New Lower Bounds on Nonlinearity and A Class of Highly Nonlinear Functions

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

[1] The University of Wollongong, Wollongong, NSW 2522, Australia
xianmo@cs.uow.edu.au
[2] Monash University, Frankston, Melbourne, VIC 3199, Australia
yuliang@mars.fcit.monash.edu.au

Abstract. Highly nonlinear Boolean functions occupy an important position in the design of secure block as well as stream ciphers. This paper proves two new lower bounds on the nonlinearity of Boolean functions. Based on the study of these new lower bounds, we introduce a class of highly nonlinear Boolean functions on odd dimensional spaces and show examples of such functions.

1 Introduction

It is well-known that highly nonlinear (Boolean) functions play an important role in designing secure stream ciphers (see [6, 13]). The dramatic success of linear cryptanalysis recently discovered by Matsui in [8] has further extended the significance of the functions to the design and analysis of block ciphers.

A challenging research topic in cryptography is to design (Boolean) functions that satisfy some or all of the critical criteria each of which forecasts the nonlinear characteristics of a function from a different perspective. These criteria include nonlinearity, propagation characteristic, correlation immunity, algebraic degree, strict avalanche characteristic, global avalanche characteristic, and so on.

This paper represents a continuation of our earlier work [16] in which two lower and two upper bounds on nonlinearity have been developed. The main difference between our present work and the work in [16] is that the bounds in [16] are expressed in terms of partial information on auto-correlations of a function, while the bounds in this paper are represented using information on the structure of $\Re$ which is the set of vectors where a function does not satisfy the propagation criterion.

The two new lower bounds motivate us to introduce a class of highly nonlinear functions which exist only on odd dimensional spaces. This should be contrasted with bent functions which exist only on even dimensional spaces. Properties of this class of functions are potentially very useful in practice. These properties include that the functions are highly nonlinear, can be very easily made balanced, and have a very simple spectrum of Walsh-Hadamard transform.

The rest of this paper is organized as follows: Section 2 introduces basic notations and relevant results. Section 3 studies functions whose $\Re$ is covered by a coset and shows that their nonlinearity is $2^{n-1} - 2^{\frac{1}{2}(n-1)}$. By extending this result, two new lower bounds on nonlinearity are derived in Section 4, where a comparison with a previously known lower bound is also carried out. Section 5 introduces a class of highly nonlinear functions. In Section 6 three types of functions are shown to fall into the class of highly nonlinear functions. Section 7 concludes the paper.

2 Preliminaries

We consider Boolean functions from V_n to $GF(2)$ (or simply functions on V_n), where 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 $\alpha_0 = (0,\ldots,0,0)$, $\alpha_1 = (0,\ldots,0,1)$, $\ldots$, $\alpha_{2^{n-1}-1} = (1,\ldots,1,1)$. 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 $c = 0$.

Next we introduce the definition of propagation criterion [9].

Definition 1. Let f be a function on V_n. We say that f satisfies

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

$f(x) \oplus f(x \oplus \alpha)$ is also called the *directional derivative* of f in the direction α. Further work on the topic can be found in [15]. To simplify our discussions, a notation indicated by $\Re$ is introduced:

Notation 1 *Let f be a function on V_n. The set of vectors in V_n with respect to which f does* not *satisfy the propagation criterion is denoted by $\Re$.*

Given two sequences $a = (a_1,\ldots,a_m)$ and $b = (b_1,\ldots,b_m)$, their component-wise sum is defined by $a + b = (a_1 + b_1,\ldots,a_m + b_m)$, and their component-wise product by $a * b = (a_1b_1,\ldots,a_mb_m)$. The scalar product $\langle a, b\rangle$ of a and b is defined as the sum of the components in $a * b$. Note that depending on where the components of a and b are drawn from, the meaning of an "addition" or "multiplication" operation may vary.

Definition 2. Let f be a function on V_n. For a vector $\alpha \in V_n$, denote by $\xi(\alpha)$ the sequence of $f(x \oplus \alpha)$. Thus $\xi(0)$ is the sequence of f itself and $\xi(0) * \xi(\alpha)$ is the sequence of $f(x) \oplus f(x \oplus \alpha)$. The *auto-correlation* of f with a shift α is defined as

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

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

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

Let ℓ_i, $0 \le i \le 2^n - 1$, be the i row (column) of H_n. By Lemma 1 of [11], ℓ_i is the sequence of a linear function $\varphi_i(x)$ defined by the scalar product $\varphi_i(x) = \langle \alpha_i, x\rangle$, where α_i is the i-th vector in V_n according to the ascending lexicographic order.

