KUIS–94–0002

Nonlinearity criteria of Boolean functions

HIROSE Shouichi IKEDA Katsuo

Tel: +81 75 753 5387
Fax: +81 75 751 0482
E-mail: {hirose, ikeda}@kuis.kyoto-u.ac.jp

July 14, 1994

Nonlinearity criteria of Boolean functions

1 Introduction

Cryptographic transformations should be nonlinear to be secure against various attacks. For example, the security of block ciphers, such as DES, which consist of iterative substitutions and permutations, strongly depends on the nonlinearity of the substitutions. Several nonlinearity criteria for Boolean functions have been proposed and investigated.

This paper discusses the properties of nonlinearity criteria and the relationships among them. It focuses on the propagation criterion, the strict avalanche criterion, and the nonlinearity.

Firstly, a necessary and sufficient condition is presented for a Boolean function with n variables to satisfy the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. From this condition, it follows that, for every even $n \geqslant 2$, Boolean functions with n variables that satisfy the PC of degree $n-1$ are perfectly nonlinear, that is, satisfy the PC of degree n. We also show that Boolean functions with n variables that satisfy the PC with respect to all but linearly independent elements are perfectly nonlinear if $n \geqslant 2$ is even and that they satisfy the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ if $\geqslant 3$ is odd.

Secondly, we discuss the construction of Boolean functions with n variables that satisfy the PC with respect to all but one or three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$.

Seberry, Zhang and Zheng[SZZ93] presented methods for the construction of balanced Boolean functions satisfying the PC of high degrees. For odd $n \geqslant 3$, they proposed a method for constructing balanced Boolean functions with n variables satisfying the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ and constructed balanced Boolean functions satisfying the PC of degree $n-1$. For even $n \geqslant 4$, they proposed a method for constructing balanced Boolean functions with n variables satisfying the PC with respect to all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ and constructed balanced Boolean functions satisfying the PC of degree about $2n/3$. This result is optimal in the sense that, for even $n \geqslant 4$, Boolean functions with n variables satisfying the PC with respect to all but less than three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ are perfectly nonlinear and that perfectly nonlinear Boolean functions are not balanced.

This report shows that, for every odd $n \geqslant 3$, Boolean functions with n variables that satisfy the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ are constructed from all perfectly nonlinear Boolean functions with $n-1$ variables. It also presents, for every even $n \geqslant 2$ a necessary and sufficient condition for Boolean functions to satisfy the PC with respect all but three linearly dependent elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. It shows that, for every even $n \geqslant 4$, Boolean functions with n variables that satisfy the PC with respect to all but three linearly dependent elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ are constructed from all perfectly nonlinear Boolean functions with $n-2$ variables.

Thirdly, this report discusses Boolean functions with n variables satisfying the PC of degree $n-2$. It shows that, for every even $n \geqslant 4$, Boolean functions with n variables satisfying the PC of degree $n-2$ are perfectly nonlinear, and that, for every odd $n \geqslant 3$, they satisfy the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$.

Lastly, some relationships between the PC and the SAC are presented.

It is apparent from the definition that the set of Boolean functions that satisfy the PC of degree 1 coincides with that of Boolean functions that satisfy the SAC of order 0. It has been shown that the Boolean functions that satisfy the SAC of order $n-2$ are perfectly nonlinear[AT90].

This report shows, for every odd $n \geqslant 3$, that the Boolean functions with n variables that satisfy the PC of degree $n-1$ satisfy the SAC of order 1, while those satisfying the PC of degree $n-2$ necessarily not and that there exist Boolean functions with n variables satisfying the SAC of order 2 and not satisfying the PC of degree $n-2$ For every even $n \geqslant 2$, it shows that perfectly nonlinear Boolean functions with n variables do not necessarily satisfy the SAC of order 1. It also shows that Boolean functions with n variables that satisfy the SAC of order $n-3$ do not necessarily satisfy the PC of degree 2 for every $n \geqslant 3$.

Section 2 contains the definitions of nonlinearity criteria. Section 3 is devoted to the discussion of Boolean functions with n variables satisfying the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$, and those satisfying the PC with respect to all but linearly independent elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. Section 4 discusses the construction of Boolean functions satisfying the PC with respect to all but one or all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. Section 5 discusses the Boolean functions with n variables satisfying the PC of degree $n-2$. Section 6 shows the relationships between the PC and the SAC.

2 Preliminaries

2.1 Walsh Transform and Boolean Functions

Let $\mathbf{R}$ denote the set of reals.

Definition 1 The *Walsh transform* of a real-valued function $f : \{0,1\}^n \to \mathbf{R}$ is

$$(\mathcal{W}(f))(\omega) = \sum_{x \in \{0,1\}^n} f(x)(-1)^{\omega \cdot x},$$

where $x = (x_1, \ldots, x_n)$, $\omega = (\omega_1, \ldots, \omega_n) \in \{0,1\}^n$ and $\omega \cdot x$ denotes the dot product $\omega_1 x_1 \oplus \cdots \oplus \omega_n x_n$. □

For simplicity, $(\mathcal{W}(f))(\omega)$ is often denoted by $F(\omega)$. The *inverse Walsh transform* is

$$f(x) = (\mathcal{W}^{-1}(F))(x) = \frac{1}{2^n} \sum_{\omega \in \{0,1\}^n} F(\omega)(-1)^{\omega \cdot x}.$$

The Walsh transform can be represented as a matrix form[Rue91]. For $f : \{0,1\}^n \to \mathbf{R}$, let $f(i)$ denote $f(x_1, \ldots, x_n)$ when $x_1 + x_2 2 + \cdots + x_n 2^{n-1} = i$. Let $[f] = [f(0), f(1), \ldots, f(2^n-1)]$ and $[F] = [F(0), F(1), \ldots, F(2^n-1)]$. The Walsh transform is represented as

$$[F] = [f] H_n,$$

where H_n denotes the Hadamard matrix of order n. H_n is defined recursively by

$$\begin{aligned} H_0 &= [1], \\ H_n &= \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}. \end{aligned}$$

H_n is a $2^n \times 2^n$ symmetric non-singular matrix, and its inverse is $2^{-n} H_n$. The inverse Walsh transform is represented as

$$[f] = 2^{-n} [F] H_n.$$

A *Boolean function* is a function of the form $f : \{0,1\}^n \to \{0,1\}^m$. $f : \{0,1\}^n \to \{0,1\}^m$ is called Boolea function with n inputs and m outputs. Let $\mathrm{B}_{n,m} = \{f \mid f : \{0,1\}^n \to \{0,1\}^m\}$. For simplicity, we denote $\mathrm{B}_{n,1}$ as B_n and call an Boolean function with n inputs and 1 output Boolean function with n inputs. Boolean functions with n inputs are also called Boolean functions with n variables.

