Structures of Cryptographic Functions with Strong Avalanche Characteristics (Extended Abstract)

Jennifer Seberry, Xian-Mo Zhang and Yuliang Zheng

Department of Computer Science
University of Wollongong, Wollongong, NSW 2522, Australia
{jennie, xianmo, yuliang}@cs.uow.edu.au

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 $N_f \geq 2^{n-1} - 2^{\frac{1}{2}(n+t)-1}$, 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 β_1, β_2, β_3 and β_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 [9], 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 [9] 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. A short summary of the results is presented in Table 1.

Due to the limit on space, detailed proofs will be left to the full version of the paper.

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 $(f(\alpha_0),\ f(\alpha_1),\dots,f(\alpha_{2^n-1}))$, and the *sequence* of f is a $(1,-1)$-sequence defined by $((-1)^{f(\alpha_0)},(-1)^{f(\alpha_1)},\dots,(-1)^{f(\alpha_{2^n-1})})$, where $\alpha_0=(0,\dots,0,0)$, $\alpha_1=(0,\dots,0,1)$, ..., $\alpha_{2^{n-1}-1}=(1,\dots,1,1)$. 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 $f(x_1,\dots,x_n)=a_1x_1\oplus\cdots\oplus a_nx_n\oplus c$, where $a_j,c\in GF(2)$, $j=1,2,\dots,n$. Furthermore f is called a *linear* function if $c=0$.

Definition 1. The *Hamming weight* of a $(0,1)$-sequence 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 $x=(x_1,\dots,x_n)$. The *nonlinearity* of f, denoted by N_f, is the minimal Hamming distance between f and all affine functions on V_n, i.e., $N_f=\min_{i=1,2,\dots,2^{n+1}} d(f,\varphi_i)$ where φ_1, φ_2, ..., $\varphi_{2^{n+1}}$ are all the affine functions on V_n.

Now we introduce the definition of propagation criterion.

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

1. the *propagation criterion with respect to* α if $f(x)\oplus f(x\oplus\alpha)$ is a balanced function, where $x=(x_1,\dots,x_n)$ and α is a vector in V_n.
2. the *propagation criterion of degree* k if it satisfies the propagation criterion with respect to all $\alpha\in V_n$ with $1\le W(\alpha)\le k$.

The above definition for propagation criterion is from [7]. Further work on the topic can be found in [6]. Note that the strict avalanche criterion (SAC) introduced by Webster and Tavares [10, 11] is equivalent to the propagation criterion of degree 1 and that the perfect nonlinearity studied by Meier and Staffelbach [4] 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 β and x, namely, $\langle \beta, x \rangle = \sum_{i=1}^{n} b_i x_i$, and $f(x) \oplus \langle \beta, x \rangle$ is regarded as a real-valued function.

Bent functions can be characterized in various ways [1, 2, 8, 12]. In particular the following four statements are equivalent:

(i) f is bent.
(ii) $\langle \xi, \ell \rangle = \pm 2^{\frac{1}{2}n}$ for any affine sequence ℓ of length 2^n, where ξ is the sequence of f.
(iii) f satisfies the propagation criterion with respect to all non-zero vectors in V_n.
(iv) M, the matrix of f, is a Hadamard matrix.

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

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

Let $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$ be the matrix of f and ξ be the sequence of f. Due to a very pretty result by R. L. McFarland (see Theorem 3.3 of [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 ℓ_i is the ith row of H_n, a Sylvester-Hadamard matrix of order 2^n. By Lemma 2 of [8], ℓ_i is the sequence of a linear function defined by $\varphi_i(x) = \langle \alpha_i, x \rangle$, where α_i is the ith vector in V_n according to the ascending alphabetical order.