Definition 3. Let f be a function on V_n. The Walsh-Hadamard transform of f is defined as

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

where $\alpha = (a_1, \ldots, a_n) \in V_n$, $x = (x_1, \ldots, x_n)$, $\langle \alpha, x\rangle$ is the scalar product of α and x, namely, $\langle \alpha, x\rangle = \bigoplus_{i=1}^n a_i x_i$, and $f(x) \oplus \langle \alpha, x\rangle$ is regarded as a real-valued function.

Definition 4. 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 minimum Hamming distance between f and all affine functions on V_n, i.e., $N_f = \min_{i=0,1,\ldots,2^{n+1}-1} d(f, \varphi_i)$ where φ_0, φ_1, ..., $\varphi_{2^{n+1}-1}$ are all the affine functions on V_n.

Note that the maximum nonlinearity of functions on V_n coincides with the covering radius of the first order binary Reed-Muller code $RM(1,n)$ of length 2^n, which is bounded from above by $2^{n-1} - 2^{\frac{1}{2}n-1}$ (see for instance [4]). Hence $N_f \le 2^{n-1} - 2^{\frac{1}{2}n-1}$ for any function on V_n.

Definition 5. A function f on V_n is called a *bent* function if its Walsh-Hadamard transform satisfies

$$\hat{f}(\alpha) = \pm 1$$

for all $\alpha \in V_n$.

Bent functions can be characterized in various ways [1, 5, 10, 11, 14]. A characterization of particular interest can be found in [5, 10]:

Lemma 6. *The following statements are equivalent:*

(i) f *is bent,*
(ii) f *satisfies the propagation criterion with respect to all non-zero vectors in* V_n*,*
(iii) $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$*, 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 $2^{n-1} - 2^{\frac{1}{2}n-1}$.

The following lemma will be used in this paper (for a proof see for instance Lemma 6 of [11].)

Lemma 7. *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 $\ell_0, \ldots, \ell_{2^n-1}$ are the rows of H_n, namely, the sequences of the linear functions on V_n.

We note that as the number of linear functions on V_n is exponential in n, it is impractical to calculate N_f for a large n by examining all linear functions against the formula in Lemma 7.

As there is a natural correspondence between an integer in $[0, \ldots, 2^n - 1]$ and a vector in V_n, in the following discussions we will use them interchangeably. The proof of the next lemma is lengthy and will be provided in the full version of this paper.

Lemma 8. *Consider the rows (columns) ℓ_j of H_n, $j = 0, 1, \ldots, 2^n - 1$. Then*

(i) $\ell_\beta = \ell_\alpha * \ell_{\alpha\oplus\beta}$, *for any vectors α and β in V_n,*
(ii) the i-th entry of $\ell_\alpha + \ell_{\alpha\oplus\beta}$ is zero (nonzero) if and only if the i-th entry of $\ell_0 + \ell_\beta$ is zero (nonzero) where $i = 0, 1, \ldots, 2^n - 1$,
(iii) if the i-th entry of $\ell_\alpha + \ell_{\alpha\oplus\beta}$ is nonzero, then it is twice as large as the i-th entry of ℓ_α.

Note that here $*$ and $+$ indicate component-wise product and component-wise sum respectively.

The following result can be found in [17]:

Lemma 9. *Let $n \ge 2$ be a positive integer and $2^n = p^2 + q^2$ where both $p \ge 0$ and $q \ge 0$ 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.*

3 Functions Whose $\Re$ is Covered by a Coset

Recall that $\Re$ denotes the set of vectors in V_n where f, a function on V_n, does not satisfies the propagation criterion (see Notation 1). In this section we show that when vectors in $\Re$ satisfy a special property, namely $\Re$ is covered by a coset, the nonlinearity of f is $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$, a very high value. This result forms the basis of our two new lower bounds to be developed in Section 4.

Let W be a ρ-dimensional subspace of V_n. Then V_n can be expressed as the union of $2^{n-\rho}$ disjoint 2^ρ-sets:

$$V_n = W \cup (\beta_1 \oplus W) \cup \cdots \cup (\beta_{2^{n-\rho}-1} \oplus W)$$

where $\beta_j \in V_n$ and each $\beta_j \oplus W$, as well as W, is called a *coset*.

Let ξ be the sequence of f. The following is a special form of the Wiener-Khintchine Theorem [2]:

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

Now we prove a theorem on which all the other results in this paper is based.