A form of representation is defined for Boolean functions with n variables.

Definition 2 The *algebraic normal form* of a Boolean function $f \in \mathrm{B}_n$ is a type of representation of f such that

$$\bigoplus_{\{i_1,\ldots,i_k\} \in \wp(\mathrm{N})} a_{\{i_1,\ldots,i_k\}} x_{i_1} \cdots x_{i_k},$$

where $\wp(\mathrm{N})$ is the power set of $\mathrm{N} = \{1, \ldots, n\}$, and $a_{\{i_1,\ldots,i_k\}} \in \{0,1\}$ for every $\{i_1, \ldots, i_k\} \in \wp(\mathrm{N})$. □

Every Boolean function can be uniquely represented as an algebraic normal form, and any two different Boolean functions cannot be represented as a same algebraic normal form.

The Walsh transform can be applied to Boolean functions in B_n when they are considered to be real-valued functions. For the analysis of Boolean functions, it is often convenient to work with $\hat{f} : \{0,1\}^n \to \{-1,1\}$, where $\hat{f}(x) \triangleq (-1)^{f(x)}$. The Walsh transform of $\hat{f}$ is

$$\hat{F}(\omega) = \sum_{x\in\{0,1\}^n} \hat{f}(x)(-1)^{\omega\cdot x} = \sum_{x\in\{0,1\}^n} (-1)^{f(x)\oplus\omega\cdot x}.$$

Definition 3 The *autocorrelation function* of a Boolean function $f : \{0,1\}^n \to \{0,1\}$ is $C_f : \{0,1\}^n \to \mathbf{N}$ such that

$$C_f(z) = \sum_{x\in\{0,1\}^n} \hat{f}(x)\hat{f}(x\oplus z),$$

where $\mathbf{N}$ is the set of integers and $x \oplus z$ denotes $(x_1 \oplus z_1, \ldots, x_n \oplus z_n)$. □

Proposition 1 shows a relationship between the autocorrelation function of f and the Walsh transform of $\hat{f}$. It states that the inverse Walsh transform of $\hat{F}^2$ is C_f.

Proposition 1 For any Boolean function f, $C_f = \mathcal{W}^{-1}(\hat{F}^2)$. □

Proposition 2 shows that the sum of $\hat{F}^2(\omega)$'s is constant for every Boolean function with n variables f.

Proposition 2 For any $f \in \mathrm{B}_n$, $\sum_{\omega\in\{0,1\}^n} \hat{F}^2(\omega) = 2^{2n}$. □

2.2 Nonlinearity Criteria for Boolean Functions

For a set S, let |S| denote the number of elements in S.

Definition 4 A Boolean function $f \in \mathrm{B}_n$ is *balanced* if and only if $|\{x|f(x) = 0\}| = |\{x|f(x) = 1\}| = 2^{n-1}$. □

An *affine* Boolean function $h \in \mathrm{B}_n$ is a Boolean function of the form of

$$h(x_1, \ldots, x_n) = \alpha_0 \oplus \alpha_1 x_1 \oplus \cdots \oplus \alpha_n x_n,$$

where $\alpha_i \in \{0,1\}$ for $0 \leqslant i \leqslant n$. The set of affine Boolean functions with n inputs is denoted as A_n. The number of affine Boolean functions with n inputs is 2^{n+1}.

The *distance* between two Boolean functions, f and g, with the same number of variables, is $d(f,g) = |\{x \mid f(x) \neq g(x)\}|$.

The nonlinearity of $f \in \mathrm{B}_n$ is the minimum distance between f and $h \in \mathrm{A}_n$.

Definition 5 The *nonlinearity* of $f \in \mathrm{B}_n$ is $\min\limits_{h\in\mathrm{A}_n} d(f,h)$. □

The nonlinearity of $f \in \mathrm{B}_n$ can be represented with $\hat{F}$.

Proposition 3 The nonlinearity of $f \in \mathrm{B}_n$ is

$$2^{n-1} - \frac{1}{2} \max_{\omega\in\{0,1\}^n} \left|\hat{F}(\omega)\right|.$$

□

Webster and Tavares [WT86] defined the strict avalanche criterion for the design criterion of substitution boxes of DES. For any $a \in \{0,1\}^n$, let $W(a)$ denote the Hamming weight of a, that is, the number of 1's in a.

Definition 6 A Boolean function $f \in \mathrm{B}_n$ is said to satisfy the *strict avalanche criterion(SAC)* if and only if $f(x) \oplus f(x \oplus a)$ is balanced for any $a \in \{0,1\}^n$ such that $W(a) = 1$. □

For a Boolean function satisfying the SAC, any 1-bit change of inputs causes the change of the output with probability 1/2.

Let $f(x_1, \ldots, x_n) \in \mathrm{B}_n$. For any $i_1, \ldots, i_m$ such that $1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n$ and $b_1, \ldots, b_m \in \{0,1\}$, let $f\mid_{x_{i_1}=b_1,\ldots,x_{i_m}=b_m} \in \mathrm{B}_{n-m}$ denote the subfunction of f obtained by substituting $b_1, \ldots, b_m$ for $x_{i_1}, \ldots, x_{i_m}$, respectively.

Forré [For90] extended the notion and defined the SAC of higher orders. The original definition by Forré was simplified by Lloyd.

Definition 7 [Llo91] A Boolean function $f \in \mathrm{B}_n$ is said to satisfy the *strict avalanche criterion of order m* if and only if, for any $i_1, \ldots, i_m$ such that $1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n$ and $b_1, \ldots, b_m \in \{0,1\}$, $f\mid_{x_{i_1}=b_1,\ldots,x_{i_m}=b_m} \in \mathrm{B}_{n-m}$ satisfies the SAC. □

It is obvious from the definition that the original SAC of Definition 6 is equivalent to the SAC of order 0. The value of a function satisfying the SAC depends on all of its variables. Lloyd[Llo91] proved that the functions satisfying the SAC of order m also satisfy the SAC of order $k(< m)$.

Let $\mathrm{SAC}_n(m)$ denote the set of $f \in \mathrm{B}_n$ satisfying the SAC of order m. It is apparent from Definition 6 that every $f \in \mathrm{B}_0 \cup \mathrm{B}_1$ does not satisfy the SAC. $\mathrm{SAC}_n(n-1) = \mathrm{SAC}_n(n) = \phi$ for every n.

Definition 8 [MS90] A Boolean function $f \in \mathrm{B}_n$ is *perfectly nonlinear* if and only if $f(x) \oplus f(x \oplus a)$ is balanced for any $a \in \{0,1\}^n$ such that $1 \leqslant W(a) \leqslant n$. □

For a perfectly nonlinear Boolean function, any change of inputs causes the change of the output with probability 1/2.