Clearly

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

On the other hand, we always have

$$MM^T = (\Delta(\alpha_i \oplus \alpha_j)),$$

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 [8] states that the distance between two functions f_1 and f_2 on V_n can be expressed as $d(f_1, f_2) = 2^{n-1} - \frac{1}{2}\langle \xi_{f_1}, \xi_{f_2} \rangle$, where ξ_{f_1} and ξ_{f_2} are the sequences of f_1 and f_2 respectively. As an immediate consequence we have:

Lemma 5. *The nonlinearity of a function f on V_n can be calculated by*

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

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

Now we prove a central result of this paper:

Theorem 6. *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 $N_f \ge 2^{n-1} - 2^{\frac{1}{2}(n+t)-1}$, where t is the rank of $\Re$.*

It was observed by Nyberg in Proposition 3 of [5] (see also a detailed discussion in [9]) that knowing the linearity dimension, say ℓ, of a function f on V_n, the nonlinearity of the function can be expressed as $N_f = 2^\ell N_r$, where N_r is the nonlinearity of a function obtained by restricting f on an $(n-\ell)$-dimensional subspace of V_n. Therefore, in a sense Theorem 6 is complementary to Proposition 3 of [5].

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 7. *Let $n \geq 2$ be a positive integer and $2^n = p^2 + q^2$ where both $p \geq 0$ and $q \geq 0$ 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.*

Now we can prove

Theorem 8. *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 $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.

A further examination of the proof for Theorem 8 reveals that a function with $|\Re| = 2$ has a very simple structure as described below.

Corollary 9. *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 $GF(2)$.

By Theorem 8 and Corollary 9, 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 10. *Let $\psi_1, \ldots, \psi_k$ be linear functions on V_n which are linearly independent. Set*

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

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

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

Proof. Note that (i) and (ii) are equivalent. Clearly, any nonzero linear combination of $\varphi_1, \ldots, \varphi_k$ is a nonzero linear function and thus it is balanced. Consequently, this lemma is equivalent to Lemma 7 of [9]. □

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

Theorem 11. *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 $k \le n$ by contradiction. Assume that $\beta_1, \ldots, \beta_k$ are linearly independent. Let ξ be the sequence of f.

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

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

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

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

Now let P be a matrix that consists of the 0th, β_1th, …, β_kth rows of H_n. Here we regard β_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

$$(\Delta(0), \Delta(\beta_1), \ldots, \Delta(\beta_k))P = (a_0^2, a_1^2, \ldots, a_{2^n-1}^2) \qquad (3)$$

where 0 in (3) is identical to α_0 in (2).

Write $P = (p_{ij})$, $i = 0, 1, \ldots k$, $j = 0, 1, \ldots, 2^n - 1$. As the top row of P is $(1, 1, \ldots, 1)$, a_j^2 in (3) can be expressed as

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

$j = 0, 1, \ldots, 2^n - 1$. Let P^* be the submatrix of P obtained by removing the top row from P. As was mentioned earlier, the β_ith row of H_n is the sequence of a linear function defined by $\psi_i(x) = \langle \beta_i, x \rangle$ (see Lemma 2 of [8]). 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 10, 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 7, $a_j^2 = a_{j_0}^2 = 2^n$. 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 7, $a_j^2 = 2^{n+1}$ 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

$$\sum_{i=1}^{k} p_{ij} \Delta(\beta_i) = c_j 2^n \qquad (4)$$

where $c_j = \pm 1$, $j = 0, 1, \ldots, 2^n - 1$. For each fixed j rewrite (4) as

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

From Lemma 10, 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 β_1, we have $\Delta(\beta_1) \neq 0$ and $c_j + c_{j_0} \neq 0$. This implies $c_j + c_{j_0} = \pm 2$, 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 10, there exists an s such that

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

This gives us

$$\sum_{i=1}^{k} p_{is}\Delta(\beta_i) = \sum_{i=1}^{k} b_i \Delta(\beta_i) = \sum_{i=1}^{k} b_i b_i 2^n = k2^n. \tag{5}$$

Since $k > 1$, (5) contradicts (4).

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 11 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 11 we have

Theorem 12. *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 13. *Let $n \geq 3$ be a positive integer and $2^n = \sum_{j=1}^{4} p_j^2$ where each $p_j \geq 0$ 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.

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

Theorem 14. *If f, a function on V_n, satisfies the propagation criterion with respect to all but four vectors (0, β_1, β_2, β_3) in V_n. Then*

(i) $\Re = \{0, \beta_1, \beta_2, \beta_3\}$ *forms a two-dimensional linear subspace of V_n,*
(ii) n must be even,
(iii) β_1, β_2 and β_3 must be linear structures of f,
(iv) the nonlinearity of f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}n}$.

As a result we have

Corollary 15. *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}.