Theorem 10. *Let f be a function on V_n with $|\Re| > 1$. Let W be a ρ-dimensional subspace of V_n such that $\Re - \{0\} \subset \beta \oplus W$ for a vector $\beta \in V_n - W$ ($\Re$ is said to be covered by the coset $\beta \oplus W$). Then*

(i) n must be odd, and
(ii) the nonlinearity N_f of f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.

Proof. First we note that $\beta \notin W$ implies $\rho < n$. As W is a subspace of V_n, there is another $(n-\rho)$-dimensional subspace Ω of V_n such that $\langle \alpha, \gamma \rangle = 0$ for each $\alpha \in \Omega$ and each $\gamma \in W$.

As $\beta \notin W$, there is a nonzero vector $\alpha \in \Omega$ such that $\langle \alpha, \beta \rangle = 1$. Now write

$$W = \{\gamma_0, \gamma_1, \gamma_2, \ldots, \gamma_{2^\rho-1}\}$$

where $\gamma_0 = 0$. Hence

$$\langle \beta \oplus \gamma_j, \alpha \rangle = 1 \tag{3}$$

for all $j = 0, 1, 2, \ldots, 2^\rho - 1$. On the other hand, since $\Re - \{0\} \subset \beta \oplus W$, (2) can be specialized as

$$(\Delta(\alpha_0), \Delta(\beta), \Delta(\beta \oplus \gamma_1), \ldots, \Delta(\beta \oplus \gamma_{2^\rho-1}))D = (\langle \xi, \ell_0 \rangle^2, \ldots, \langle \xi, \ell_{2^n-1} \rangle^2) \tag{4}$$

where D is a $(1+2^\rho) \times 2^n$ sub-matrix of H_n, consisting of the 0-th, β-th, $\beta \oplus \gamma_1$-th, …, and $\beta \oplus \gamma_{2^\rho-1}$-th rows of H_n. Note that (4) holds regardless of the order of γ_1, γ_2, …, $\gamma_{2^\rho-1}$, since we have defined the order of the rows of D to be identical to that of $\Delta(\beta), \Delta(\beta \oplus \gamma_1), \ldots, \Delta(\beta \oplus \gamma_{2^\rho-1})$.

It follows from Lemma 1 of [17] that the entry on the cross of the α_i-th and α_j-th columns of H_n is $(-1)^{\langle \alpha_i, \alpha_j \rangle}$. Let η_γ denote the γ-th column of D. Note that η_0 is of all-one.

Now we turn our attention to the vector α mentioned earlier in the proof. Recall that the α-th column of H_n, denoted by ℓ_α, is the sequence of a linear function defined by $\psi(x) = \langle \alpha, x \rangle$. Thus, the δ-th entry of ℓ_α is -1 if and only if $\psi(\delta) = 1$, where $\delta \in V_n$. What (3) means is that $\psi(\beta \oplus \gamma_j) = 1$. Hence the β-th, $\beta \oplus \gamma_1$-th, …, $\beta \oplus \gamma_{2^\rho-1}$-th entries of ℓ_α are all -1. Since η_α is a subsequence of ℓ_α, the entries of η_α are all -1 except for the top entry whose value is one. Hence we have

$$\eta_0 + \eta_\alpha = (2, 0, \ldots, 0)^T. \quad (5)$$

By Lemma 8,

$$\eta_\gamma + \eta_{\gamma\oplus\alpha} = \eta_0 + \eta_\alpha = (2, 0, \ldots, 0)^T. \quad (6)$$

where γ is an arbitrary vector in V_n.

Now we restrict e_γ to be a sequence of length 2^n, whose the γ-th and $\alpha \oplus \gamma$-th entries are both one, while all the other entries are zero. Then by the definition of D, we have $De_\gamma^T = \eta_\gamma + \eta_{\gamma\oplus\alpha} = (2, 0, \ldots, 0)^T$. Multiplying both sides of (4) by e_γ^T gives rise to

$$2\Delta(\alpha_0) = \langle \xi, \ell_\gamma \rangle^2 + \langle \xi, \ell_{\alpha\oplus\gamma} \rangle^2. \quad (7)$$

Note that $\alpha_0 = 0$. Hence $\langle \xi, \ell_\gamma \rangle^2 + \langle \xi, \ell_{\alpha\oplus\gamma} \rangle^2 = 2^{n+1}$. To complete the proof, we consider two cases: n even and n odd.

Case 1: n is even. By Lemma 9, $\langle \xi, \ell_\gamma \rangle^2 = \langle \xi, \ell_{\alpha\oplus\gamma} \rangle^2 = 2^n$. Note that γ is arbitrary. This implies that f is a bent function satisfying $\Re = \{0\}$, which contradicts the assumption that $|\Re| > 1$. Hence n cannot be even.