The following proposition directly follows from the definition of the autocorrelation function and the perfect nonlinearity.

Proposition 4 Let $f \in \mathrm{B}_n$. f is perfectly nonlinear if and only if $C_f(z) = 0$ for every $z \in \{0,1\}^n - \{(0, \ldots, 0)\}$. □

Meier and Staffelbach[MS90] proved that the set of perfectly nonlinear Boolean functions coincides with the set of Boolean *bent* functions defined by Rothaus[Rot76].

Definition 9 $f \in \mathrm{B}_n$ is defined to be a Boolean bent function if and only if $\left|\hat{F}(\omega)\right| = 2^{n/2}$ for every $\omega \in \{0,1\}^n$. □

Proposition 5 $f \in \mathrm{B}_n$ is perfectly nonlinear if and only if $\left|\hat{F}(\omega)\right| = 2^{n/2}$ for every $\omega \in \{0,1\}^n$. □

Preneel, et al.[PLLGV91] extended the notion of the perfect nonlinearity and defined the propagation criterion.

Definition 10 A Boolean function $f \in \mathrm{B}_n$ is said to satisfy the *propagation criterion(PC) of degree k* if and only if $f(x) \oplus f(x \oplus a)$ is balanced for any $a \in \{0,1\}^n$ such that $1 \leqslant W(a) \leqslant k$. □

Let $\mathrm{PC}_n(k)$ denote the set of Boolean functions with n variables satisfying the propagation criterion of degree k. $\mathrm{PC}_n(n)$ is the set of perfectly nonlinear Boolean functions with n variables.

Definition 11 A Boolean function $f \in \mathrm{B}_n$ is said to satisfy the *propagation criterion(PC) with respect to* $\mathrm{A} \subseteq \mathrm{V}_n$ if and only if $f(x) \oplus f(x \oplus a)$ is balanced for every $a \in \mathrm{A}$. □

Proposition 6 Let $f \in \mathrm{B}_n$ and $\mathrm{A} \subseteq \mathrm{V}_n$. f satisfies the PC with respect to A if and only if $C_f(z) = 0$ for every $z \in \mathrm{V}_n - \mathrm{A}$. □

3 Propagation criteria of Boolean functions

3.1 A necessary and sufficient condition for the propagation criterion of degree $n-1$

In this section, we investigate Boolean functions that satisfy the PC of degree $n-1$.

We begin by presenting a bit general theorem that gives a necessary and sufficient condition for $f \in \mathrm{B}_n$ to satisfy the PC with respect to all but one elements in V_n. Before presenting the theorem, we prove two simple lemmas.

For $a = (a_1, \ldots, a_n) \in \{0,1\}^n$, let $dec(a) = a_1 + 2a_2 + \cdots + 2^{n-1}a_n$.

Lemma 1 Let $m \geqslant 0$ be an integer. The integers $x, y \geqslant 0$ satisfying the equation

$$x^2 + y^2 = 2^m$$

is,

- for even m, $x = 2^{m/2}$ and $y = 0$, or $x = 0$ and $y = 2^{m/2}$,
- for odd m, $x = y = 2^{(m-1)/2}$.

(Proof) If one of x and y is 0, then m is even and the other is $2^{m/2}$.

If we assume that $x \neq 0$ and $y \neq 0$, then, we can represent x and y as

$$x = 2^{e_x} q_x,\ y = 2^{e_y} q_y,$$

respectively, where $e_x \geqslant 0$, $e_y \geqslant 0$, and $q_x \geqslant 1$, $q_y \geqslant 1$ are odd. Without loss of generality, it can be assumed that $e_y \geqslant e_x \geqslant 0$. Thus,

$$\begin{aligned} 2^{2e_x}{q_x}^2 + 2^{2e_y}{q_y}^2 &= 2^m \\ {q_x}^2 + 2^{2(e_y - e_x)}{q_y}^2 &= 2^{m-2e_x}. \end{aligned}$$

Since ${q_x}^2 + 2^{2(e_y-e_x)}{q_y}^2 \geqslant 2$, $m - 2e_x \geqslant 1$, which implies that ${q_x}^2 + 2^{2(e_y-e_x)}{q_y}^2$ is even. Thus, $e_y - e_x = 0$ since q_x and q_y are odd. For

$${q_x}^2 + {q_y}^2 = 2^{m-2e_x},$$

since ${q_x}^2 + {q_y}^2$ is a multiple of 2 but not of 4, $m - 2e_x = 1$. Hence, $e_x = e_y = (m-1)/2$ and $q_x = q_y = 1$. This implies m is odd and $x = y = 2^{(m-1)/2}$.

The lemma has been proved. □

Let V_n denote $\{0,1\}^n - \{(0,\ldots,0)\}$.

Lemma 2 For every $f \in \mathrm{B}_n$,

$$\left[\hat{F}^2(0), \ldots, \hat{F}^2(2^n - 1)\right] = \left[C_f(0), \ldots, C_f(2^n - 1)\right] H_n$$

(Proof) This lemma directly follows from Proposition 1. □

The following theorem presents a necessary and sufficient condition for a Boolean function to satisfy the PC with respect to all but one nonzero vectors.

For every $b = (b_1, \ldots, b_n) \in \{0,1\}^n$, let v_b denote the $dec(b)+1$-th column vector of H_n, and let $l_b(x_1, \ldots, x_n) = b_1 x_1 \oplus \cdots \oplus b_n x_n$.

Theorem 1 Let $b \in \mathrm{V}_n$. $f \in \mathrm{B}_n$ satisfies the PC with respect to $\mathrm{V}_n - \{b\}$ if and only if,

- for even $n \geqslant 2$, $\left|\hat{F}(\omega)\right| = 2^{n/2}$ for every $\omega \in \{0,1\}^n$,

- for odd $n \geqslant 3$,

$$\left|\hat{F}(\omega)\right| = \begin{cases} 2^{(n+1)/2} & \text{if } b \cdot \omega = 0 \\ 0 & \text{if } b \cdot \omega = 1, \end{cases}$$

or

$$\left|\hat{F}(\omega)\right| = \begin{cases} 2^{(n+1)/2} & \text{if } b \cdot \omega = 1 \\ 0 & \text{if } b \cdot \omega = 0. \end{cases}$$