In [8], 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 15 and 9 with results shown in [8], we conclude that *the methods of repeating bent functions presented in [8] 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 $\Re = \{0, \beta_1, \beta_2, \beta_3, \beta_4\}$. In the full paper we show the following result:

Theorem 16. *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.

8.1 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

$$f_5(z) = f_5(y,x) = \langle \omega(y), x \rangle \tag{6}$$

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

$$\begin{aligned} f_5(y_1,y_2,x_1,x_2,x_3) = (1 \oplus y_1)(1 \oplus y_2)x_1 \oplus (1 \oplus y_1)y_2x_2 \oplus \\ y_1(1 \oplus y_2)(x_1 \oplus x_2) \oplus y_1y_2(x_2 \oplus x_3) \end{aligned} \tag{7}$$

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 φ is regarded as a linear function on V_3. By Lemma 1 of [8], ℓ_{100}, ℓ_{010}, ℓ_{110}, ℓ_{011} are four different rows of H_3. By Lemma 2 of [8], 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 $t \geq 5$ 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

$$f(w) = g(v) \oplus h(u) \tag{8}$$

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

Lemma 17. *A function constructed by (8) 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 Δ_f, Δ_g and Δ_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 β_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 (8) is balanced if g is balanced. As the function f_5 on V_5 defined in (7) is balanced, we have

Theorem 18. *For any odd $n \geq 5$, 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 (7). Note that $h(x_6, x_7)$ is a bent function on V_2, by Theorem 18, 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 $|\Re| = 6$

In the full paper we prove that there is *no* function with $|\Re| = 6$.

Theorem 19. *There exists no function on V_n such that $|\Re| = 6$.*

10 Degrees of Propagation

In [8] 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 β_1, β_2, β_3 and β_4, and that β_1, β_2 and β_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 18, show that for any odd $n \geq 5$, 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 $|\Re| \leq 6$.

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.

References

1. Adams, C. M., Tavares, S. E.: Generating and counting binary bent sequences. IEEE Transactions on Information Theory **IT-36 No. 5** (1990) 1170–1173
2. Dillon, J. F.: A survey of bent functions. The NSA Technical Journal (1972) 191–215

$\Re$	$\{0\}$	$\{0, \beta\}$	$\{0, \beta_1, \beta_2, \beta_3\}$	$\{0, \beta_1, \beta_2, \beta_3, \beta_4\}$
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 (7), h is bent.
Nonzero linear structure(s)	No	β	$\beta_1, \beta_2, \beta_3$	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.)*

3. Evertse, J.-H.: Linear structures in blockciphers. In Advances in Cryptology - EUROCRYPT'87 (1988) vol. 304, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 249–266
4. Meier, W., Staffelbach, O.: Nonlinearity criteria for cryptographic functions. In Advances in Cryptology - EUROCRYPT'89 (1990) vol. 434, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 549–562
5. Nyberg, K.: On the construction of highly nonlinear permutations. In Advances in Cryptology - EUROCRYPT'92 (1993) vol. 658, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 92–98
6. Preneel, B., Govaerts, R., Vandewalle, J.: Boolean functions satisfying higher order propagation criteria. In Advances in Cryptology - EUROCRYPT'91 (1991) vol. 547, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 141–152
7. Preneel, B., Leekwijck, W. V., Linden, L. V., Govaerts, R., Vandewalle, J.: Propagation characteristics of boolean functions. In Advances in Cryptology - EUROCRYPT'90 (1991) vol. 437, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 155–165
8. Seberry, J., Zhang, X. M., Zheng, Y.: Nonlinearity and propagation characteristics of balanced boolean functions. To appear in *Information and Computation* 1994
9. Seberry, J., Zhang, X. M., Zheng, Y.: Relationships among nonlinearity criteria. Presented at *EUROCRYPT'94* 1994
10. Webster, A. F.: Plaintext/ciphertext bit dependencies in cryptographic system. Master's Thesis, Department of Electrical Engineering, Queen's University, Ontario, Cannada 1985

11. Webster, A. F., Tavares, S. E.: On the design of S-boxes. In Advances in Cryptology - CRYPTO'85 (1986) vol. 219, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 523–534
12. Yarlagadda, R., Hershey, J. E.: Analysis and synthesis of bent sequences. IEE Proceedings (Part E) **136** (1989) 112–123