Case 2: n is odd. By Lemma 9, one of $\langle \xi, \ell_\gamma \rangle^2$ and $\langle \xi, \ell_{\alpha\oplus\gamma} \rangle^2$ takes the value 2^{n+1} and the other zero. As γ is arbitrary, by Lemma 7, the nonlinearity N_f of f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.

The following corollary of Theorem 10 is more useful in situations where the outcomes of summing vectors in $\Re$ are easy to verify.

Corollary 11. *Let f be a function on V_n and $|\Re| > 1$. Assume that for any t with $0 \le t \le |\Re|$ and any t nonzero vectors $\gamma_1, \gamma_2, \ldots, \gamma_t$ in $\Re$, whenever $\gamma_1 \oplus \gamma_2 \oplus \cdots \oplus \gamma_t = 0$ is satisfied, t is even. Then the following two statements hold:*

(i) n is odd,
(ii) the nonlinearity N_f of f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.

Proof. First we note that the rank of $\alpha \oplus \Re$ is a constant for all $\alpha \in \Re$. To prove this claim, one can verify that for any vectors α, $\beta \in \Re$, each vector in $\alpha \oplus \Re$ is a linear combination of vectors in $\beta \oplus \Re$. Linear algebra tells us that the rank of $\alpha \oplus \Re$ must be less than or equal to that of $\beta \oplus \Re$. Symmetrically, the rank of $\beta \oplus \Re$ must be less than or equal to that of $\alpha \oplus \Re$. Hence the claim is true.

Now fix a nonzero vector $\gamma \in V_n$. Let W be the subspace consisting of all the linear combinations of vectors in $\gamma \oplus \Re$. We show that $\gamma \notin W$. Assume for contradiction that $\gamma \in W$. Then γ can be expressed as $\gamma = \bigoplus_1^s (\gamma \oplus \gamma_j')$, where $\gamma_j' \in \Re$ and $s \le |\Re|$. Thus we have $\gamma \oplus [\bigoplus_1^s (\gamma \oplus \gamma_j')] = 0$. When s is odd, the equation becomes $\bigoplus_1^s \gamma_j' = 0$. This contradicts the assumption on f, namely when $\bigoplus_1^s \gamma_j' = 0$, s must be even. Consequently, we must have $\gamma \notin W$.

Finally the corollary follows from Theorem 10 by noting the fact that $\Re - \{0\} \subset \gamma \oplus (\gamma \oplus \Re) \subset \gamma \oplus W$, i.e., $\Re$ is covered by the coset $\gamma \oplus W$ with $\gamma \notin W$.

Functions satisfying the conditions in Corollary 11 do exist. See Examples 1 and 2 in Section 6.

4 Two New Lower Bounds on Nonlinearity

This section extends Theorem 10 in two different directions to obtain two separate lower bounds on the nonlinearity of Boolean functions. A comparison with a lower bound implied by a result in [3] is also carried out.

First we consider a function f on V_n whose $\Re$ is covered by a coset together with t other vectors. We show that the nonlinearity of f is bounded from below by $2^{n-1} - 2^{\frac{1}{2}(n-1)}\sqrt{1+t}$.

Theorem 12. *Let f be a function on V_n and $|\Re| > 1$ and W be a ρ-dimensional subspace of V_n. Assume that there exist $t+1$ vectors in $V_n - W$, say β_1, ..., β_t and β, such that*

$$\Re - \{0\} \subset \{\beta_1, \ldots, \beta_t\} \cup (\beta \oplus W).$$

Then the nonlinearity N_f of f satisfies

$$N_f \geq 2^{n-1} - 2^{\frac{1}{2}(n-1)}\sqrt{1+t}.$$

Proof. The main ideas behind the proof of this theorem are similar to those of Theorem 10. Here we only highlight the major differences with the proof of Theorem 10.

As in the proof of Theorem 10, let $W = \{\gamma_0, \gamma_1, \gamma_2, \ldots, \gamma_{2^\rho-1}\}$. Then since $\Re - \{0\} \subset \{\beta_1, \ldots, \beta_t\} \cup \beta \oplus W$, (2) will be specialized as

$$\begin{aligned}(\Delta(\alpha_0), \Delta(\beta_1), \ldots, \Delta(\beta_t), \Delta(\beta), \quad & \Delta(\beta \oplus \gamma_1), \ldots, \Delta(\beta \oplus \gamma_{2^\rho-1}))D \\ &= (\langle \xi, \ell_0 \rangle^2, \ldots, \langle \xi, \ell_{2^n-1} \rangle^2) \qquad (8)\end{aligned}$$

where D is a $(1+t+2^\rho) \times 2^n$ sub-matrix of H_n, consisting of the 0-th, β_1-th, ..., β_t-th, β-th, $\beta \oplus \gamma_1$-th, ..., $\beta \oplus \gamma_{2^\rho-1}$-th rows of H_n.