(Proof) $f \in \mathrm{B}_n$ satisfies the PC with respect to $\mathrm{V}_n - \{b\}$ if and only if $C_f(a) = 0$ for every $a \in \mathrm{V}_n - \{b\}$. Thus, from Lemma 2, $\left[\hat{F}^2\right]$ can be represented as

$$\left[\hat{F}^2\right] = C_f(0)v_{\mathbf{0}} + C_f(b)v_b.$$

Let

$$u_0 = ({v_{\mathbf{0}}}^{\mathrm{T}} + {v_b}^{\mathrm{T}})/2,$$

$$u_1 = ({v_{\mathbf{0}}}^{\mathrm{T}} - {v_b}^{\mathrm{T}})/2,$$

where ${v_0}^{\mathrm{T}}$ and ${v_{dec(b)}}^{\mathrm{T}}$ are the transposes of v_0 and $v_{dec(b)}$, respectively. Then, $\left[\hat{F}^2\right]$ is able to be represented as

$$\left[\hat{F}^2\right] = c_0u_0 + c_1u_1,$$

where $c_0 = C_f(0) + C_f(b)$ and $c_1 = C_f(0) - C_f(b)$. Since

$$\begin{aligned} u_0 &= [1 \oplus l_b(0), \ldots, 1 \oplus l_b(2^n - 1)], \\ u_1 &= [l_b(0), \ldots, l_b(2^n - 1)], \end{aligned}$$

$$\hat{F}^2(\omega) = \begin{cases} c_0 & \text{if } b \cdot \omega = 0, \\ c_1 & \text{if } b \cdot \omega = 1. \end{cases}$$

Let $\left|\hat{F}(\omega)\right| = \hat{F}_0$ for every ω such that $b \cdot \omega = 0$, and $\left|\hat{F}(\omega)\right| = \hat{F}_1$ for every ω such that $b \cdot \omega = 1$. Since $\sum_{\omega \in \{0,1\}^n} \hat{F}^2(\omega) = 2^{2n}$,

$$\hat{F}_0^2 + \hat{F}_1^2 = 2^{n+1}.$$

Hence, from Lemma 1,

- When n is even, $\hat{F}_0 = \hat{F}_1 = 2^{n/2}$.
- When n is odd, $\hat{F}_0 = 0$, $\hat{F}_1 = 2^{(n+1)/2}$, or $\hat{F}_0 = 2^{(n+1)/2}$, $\hat{F}_1 = 0$.

The theorem has been proved. □

Boolean functions in B_n satisfying the PC with respect to $\mathrm{V}_n - \{(1, \ldots, 1)\}$ are the ones satisfying the PC of degree $n - 1$. Thus, the following two corollaries are immediately derived from Theorem 1.

Corollary 1 For even $n \geqslant 2$, $\mathrm{PC}_n(n-1) = \mathrm{PC}_n(n)$. □

Corollary 2 For odd $n \geqslant 3$, $f \in \mathrm{PC}_n(n-1)$ if and only if,

$$\left|\hat{F}(\omega)\right| = \begin{cases} 2^{(n+1)/2} & \text{if } W(\omega) \text{ is even} \\ 0 & \text{if } W(\omega) \text{ is odd,} \end{cases}$$

or

$$\left|\hat{F}(\omega)\right| = \begin{cases} 2^{(n+1)/2} & \text{if } W(\omega) \text{ is odd} \\ 0 & \text{if } W(\omega) \text{ is even.} \end{cases}$$

□

Corollary 3 Let $n \geqslant 3$ be odd and $b \in \mathrm{V}_n$. If $f \in \mathrm{B}_n$ satisfies the PC with respect to $\mathrm{V}_n - \{b\}$, then

$$f(x) \oplus f(x \oplus b) \equiv 0 \text{ or } 1.$$

(Proof) For odd $n \geqslant 3$, if $f \in \mathrm{B}_n$ satisfies the PC with respect to $\mathrm{V}_n - \{b\}$, then, from the proof of Theorem 1,

$$\begin{aligned} C_f(0) + C_f(b) &= 2^{n+1} \\ C_f(0) - C_f(b) &= 0, \end{aligned}$$

or

$$\begin{aligned} C_f(0) + C_f(b) &= 0 \\ C_f(0) - C_f(b) &= 2^{n+1}. \end{aligned}$$

For the former case, $C_f(b) = 2^n$, and for the latter case $C_f(b) = -2^n$. $C_f(b) = 2^n$ and $C_f(b) = -2^n$ implies that $f(x) \oplus f(x \oplus b) \equiv 0$ and $f(x) \oplus f(x \oplus b) \equiv 1$, respectively. □

From Theorem 1 and Proposition 3, the following corollary can be derived immediately.

Corollary 4 Let $n \geqslant 3$ be odd. If $f \in \mathrm{B}_n$ satisfies the PC with respect to all but one elements in V_n, then the nonlinearities of f is $2^{n-1} - 2^{(n-1)/2}$. □

The above corollary states that, for every odd $n \geqslant 3$, the nonlinearities of $f \in \mathrm{B}_n$ which satisfies the PC with respect to all but one elements in V_n are high and uniquely determined.

The particular case of Corollary 4 is as follows.

Corollary 5 Let $n \geqslant 3$ be odd. If $f \in \mathrm{PC}_n(n-1)$, then the nonlinearities of f is $2^{n-1} - 2^{(n-1)/2}$. □

3.2 A necessary and sufficient condition for the propagation criterion with respect to all or all but one nonzero elements

This section is devoted to a necessary and sufficient condition for Boolean functions in B_n to satisfy the PC with respect to all nonzero vectors for even n and with respect to all but one nonzero vectors for odd n.

Lemma 3 Let k be any integer such that $1 \leqslant k \leqslant n$ and $b_1, \ldots, b_k \in \{0,1\}^n$ be linearly independent. let $r_1, \ldots, r_k \in \{0,1\}$. The number of elements in $\{0,1\}^n$ satisfying the following equations are 2^{n-k}.

$$\begin{cases} l_{b_1}(x_1, \ldots, x_n) &= r_1 \\ \qquad\vdots & \\ l_{b_k}(x_1, \ldots, x_n) &= r_k \end{cases}$$

□

Theorem 2 Let n and k be any integers such that $n \geqslant 2$ and $1 \leqslant k \leqslant n$. Let $b_1, \ldots, b_k \in \{0,1\}^n$ be linearly independent. If $f \in \mathrm{B}_n$ satisfies the PC with respect to $\mathrm{V}_n - \{b_1, \ldots, b_k\}$, then,

1. when n is even, $f \in \mathrm{PC}_n(n)$,
2. when n is odd, for some i such that $1 \leqslant i \leqslant k$, f satisfies the PC with respect to $\mathrm{V}_n - \{b_i\}$.

