinguish three different cases to which all other cases can be reduced:

Case 1: $\beta_5 = \beta_1 \oplus \beta_2 = \alpha_1 \oplus \alpha_2 = \alpha_3$.

Case 2: $\beta_5 = \beta_1 \oplus \beta_2 \oplus \beta_3 = \alpha_1 \oplus \alpha_2 \oplus \alpha_4 = \alpha_7$.

Case 3: $\beta_5 = \beta_1 \oplus \beta_2 \oplus \beta_3 \oplus \beta_4 = \alpha_1 \oplus \alpha_2 \oplus \alpha_4 \oplus \alpha_8 = \alpha_{15}$.

The proof for the rank of 4 is a generalization of that for the rank of 3. In particular, in Case 1, the matrix $P$ consists of the 0th, 1st, 2nd, 3rd, 4th and 8th rows, in Case 2, of the 0th, 1st, 2nd, 4th, 7th and 8th rows, and in Case 3, of the 0th, 1st, 2nd, 4th, 8th and 15th rows of $H_n$. In each case, $P_j$ is a $6 \times 16$ matrix.

We derive a contradiction for each of the three cases. For Case 1, we establish four sets, each having four equations, from the 0th, 1st, 14th and 15th columns, the 2nd, 3rd, 12th and 13th columns, the 4th, 5th, 10th and 11th columns, and the 6th, 7th, 8th and 9th columns of $P_j$. For Case 2, we need a set of eight equations, which are constructed from the first eight columns of $P_j$. And For Case 3 a set of four equations is constructed from the first four columns of $P_j$. Note that each case defines a different $P_j$.

Careful analysis shows that:

**Theorem 8** *There exists no function on $V_n$ such that $|\Re| = 6$.*

## 10 Degrees of Propagation

In [9] it has been shown that if $f$ is a function on $V_n$ with $|\Re| = 2$, then, through a nonsingular linear transformation on input coordinates, $f$ can be converted into a function satisfying the propagation criterion of degree $n-1$. Similarly, when $|\Re| = 4$, the degree can be $\approx \frac{2}{3}n$. In this section we show that with $|\Re| = 5$, the degree can be $n-3$.

Assume that the four nonzero vectors in $\Re$ are $\beta_1$, $\beta_2$, $\beta_3$ and $\beta_4$, and that $\beta_1$, $\beta_2$ and $\beta_3$ are a basis of $\Re = \{0, \beta_1, \beta_2, \beta_3, \beta_4\}$. Let $B$ be an $n \times n$ nonsingular matrix on $GF(2)$ with the property that

$$\begin{aligned}\beta_1 B &= (1,\ldots,1,0,0,1)\\ \beta_2 B &= (1,\ldots,1,0,1,0)\\ \beta_3 B &= (1,\ldots,1,1,0,0)\end{aligned}$$

As $\beta_4 = \beta_1 \oplus \beta_2 \oplus \beta_3$, we have

$$\beta_4 B = (\beta_1 \oplus \beta_2 \oplus \beta_3)B = (1,\ldots,1,1,1,1).$$

Now let $g(x) = f(xB)$. Then $g$ satisfies the propagation criterion of degree $n-3$, as the only exceptional vectors are $(0,\ldots,0,0,0,0)$, $(1,\ldots,1,0,0,1)$, $(1,\ldots,1,0,1,0)$, $(1,\ldots,1,1,0,0)$ and $(1,\ldots,1,1,1,1)$. These discussions, together with Theorem 7, show that for any odd $n \geqq 5$, there exists balanced functions on $V_n$ that satisfy the propagation criterion of degree $n-3$ and do not possess a nonzero linear structure.

Table 1 shows structural properties of functions with $|\Re| \leqq 6$.

## 11 Final Remarks

We have presented a quantitative relationship between propagation characteristic and nonlinearity. We have shown that no functions satisfy the propagation criterion with respect to

| $\Re$ | $\{0\}$ | $\{0, \beta\}$ | $\{0, \beta_1, \beta_2, \beta_3\}$ | $\{0, \beta_1, \beta_2, \beta_3, \beta_4\}$ |
|---|---|---|---|---|
| Dimension $n$ | even | odd | even | odd |
| Form of function | bent | $cx_n \oplus$ $h(x_1, \ldots, x_{n-1})$, $h$ is bent. | $c_1 x_n \oplus c_2 x_{n-1} \oplus$ $h(x_1, \ldots, x_{n-2})$, $h$ is bent. | e.g. $f_5(x_1, \ldots, x_5) \oplus$ $h(x_6, \ldots, x_n)$, $f_5$ is defined in (36), $h$ is bent. |
| Nonzero linear structure(s) | No | $\beta$ | $\beta_1, \beta_2, \beta_3$ | No |
| Nonlinearity | $2^{n-1} - 2^{\frac{1}{2}n-1}$ | $2^{n-1} - 2^{\frac{1}{2}(n-1)}$ | $2^{n-1} - 2^{\frac{1}{2}n}$ | $2^{n-1} - 2^{\frac{1}{2}(n-1)}$ |
| Degree of propagation | $n$ | $n-1$ | $\approx \frac{2}{3}n$ | $n-3$ |
| Is $\Re$ a subspace ? | Yes | Yes | Yes | No. However, $\beta_1 \oplus \beta_2 \oplus \beta_3 \oplus \beta_4 = 0$. |
| Rank of $\Re$ | 0 | 1 | 2 | 3 |

Table 1: *Structural Properties of Highly Nonlinear Functions (Functions with three or six exceptional vectors do* not *exist.)*

all but three or six vectors. We have also completely decided the structures and construction methods of cryptographic functions that satisfy the propagation criterion with respect to all but two, four or five vectors. An interesting topic for future research is to investigate the structures of functions with seven or more exceptional vectors.

## 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

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

[2] J. F. Dillon. A survey of bent functions. *The NSA Technical Journal*, pages 191–215, 1972. (unclassified).

[3] J.-H. Evertse. Linear structures in blockciphers. In *Advances in Cryptology - EUROCRYPT'87*, volume 304, Lecture Notes in Computer Science, pages 249–266. Springer-Verlag, Berlin, Heidelberg, New York, 1988.

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

[5] 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.

[6] K. Nyberg. On the construction of highly nonlinear permutations. In *Advances in Cryptology - EUROCRYPT'92*, volume 658, Lecture Notes in Computer Science, pages 92–98. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[7] B. Preneel, R. Govaerts, and J. Vandewalle. Boolean functions satisfying higher order propagation criteria. In *Advances in Cryptology - EUROCRYPT'91*, volume 547, Lecture Notes in Computer Science, pages 141–152. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[8] B. Preneel, W. V. Leekwick, 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.

[9] J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. To appear in *Information and Computation*, 1994.

[10] J. Seberry, X. M. Zhang, and Y. Zheng. Relationships among nonlinearity criteria. Presented at *EUROCRYPT'94*, 1994.

[11] A. F. Webster. Plaintext/ciphertext bit dependencies in cryptographic system. Master's Thesis, Department of Electrical Engineering, Queen's University, Ontario, Cannada, 1985.

[12] A. F. Webster and S. E. Tavares. On the designs 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.

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