Now instead of (5), we have

$$\eta_0 + \eta_\alpha = (** \cdots *) \qquad (9)$$

where the components of $(** \cdots *)$ are all from $\{0, 2, -2\}$ and $(** \cdots *)$ contains at least 2^ρ zeros. Thus $De_\gamma^T = \eta_\gamma + \eta_{\alpha\oplus\gamma} = \eta_0 + \eta_\alpha = (** \cdots *)$ contains at most $(1+t)$ 2s or -2s, where e_γ is a sequence of length 2^n whose γ-th and $\alpha \oplus \gamma$-th entries are one and all the other entries are zero. Multiplying both sides of (8) by e_γ^T and noting the fact that $|\Delta(\gamma)| \leq 2^n$ for all $\gamma \in V_n$, we have $\langle \xi, \ell_\gamma \rangle^2 + \langle \xi, \ell_{\alpha\oplus\gamma} \rangle^2 \leq 2(1+t)2^n$. Hence $|\langle \xi, \ell_\gamma \rangle| \leq 2^{n+1}\sqrt{1+t}$. As γ is arbitrary, by Lemma 7, $N_f \geq 2^{n-1} - 2^{\frac{1}{2}(n-1)}\sqrt{1+t}$.

While Theorem 12 extends Theorem 10 by adding a parameter t, the next theorem does it by taking into account two parameters s and w, where s is the number of nonzero vectors in $\Re$, and w is the maximum Hamming weight of vectors determined by $\Re$.

Theorem 13. *Let f be a function on V_n with $|\Re| > 1$. Set $\Re = \{\beta_0, \beta_1, \ldots, \beta_s\}$ where $\beta_0 = 0$. Let $w = \max\{W_h(\varphi_{\beta_1}(x), \ldots, \varphi_{\beta_s}(x)) | x \in V_n\}$, where $\varphi_{\beta_i}(x) = \langle \beta_i, x\rangle$ is a linear function on V_n defined by β_i. Then the nonlinearity N_f of f satisfies $N_f \geq 2^{n-1} - 2^{\frac{1}{2}(n-1)}\sqrt{1+s-w}$.*

Proof. Again the proof is similar to that of Theorem 10. Under the condition stated in the theorem, (2) can be specialized as

$$(\Delta(\beta_0), \Delta(\beta_1), \ldots, \Delta(\beta_s))D = (\langle \xi, \ell_0\rangle^2, \ldots, \langle \xi, \ell_{2^n-1}\rangle^2) \quad (10)$$

where D is a $(1+s) \times 2^n$ sub-matrix of H_n, consisting of the β_0-th, β_1-th, ..., β_s-th rows of H_n. Since $w = \max\{W_h(\varphi_{\beta_1}(x), \ldots, \varphi_{\beta_s}(x)) | x \in V_n\}$, there is a vector $\alpha \in V_n$ such that $W_h(\varphi_{\beta_1}(\alpha), \ldots, \varphi_{\beta_s}(\alpha)) = w$. Correspondingly, the α-th column of D contains exactly w minus components.

The crux of the proof is that $De_\gamma^T = \eta_\gamma + \eta_{\gamma\oplus\alpha} = \eta_0 + \eta_\alpha = (* * \cdots *)$, where $(* * \cdots *)$ contains exactly $1+s-w$ non-zeros, and each component of $(* * \cdots *)$ comes from $\{0, 2, -2\}$. Multiplying both sides of (10) by e_γ^T leads to $\langle \xi, \ell_\gamma\rangle^2 + \langle \xi, \ell_{\alpha\oplus\gamma}\rangle^2 \leq 2(1+s-w)2^n$, and $|\langle \xi, \ell_\gamma\rangle| \leq 2^{\frac{1}{2}(n+1)}\sqrt{1+s-w}$. As γ is arbitrary in V_n, we have $N_f \geq 2^{n-1} - 2^{\frac{1}{2}(n-1)}\sqrt{1+s-w}$.