(Proof) Since $C_f(z) = \sum_{x\in\{0,1\}^n} \hat{f}(x)\hat{f}(x \oplus z)$, $f \in \mathrm{B}_n$ satisfies the PC with respect to $\mathrm{V}_n - \{b_1, \ldots, b_k\}$ if and only if $C_f(a) = 0$ for every $a \in \mathrm{V}_n - \{b_1, \ldots, b_k\}$. Thus from Lemma 2, $\left[\hat{F}^2\right]$ can be represented as

$$\left[\hat{F}^2\right] = C_f(0){v_0}^{\mathrm{T}} + C_f(b_1){v_{b_1}}^{\mathrm{T}} + \cdots + C_f(b_k){v_{b_k}}^{\mathrm{T}},$$

Let

$$\begin{aligned} u_0 &= {v_0}^{\mathrm{T}}, \\ u_i &= ({v_0}^{\mathrm{T}} + {v_{b_i}}^{\mathrm{T}})/2 \text{ for } 1 \leqslant i \leqslant k, \end{aligned}$$

then we can rewrite $\left[\hat{F}^2\right]$ as

$$\left[\hat{F}^2\right] = c_0u_0 + c_1u_1 + \cdots + c_ku_k,$$

where

$$\begin{aligned} c_0 &= C_f(0) - \sum_{i=1}^{k} C_f(b_i) \\ c_i &= 2C_f(b_i). \end{aligned}$$

Since

$$\begin{aligned} u_0 &= [1, \ldots, 1], \\ u_i &= [1 \oplus l_{b_k}(0), \ldots, 1 \oplus l_{b_k}(2^n - 1)] \text{ for } 1 \leqslant i \leqslant k, \end{aligned}$$

and l_{b_i} is balanced for every $b_i \in \mathrm{V}_n$,

$$\sum_{\omega\in\{0,1\}^n} \hat{F}^2(\omega) = 2^n c_0 + 2^{n-1}(c_1 + \cdots + c_k) = 2^{2n}.$$

Thus,

$$2c_0 + c_1 + \cdots + c_k = 2^{n+1}.$$

From Lemma 3, there exist some $\omega \in \{0, 1\}^n$ such that

$$\hat{F}^2(\omega) = c_0.$$

There also exist some $\omega \in \{0, 1\}^n$ such that, for any j such that $1 \leqslant j \leqslant k$ and $i_1, \ldots, i_j$ such that $1 \leqslant i_1 < \cdots < i_j \leqslant k$,

$$\hat{F}^2(\omega) = c_0 + c_{i_1} + \cdots + c_{i_j}.$$

For the case where n is even. Since $2c_0 + c_1 + \cdots + c_k = 2^{n+1}$,

$$\begin{aligned} c_0 + (c_0 + c_1 + \ldots + c_k) &= 2^{n+1} \\ (c_0 + c_1) + (c_0 + c_2 + \ldots + c_k) &= 2^{n+1} \\ &\cdots \\ (c_0 + c_k) + (c_0 + c_1 + \ldots + c_{k-1}) &= 2^{n+1}, \end{aligned}$$

from Lemma 1,

$$c_0 = c_0 + c_1 = \cdots = c_0 + c_k = 2^n,$$

Thus,

$$c_0 = 2^n, c_1 = \cdots = c_k = 0.$$

Hence, for every $\omega \in \{0,1\}^n$,

$$|\hat{F}(\omega)| = 2^{n/2}.$$

For the case where n is odd. From Lemma 1,

$$c_0 = 0 \text{ or } 2^{n+1},$$

and, for any j such that $1 \leqslant j \leqslant k$ and $i_1, \ldots, i_j$ such that $1 \leqslant i_1 < \cdots < i_j \leqslant k$,

$$c_0 + c_{i_1} + \cdots + c_{i_j} = 0 \text{ or } 2^{n+1}.$$

(i) If we assume $c_0 = 0$, then

$$c_0 + c_1 + \cdots + c_k = 2^{n+1}.$$

Since $c_0 + c_i = 0$ or 2^{n+1} for every i such that $1 \leqslant i \leqslant k$,

$$c_i = 0 \text{ or } 2^{n+1}.$$

Thus, only any one of $c_1, \ldots, c_k$ is 2^{n+1} and the others are all 0. Hence, for some b_i,

$$|\hat{F}(\omega)| = \begin{cases} 2^{(n+1)/2} & \text{if } b_i \cdot \omega = 0 \\ 0 & \text{if } b_i \cdot \omega = 1. \end{cases}$$

(ii) If we assume $c_0 = 2^{n+1}$, then

$$c_0 + c_1 + \cdots + c_k = 0.$$

Since $c_0 + c_i = 0$ or 2^{n+1} for every i such that $1 \leqslant i \leqslant k$,

$$c_i = 0 \text{ or } -2^{n+1}.$$

Thus, only any one of $c_1, \ldots, c_k$ is -2^{n+1} and the others are all 0. Hence, for some b_i,

$$|\hat{F}(\omega)| = \begin{cases} 2^{(n+1)/2} & \text{if } b_i \cdot \omega = 1 \\ 0 & \text{if } b_i \cdot \omega = 0. \end{cases}$$

Hence, the theorem has been proved. □

4 Boolean functions satisfying the PC with respect to all but one or three nonzero elements

This section gives an exact characterization of Boolean functions with the odd number of inputs that satisfy the PC with respect to all but one nonzero vectors. The motivation of this research is a method in [SZZ93] to construct balanced Boolean functions with the odd number of inputs that satisfy the PC with respect to all but one nonzero vectors and that to construct balanced Boolean functions with the even number of inputs that satisfy the PC with respect to all but three nonzero vectors.

4.1 Boolean functions with the odd number of variables

This section presents, for odd $n \geqslant 3$, a spectral property of Boolean functions in B_n that satisfy the PC with respect to all but one elements in V_n. This is an exact characterizartion of such Boolean functions.

Seberry, et al.[SZZ93] presented a simple method that, for any odd $n \geqslant 3$, generates balanced Boolean functions in B_n satisfying the PC with respect to all but one elements in V_n from Boolean functions in $\mathrm{PC}_{n-1}(n-1)$.

In this section, it is shown that, for every odd $n \geqslant 3$, one can construct all Boolean functions that satisfy the PC with respect to all but one elements in V_n from all Boolean functions in $\mathrm{PC}_{n-1}(n-1)$. It also gives a construction method that is slightly different from the method of Seberry, et al. and that reflects spectral properties. Some results are presented for the number of Boolean functions satisfying the PC with respect to all but one nonzero vectors.

A lemma is firstly proved which is a basis of the following discussion. It states that, for any $a \in \mathrm{V}_n$, for each column v of the matrix constructed from i-th rows of H_n such that the dot product of a and the binary representation of i is equal to 0 or 1, there exists a column in H_{n-1} that is equal to v or $-v$.

We define some notations. For a matrix M, let $col(M,i)$ be the i-th column of M. For $a = (a_1, \ldots, a_n)$ and $1 \leqslant i \leqslant n$, let $\langle a \rangle_i$ denotes $(a_1, \ldots, a_i)$.