As was pointed out in [16], the work by Carlet [3] implies a lower bound on nonlinearity:

$$N_f \geq 2^{n-1} - 2^{\frac{1}{2}n-1}\sqrt{|\Re|}$$

for any function f on V_n. With Theorem 13, we have $w \geq 0$ and $1+s-w = |\Re| - w \geq |\Re|$. Hence

$$2^{n-1} - 2^{\frac{1}{2}(n-1)}\sqrt{1+s-w} \geq 2^{n-1} - 2^{\frac{1}{2}n-1}\sqrt{|\Re|}$$

namely, Theorem 13 gives a better lower bound on nonlinearity than that implied in [3].

5 A Class of Highly Nonlinear Functions

In an earlier work [11], we constructed, in a recursive manner, balanced Boolean functions that have a nonlinearity far higher than that achievable by all previously known methods. The functions obtained in [11], however, have a small shortcoming in that their algebraic representation are complicated and their spectra of Walsh-Hadamard transform are hard to analyze.

Observing the two lower bounds in Theorems 12 and 13, we ask a natural question: are there functions that achieve a nonlinearity of $2^{n-1} - 2^{\frac{1}{2}n-1}$ with a *simple* spectrum of Walsh-Hadamard transform. It turns out that the answer to the question is affirmative. Among the functions that support the affirmative answer, of particular interest are those whose Walsh-Hadamard transforms take the value of 0 or $\pm 2^{\frac{1}{2}}$.

From Case 2 in the proof of Theorem 10 we conclude that

Corollary 14. *Functions satisfying the conditions in Corollary 11 or in Theorem 10 all satisfy the property that their Walsh-Hadamard transforms take the value of* 0 *or* $\pm 2^{\frac{1}{2}}$.

We now compare these functions with bent functions. Recall Definition 5 and Lemma 6. In particular, we know that if g is a bent function on V_n, then n must be even, and the function satisfies $\langle \eta, \ell_i \rangle = \pm 2^{\frac{1}{2}n}$ for all $j = 0, 1, \ldots, 2^n - 1$, where η is the sequence of g.

Corollary 15. *A function* f *on* V_n *whose Walsh-Hadamard transform takes the value of* 0 *or* $\pm 2^{\frac{1}{2}}$ *has the following properties*

(i) it exists only for n *odd,*
(ii) $\langle \xi, \ell_i \rangle = 0$ *for exactly half of the* 2^n *rows* ℓ_i *in* H_n*, and* $\langle \xi, \ell_i \rangle = \pm 2^{\frac{1}{2}(n+1)}$ *for the other half of the rows* ℓ_i *in* H_n*, where* ξ *denotes the sequence of* f*,*
(iii) the nonlinearity N_f *of* f *satisfies* $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$,
(iv) let A *be an arbitrary nonsingular* $n \times n$ *matrix over GF(2) and* β *be any vector in* V_n*, then the Walsh-Hadamard transform of* $g(x) = f(Ax \oplus \beta)$ *too takes the value of* 0 *or* $\pm 2^{\frac{1}{2}}$.
(v) for any affine function on V_n*, say* φ*, the Walsh-Hadamard transform of* $f \oplus \psi$ *takes the value of* 0 *or* $\pm 2^{\frac{1}{2}}$.

Property (i) follows from the spectrum of the Walsh-Hadamard transform of f. Property (ii) can be easily proved using Parseval's equation $\sum_{i=0}^{2^n-1} \langle \xi, \ell_i \rangle^2 = 2^{2n}$ (see Page 416, [7]). Property (iii) follows from Property (ii).

To prove Property (iv), we set $u = Ax \oplus \beta$. Let η be the sequence of g and ℓ be any row of H_n, i.e., the sequence of a linear function, say φ, on V_n. Note that φ can be expressed as $\varphi(x) = \langle \alpha, x \rangle$, $\alpha \in V_n$. Consider

$$\begin{aligned} \langle \eta, \ell \rangle &= \sum_{x \in V_n} (-1)^{g(x) \oplus \langle \alpha, x \rangle} \\ &= \sum_{x \in V_n} (-1)^{f(Ax \oplus \beta) \oplus \langle \alpha, x \rangle} \\ &= \sum_{u \in V_n} (-1)^{f(u) \oplus \langle \alpha, A^{-1}(u \oplus \beta) \rangle} \end{aligned} \tag{11}$$

Since $\langle \alpha, A^{-1}(u \oplus \beta) \rangle$ is an affine function, there are $\alpha' \in V_n$ and $c \in GF(2)$ such that $\langle \alpha, A^{-1}(u \oplus \beta) \rangle = \langle \alpha', u \rangle \oplus c$. Hence (11) can be rewritten as

$$\langle \eta, \ell \rangle = \sum_{x \in V_n} (-1)^{g(x) \oplus \langle \alpha, x \rangle} = \sum_{u \in V_n} (-1)^{f(u) \oplus \langle \alpha', u \rangle \oplus c} \tag{12}$$

where $u = Ax \oplus \beta$. Since the Walsh-Hadamard transform of f takes the value of 0 or $\pm 2^{\frac{1}{2}}$, $\sum_{u \in V_n} (-1)^{f(u) \oplus \langle \alpha', u \rangle \oplus c} = \pm 2^{\frac{1}{2}(n+1)}$. Thus (12) implies that the Walsh-Hadamard transform of g too takes the value of 0 or $\pm 2^{\frac{1}{2}}$.

Finally we show that Property (v) is satisfied. Similarly to the proof of (iv), let $\varphi = \langle \alpha, x \rangle$ be any linear function on V_n. Consider

$$\sum_{x \in V_n} (-1)^{(f(x) \oplus \varphi(x)) \oplus \langle \alpha, x \rangle} = \sum_{x \in V_n} (-1)^{f(x) \oplus \psi(x) \oplus \varphi(x)} \tag{13}$$

Since $\psi \oplus \varphi$ is also a linear function, (13) can only take the value of 0 or $\pm 2^{\frac{1}{2}(n+1)}$.

Both bent functions and the class of functions discussed above are highly nonlinear. In cryptography we often require highly nonlinear and also balanced functions. For this reason, bent functions hardly find direct applications in cryptography.

In contrast, we can always modify a function whose Walsh-Hadamard transform takes the value of 0 or $\pm 2^{\frac{1}{2}}$ to a balanced one, by adding a suitable linear function.

Corollary 16. *Let f be a function on V_n whose Walsh-Hadamard transform takes the value of 0 or $\pm 2^{\frac{1}{2}}$. Then there exists a linear function ψ on V_n such that $f \oplus \psi$ is balanced and its Walsh-Hadamard transform too takes the value of 0 or $\pm 2^{\frac{1}{2}}$.*

Proof. Let ξ be the sequence of f. From Corollary 15, there is a row of H_n, say ℓ, i.e. the sequence of a linear function, say ψ, on V_n, such that $\langle \xi, \ell \rangle = 0$. Note that ψ can be expressed as $\psi(x) = \langle \alpha, x \rangle$, $\alpha \in V_n$. $\langle \xi, \ell \rangle = 0$ can be rewritten as $\sum_{x \in V_n} (-1)^{f(x) \oplus \psi(x)} = 0$, which in turn implies that $f \oplus \psi$ is balanced.

Note that the above technique is not applicable to a bent function f, since $f \oplus \psi$ is also bent for any linear function ψ.

6 Examples of Highly Nonlinear Functions

To complement our theoretical studies carried out in the previous sections, now we show three infinite sets of functions whose Walsh-Hadamard transforms all take the value of 0 or $\pm 2^{\frac{1}{2}}$.

Example 1. Let

$$g(x_1, \ldots, x_5) = (1 \oplus x_1)(1 \oplus x_2)x_3 \oplus (1 \oplus x_1)x_2 x_4 \oplus x_1(1 \oplus x_2)(x_3 \oplus x_4) \oplus x_1 x_2 (x_4 \oplus x_5)$$

and $f(v, u) = g(v) \oplus h(u)$, where $v \in V_5$ and h is a bent function on V_{n-5}. From [17], the set $\Re$ associated with f is composed of five vectors: $(0, \ldots, 0)$, $(0,0,0,1,0,\ldots,0)$, $(0,0,1,0,0,\ldots,0)$, $(0,1,0,1,0,\ldots,0)$, and $(0,1,1,0,0,\ldots,0)$. Let W be the set of the following four vectors: $(0,\ldots,0)$, $(0,0,1,1,0,\ldots,0)$, $(0,1,0,0,0,\ldots,0)$ and $(0,1,1,1,0,\ldots,0)$. It is easy to verify that W is a 2-dimensional subspace and $\Re - \{0\} \subset (0,0,0,1,0,\ldots,0) \oplus W$. Hence $\Re$ is covered by $(0,0,0,1,0,\ldots,0) \oplus W$, and by Corollary 14, the Walsh-Hadamard transform of f takes the value of 0 or $\pm 2^{\frac{1}{2}}$. The reader is directed to [17] where it is suggested that the way g on V_5 is constructed can be extended to V_t for all odd $t > 5$.