Lemma 4 For every $a \in \mathrm{V}_n$, let $K_n(a,0)$ and $K_n(a,1)$ be $2^{n-1} \times 2^n$ matrices that are constructed by removing all $(dec(\omega)+1)$-th rows of H_n, where $a \cdot \omega = 1$ and $a \cdot \omega = 0$, respectively. Then,

- for each column v of H_{n-1}, $K_n(a,0)$ has two columns that is equal to v, and $K_n(a,1)$ has v and $-v$,
- for every i such that $1 \leqslant i \leqslant 2^n$,

$$\begin{aligned} col(K_n(a,0),i) &= col(K_n(a,1),i) \text{ or} \\ col(K_n(a,0),i) &= -col(K_n(a,1),i). \end{aligned}$$

(Proof) We prove the theorem by induction. When $n = 1$, since $H_0 = [1]$ and

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$K_1(1,0) = [1,1]$ and $K_1(1,1) = [1,-1]$. The theorem is proved for $n = 1$.

For $n \geqslant 2$, we consider the following two cases: One is the case where $a_n = 0$ and the other is the one where $a_n = 1$.

<u>*For the Case where $a_n = 0$.*</u> Since

$$a \cdot (\omega_1, \ldots, \omega_{n-1}, 0) = a \cdot (\omega_1, \ldots, \omega_{n-1}, 1),$$

and

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$$

for $c = 0, 1$,

$$K_n(a,c) = \begin{bmatrix} K_{n-1}(\langle a \rangle_{n-1}, c) & K_{n-1}(\langle a \rangle_{n-1}, c) \\ K_{n-1}(\langle a \rangle_{n-1}, c) & -K_{n-1}(\langle a \rangle_{n-1}, c) \end{bmatrix}.$$

When $c = 0$, from the inductive assumption, for every column of H_{n-2}, $K_{n-1}(\langle a \rangle_{n-1}, 0)$ has exactly two columns which are equal to it. Thus, by permuting the columns of $K_n(a,0)$,

$$\begin{bmatrix} H_{n-2} & H_{n-2} & H_{n-2} & H_{n-2} \\ H_{n-2} & H_{n-2} & -H_{n-2} & -H_{n-2} \end{bmatrix}.$$

is obtained. This implies that, for each column of H_{n-1}, $K_n(a,0)$ has exactly two columns which are equal to it.

When $c=1$, for every column v' of H_{n-2}, $K_{n-1}(\langle a\rangle_{n-1},0)$ has v' and $-v'$. Thus, for each column v of H_{n-1}, $K_n(a,0)$ has v and $-v$.

It is also easily derived from the inductive assumption that, for every i such that $1 \leqslant i \leqslant 2^n$,

$$\begin{aligned} col(K_n(a,0),i) &= col(K_n(a,1),i) \text{ or} \\ col(K_n(a,0),i) &= -col(K_n(a,1),i). \end{aligned}$$

For the Case where $a_n = 1$. If $a = (0,\ldots,0,1)$, then

$$\begin{aligned} K_n(a,0) &= \begin{bmatrix} H_{n-1} & H_{n-1} \end{bmatrix}, \\ K_n(a,1) &= \begin{bmatrix} H_{n-1} & -H_{n-1} \end{bmatrix}. \end{aligned}$$

It is apparent that the theorem holds for this case.

If $a \neq (0,\ldots,0,1)$, since

$$a \cdot (\omega_1,\ldots,\omega_{n-1},0) = a \cdot (\omega_1,\ldots,\omega_{n-1},1) \oplus 1,$$

$$K_n(a,c) = \begin{bmatrix} K_{n-1}(\langle a\rangle_{n-1},c) & K_{n-1}(\langle a\rangle_{n-1},c) \\ K_{n-1}(\langle a\rangle_{n-1},1\oplus c) & -K_{n-1}(\langle a\rangle_{n-1},1\oplus c) \end{bmatrix}$$

for $c = 0,1$. Since, for every j such that $1 \leqslant j \leqslant 2^{n-1}$,

$$\begin{aligned} col(K_{n-1}(a,0),j) &= col(K_{n-1}(a,1),j) \text{ or} \\ col(K_{n-1}(a,0),j) &= -col(K_{n-1}(a,1),j), \end{aligned}$$

for every a, there exists some $2^n \times 2^n$ nondegenerate matrix Π such that

$$K_n(a,c)\,\Pi = \begin{bmatrix} K_{n-1}(\langle a\rangle_{n-1},c) & K_{n-1}(\langle a\rangle_{n-1},c) \\ K_{n-1}(\langle a\rangle_{n-1},c) & -K_{n-1}(\langle a\rangle_{n-1},c) \end{bmatrix}.$$

Π is a matrix that exchanges l-th and $(l+2^{n-1})$-th columns of $K_n(a,c)$ for every l such that $1 \leqslant l \leqslant 2^{n-1}$ and

$$col(K_{n-1}(a,1\oplus c),l) = -col(K_{n-1}(a,c),l).$$

This is the same case as the one where $a_n = 0$. Hence, the theorem has been proved. □

An example of Lemma 4 is given.

Example 1 Let $n=4$ and $a=(0,1,0,1)$. Let $H_4 = [v_1^4,\ldots,v_{16}^4]$ and $H_3 = [v_1,\ldots,v_8]$. Then,

$$\begin{aligned} K_4(a,0) &= \begin{bmatrix} v_1^4 & v_3^4 & v_6^4 & v_8^4 & v_{10}^4 & v_{12}^4 & v_{13}^4 & v_{15}^4 \end{bmatrix}^{\mathrm{T}} \\ &= \begin{bmatrix} v_1 & v_2 & v_5 & v_6 & v_3 & v_4 & v_7 & v_8 \\ v_5 & v_6 & v_1 & v_2 & v_7 & v_8 & v_3 & v_4 \end{bmatrix}, \\ K_4(a,1) &= \begin{bmatrix} v_2^4 & v_4^4 & v_5^4 & v_7^4 & v_9^4 & v_{11}^4 & v_{14}^4 & v_{16}^4 \end{bmatrix}^{\mathrm{T}} \\ &= \begin{bmatrix} v_1 & v_2 & -v_5 & -v_6 & v_3 & v_4 & -v_7 & -v_8 \\ v_5 & v_6 & -v_1 & -v_2 & v_7 & v_8 & -v_3 & -v_4 \end{bmatrix}. \end{aligned}$$

For each column v_i of H_3, $K_4(a,0)$ has two columns that are equal to v_i, and $K_4(a,1)$ has a column that is equal to v_i and a column that is equal to $-v_i$.

$$col(K_4(a,0),i) = \begin{cases} col(K_4(a,1),i) & \text{for } i = 1,2,5,6,9,10,13,14, \\ -col(K_4(a,1),i) & \text{for } i = 3,4,7,8,11,12,15,16. \end{cases}$$

□

The following theorem implies an injective mapping from the set of Boolean functions in B_n that satisfy the PC with respect to all but one nonzero vectors to $\mathrm{PC}_{n-1}(n-1)$ for odd $n \geqslant 3$.

Theorem 3 Let $n \geqslant 3$ be odd. Let $f \in \mathrm{B}_n$ and $b \in \{0,1\}^n$. Suppose f satisfies the PC with respect to $\mathrm{V}_n - \{b\}$. For $\alpha_1, \ldots, \alpha_{2^{n-1}} \in \{0,1\}^n$ such that $0 \leqslant dec(\alpha_1) < \cdots < dec(\alpha_{2^{n-1}}) \leqslant 2^n - 1$ and $\hat{F}(\alpha_i) \neq 0$ for $1 \leqslant i \leqslant 2^{n-1}$, let $f_W \in \mathrm{B}_{n-1}$ be defined as

$$\left[\hat{f}_W(0), \ldots, \hat{f}_W(2^{n-1}-1)\right] = \frac{1}{2^{\frac{n+1}{2}}}\left[\hat{F}(\alpha_1), \ldots, \hat{F}(\alpha_{2^{n-1}})\right].$$

Then, f_W is perfectly nonlinear.

(Proof) From the definition of the inverse Walsh transform,

$$\frac{1}{2^n}\left[\hat{F}(0), \ldots, \hat{F}(2^n-1)\right] H_n = \left[\hat{f}(0), \ldots, \hat{f}(2^n-1)\right].$$

Since f satisfies the PC with respect to $\mathrm{V}_n - \{b\}$,

$$\left|\hat{F}(\omega)\right| = \begin{cases} 2^{(n+1)/2} & \text{if } b \cdot \omega = 0 \\ 0 & \text{if } b \cdot \omega = 1 \end{cases} \text{ or } \begin{cases} 2^{(n+1)/2} & \text{if } b \cdot \omega = 1 \\ 0 & \text{if } b \cdot \omega = 0. \end{cases}$$

Thus,

$$\begin{aligned} \frac{1}{2^n}\left[\hat{F}(\alpha_1), \ldots, \hat{F}(\alpha_{2^{n-1}})\right] K_n(b,c) &= \left[\hat{f}(0), \ldots, \hat{f}(2^n-1)\right] \\ \left[\hat{f}_W(0), \ldots, \hat{f}_W(2^{n-1}-1)\right] K_n(b,c) &= 2^{\frac{n-1}{2}}\left[\hat{f}(0), \ldots, \hat{f}(2^n-1)\right]. \end{aligned}$$

where $c = 0$ and $c = 1$, respectively. From Lemma 4, for $K_n(b,c)$, there exists a nondegenerate $2^n \times 2^n$-matrix Π such that

$$K_n(b,c)\,\Pi = \left[\begin{array}{cc} H_{n-1} & (-1)^c H_{n-1} \end{array}\right]$$

Π exchanges columns of matrices when operated from the right of them. Hence,

$$\begin{aligned} &\left[\hat{f}_W(0), \ldots, \hat{f}_W(2^{n-1}-1)\right]\left[\begin{array}{cc} H_{n-1} & (-1)^c H_{n-1} \end{array}\right] = \\ &\qquad 2^{\frac{n-1}{2}}\left[\hat{f}(0), \ldots, \hat{f}(2^n-1)\right] \Pi. \end{aligned}$$

This equation shows that, for every $\omega \in \{0,1\}^{n-1}$,

$$\left|\left(\mathcal{W}(\hat{f}_W)\right)(\omega)\right| = 2^{\frac{n-1}{2}}.$$

This completes the proof. □

The following theorem states that the mapping in Theorem 3 is surjective.

Theorem 4 Let $n \geqslant 3$ be odd and $g \in \mathrm{B}_{n-1}$. Let $\alpha_1, \ldots, \alpha_{2^{n-1}} \in \{0,1\}^n$, $b \in \mathrm{V}_n$ and $c \in \{0,1\}$ such that $0 \leqslant dec(\alpha_1) < \cdots < dec(\alpha_{2^{n-1}}) \leqslant 2^n - 1$ and $b \cdot \alpha_i = c$ for $1 \leqslant i \leqslant 2^{n-1}$. Let $\hat{F} : \{0,1\}^n \to \mathbf{N}$ be defined as

$$\hat{F}(\omega) = \begin{cases} 2^{(n+1)/2}\hat{g}(i-1) & \text{if } \omega = \alpha_i, \\ 0 & \text{otherwise,} \end{cases}$$

and $\hat{f} = (\mathcal{W}^{-1}(\hat{F}))$. If g is perfectly nonlinear, then $\hat{f} : \{0,1\}^n \to \{-1,1\}$ and f satisfies the PC with respect to $\mathrm{V}_n - \{b\}$.

(Proof) Since $\hat{F}(\omega) = 0$ when $\omega \neq \alpha_i$ and $b \cdot \alpha_i = c$ for $1 \leqslant i \leqslant 2^{n-1}$,

$$\begin{aligned}
\left[\hat{f}\right] &= \frac{1}{2^n}\left[\hat{F}(0), \ldots, \hat{F}(2^n - 1)\right] H_n \\
&= \frac{1}{2^n}\left[\hat{F}(\alpha_1), \ldots, \hat{F}(\alpha_{2^{n-1}})\right] K_n(b, c) \\
&= \frac{1}{2^{\frac{n-1}{2}}}\left[[\hat{g}(0), \ldots, \hat{g}(2^{n-1} - 1)\right] K_n(b, c)
\end{aligned}$$

From Lemma 4, for $K_n(b,c)$, there exists a nondegenerate $2^n \times 2^n$-matrix Π such that

$$K_n(b,c)\ \Pi = \left[\begin{array}{cc} H_{n-1} & (-1)^c H_{n-1} \end{array}\right]$$

Π exchanges columns of matrices when operated from the right of them. Hence,

$$\begin{aligned}
\left[\hat{f}\right]\ \Pi &= \frac{1}{2^{\frac{n-1}{2}}}\left[\hat{g}(0), \ldots, \hat{g}(2^{n-1} - 1)\right]\left[\begin{array}{cc} H_{n-1} & (-1)^c H_{n-1} \end{array}\right] \\
&= \frac{1}{2^{\frac{n-1}{2}}}\left[\begin{array}{cc} \hat{G} & (-1)^c \hat{G} \end{array}\right].
\end{aligned}$$

Since $\left|\hat{G}(\omega)\right| = 2^{\frac{n-1}{2}}$ for every $\omega \in \{0,1\}^{n-1}$, $\hat{f} : \{0,1\}^n \to \{-1,1\}$ and, from Theorem 1, f satisfies the PC with respect to $\mathrm{V}_n - \{b\}$. □

From Theorem 3 and 4, it is obvious that the algorithm below generates all the Boolean functions in B_n that satisfy the PC with respect to all but one nonzero vectors from all the Boolean functions in $\mathrm{PC}_{n-1}(n-1)$ for odd $n \geqslant 3$.