Example 2. Consider $f(x) = cx_1 \oplus g(x_2, \ldots, x_n)$ where $x = (x_1, \ldots, x_n)$, $c \in GF(2)$ and g is a bent function on V_{n-1}. From [17], $\Re = \{(0, \ldots, 0),\ (1, 0, \ldots, 0)\}$. Obviously f satisfies the conditions mentioned in Corollary 11. By Corollary 14, the Walsh-Hadamard transform of f takes the value of 0 or $\pm 2^{\frac{1}{2}}$.

Example 3. Let e_i be the ith row of H_k. Hence $e_0, e_1, \ldots, e_{2^k-1}$ are the sequences of all the 2^k linear functions on V_k. Note that the length of each linear sequence e_i is 2^k. Thus one can see that the concatenation of any 2^{k-1} different linear sequences of length 2^k is the sequence of a function on V_{2k-1} whose Walsh-Hadamard transform of f takes the value of 0 or $\pm 2^{\frac{1}{2}}$:

$$e_{j_1}, \ldots, e_{j_{2^{k-1}}} \tag{14}$$

where $\{j_1, \ldots, j_{2^{k-1}}\} \subset \{0, 1 \ldots, 2^k - 1\}$. The explicit polynomial representation of the sequence indicated in (14) can be obtained using a technique shown in [11].

The function in Example 1 is balanced. The functions in the other two examples will be also balanced when extra conditions are satisfied. More specifically, the function in Example 2 will be balanced if $c = 1$, and the function in Example 3 will be so if $\{j_1, \ldots, j_{2^{k-1}}\} \subset \{1 \ldots, 2^k - 1\}$.

7 Conclusion

We have studied functions whose $\Re$ is covered by a coset, and proved two lower bounds on nonlinearity. We have also introduced a class of highly nonlinear functions which have a simple spectrum of Walsh-Hadamard transform and exist only on odd dimensional spaces. Further research includes the investigation of other nonlinear characteristics of this class of functions, including but not limited to algebraic degree, global avalanche characteristics [15], and correlation immunity [12].

Acknowledgment

The first author was supported by a Queen Elizabeth II Fellowship (223 23 1001). Part of the second author's work was completed while on sabbatical at the University of Tokyo. He would like to extend his thanks to Professor Hideki Imai for his hospitality.

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. K. G. Beauchamp. *Applications of Walsh and Related Functions with an Introduction to Sequency Functions.* Microelectronics and Signal Processing. Academic Press, London, New York, Tokyo, 1984.

3. Claude Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, 3:135–145, 1993.
4. G. D. Cohen, M. G. Karpovsky, Jr. H. F. Mattson, and J. R. Schatz. Covering radius — survey and recent results. *IEEE Transactions on Information Theory*, IT-31(3):328–343, 1985.
5. J. F. Dillon. A survey of bent functions. *The NSA Technical Journal*, pages 191–215, 1972. (unclassified).
6. C. Ding, G. Xiao, and W. Shan. *The Stability Theory of Stream Ciphers*, volume 561 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Heidelberg, New York, 1991.
7. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, New York, Oxford, 1978.
8. M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT'93*, volume 765, Lecture Notes in Computer Science, pages 386–397. Springer-Verlag, Berlin, Heidelberg, New York, 1994.
9. B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, volume 437, Lecture Notes in Computer Science, pages 155–165. Springer-Verlag, Berlin, Heidelberg, New York, 1991.
10. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.
11. J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. *Information and Computation*, 119(1):1–13, 1995.
12. T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30 No. 5:776–779, 1984.
13. H. Tanaka and T. Kaneko. A linear attack to the random generator by non linear combiner. In *Proceedings of 1996 IEEE International Symposium on Information Theory and Its Applications*, volume 1, pages 331–334, Victoria, B.C., Canada, September 1996.
14. R. Yarlagadda and J. E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceedings (Part E)*, 136:112–123, 1989.
15. X. M. Zhang and Y. Zheng. GAC — the criterion for global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science*, 1(5):316–333, 1995. (available at `http://hgiicm.tu-graz.ac.at/`).
16. X. M. Zhang and Y. Zheng. Auto-correlations and new bounds on the nonlinearity of boolean functions. In *Advances in Cryptology - EUROCRYPT'96*, volume 1070, Lecture Notes in Computer Science, pages 294–306. Springer-Verlag, Berlin, Heidelberg, New York, 1996.
17. X. M. Zhang and Y. Zheng. Characterizing the structures of cryptographic functions satisfying the propagation criterion for almost all vectors. *Design, Codes and Cryptography*, 7(1/2):111–134, 1996. special issue dedicated to Gus Simmons.

This article was processed using the LaTeX macro package with LLNCS style