Algorithm 1

input $p \in \mathrm{PC}_{n-1}(n-1)$, $b \in \mathrm{V}_n$ for odd $n \geqslant 3$.

output $f_0, f_1 \in \mathrm{B}_n$ that satisfy the the PC with respect to $V_n - \{b\}$.

procedure

1. Let $c \in \{0,1\}$ and $\alpha_1^c, \ldots, \alpha_{2^{n-1}}^c \in \{0,1\}^n$ such that

   $$0 \leqslant dec(\alpha_1^c) \leqslant \cdots \leqslant dec(\alpha_{2^{n-1}}^c) \leqslant 2^n - 1,$$

   and, for $1 \leqslant i \leqslant 2^{n-1}$,

   $$b \cdot \alpha_i^c = c.$$

2. Let

   $$\hat{F}_c(\omega) = \begin{cases} 2^{(n+1)/2}\hat{p}(i-1) & \text{if } \omega = \alpha_i^c \\ 0 & \text{otherwise,} \end{cases}$$

   where $\hat{F}_c = \mathcal{W}(\hat{f}_c)$.

3. Let

   $$\left[\hat{f}_c\right] = \frac{1}{2^n}\left[\hat{F}_c\right] H_n.$$

□

For Algorithm 1, since

$$\hat{F}(0) = \sum_{x \in \{0,1\}^n} (-1)^{f(x)} = 0,$$

f is balanced, and g is not balanced since $\hat{G}(0) \neq 0$. For every $p \in \mathrm{PC}_{n-1}(n-1)$ and $b \in \mathrm{V}_n$, let $Alg_n(p,b)$ denotes the set of the Boolean functions obtained by the above algorithm, which satisfy the PC with respect to $\mathrm{V}_n - \{b\}$. Since H_n is nondegenerate, for any different pairs (p,b) and (p',b'), $Alg_n(p,b) \cap Alg_n(p',b') = \phi$. Thus the following corollary can be obtained.

Corollary 6 For every odd $n \geqslant 3$, the number of Boolean functions in B_n which satisfy the PC with respect to all but one elements in V_n is $2(2^n-1)|\mathrm{PC}_{n-1}(n-1)|$, and the half of them are balanced. □

In particular, for the Boolean functions with n variables satisfying the PC of degree $n-1$, the following corollary is derived.

Corollary 7 For every odd $n \geqslant 3$,

- $|\mathrm{PC}_n(n-1)| = 2|\mathrm{PC}_{n-1}(n-1)|$,
- the number of balanced functions in $\mathrm{PC}_n(n-1)$ is $|\mathrm{PC}_{n-1}(n-1)|$.

□

4.2 Boolean functions with the even number of variables

Theorem 2 says that, for even $n \geqslant 2$, Boolean functions which satisfy the PC with respect to all but one or two nonzero vectors are perfectly nonlinear, because less than three different nonzero vectors are always linearly independent. Perfectly nonlinear Boolean functions are not balanced.

Seberry, et al.[SZZ93] presented a method for constructing balanced Boolean functions satisfying the PC with respect to all but three elements in V_n for every even $n \geqslant 4$. Their result is optimal in the sense that there exist no balanced Boolean functions which satisfy the PC with respect to all but less than three nonzero vectors.

Proposition 7 [SZZ93] Let $n \geqslant 4$ be even. For any pair of $b_1, b_2 \in \mathrm{V}_n$ such that $b_1 \neq b_2$, there exist balanced Boolean functions in B_n satisfying the PC with respect to $\mathrm{V}_n - \{b_1, b_2, b_1 \oplus b_2\}$. □

In this section, for even $n \geqslant 4$, an exact characterization is presented of Boolean functions in B_n satisfying the PC with respect to all but three linearly dependent elements in V_n. A method of construction of such Boolean functions are also presented, and some relationships between the number of them and that of perfectly nonlinear Boolean functions are given.

Firstly, we present two simple lemmas.

Lemma 5 There exist no positive integers x, y, z and m such that $x^2+y^2+z^2 = 2^m$.

(Proof) Suppose that x, y, z are positive integers. Then, x, y, z can be represented as

$$x = 2^{e_1}q_1,\ y = 2^{e_2}q_2,\ z = 2^{e_3}q_3,$$

where $e_1, e_2, e_3 \geqslant 0$, and q_1, q_2, q_3 are odd integers. Without loss of generality, we may assume that $0 \leqslant e_1 \leqslant e_2 \leqslant e_3$. If $x^2+y^2+z^2 = 2^m$, then

$$\begin{aligned} 2^{2e_1}{q_1}^2 + 2^{2e_2}{q_2}^2 + 2^{2e_3}{q_3}^2 &= 2^m \\ {q_1}^2 + 2^{2(e_2-e_1)}{q_2}^2 + 2^{2(e_3-e_1)}{q_3}^2 &= 2^{m-2e_1}. \end{aligned}$$

Since the left-hand side of the above equation is greater than 3, $m - 2e_1 \geqslant 2$, which implies that the left-hand side is even. Thus, $e_2 - e_1 = 0$ and $e_3 - e_1 \geqslant 1$. Then,

$${q_1}^2 + {q_2}^2 = 2^{m-2e_1} - 2^{2(e_3-e_1)}{q_3}^2.$$

Since both of q_1 and q_2 are odd, ${q_1}^2 + {q_2}^2$ is a multiple of 2 but not of 4. This contradicts that $m - 2e_1 \geqslant 2$ and $2(e_3 - e_1) \geqslant 2$. Hence, the lemma has been proved. □

Lemma 6 Let w, x, y, z and m be positive integers. $w^2+x^2+y^2+z^2=2^m$ if and only if m is even and $w=x=y=z=2^{(m-2)/2}$.

(Proof) Suppose that w, x, y, z are positive integers. Then, they are able to be represented as

$$w=2^{e_1}q_1,\ x=2^{e_2}q_2,\ y=2^{e_3}q_3,\ z=2^{e_4}q_4,$$

where $e_1,e_2,e_3,e_4\geqslant 0$, and q_1,q_2,q_3,q_4 are odd integers. Without loss of generality, we may assume that $0\leqslant e_1\leqslant e_2\leqslant e_3\leqslant e_4$. Since $w^2+x^2+y^2+z^2=2^m$,

$$\begin{array}{rcl} 2^{2e_1}{q_1}^2+2^{2e_2}{q_2}^2+2^{2e_3}{q_3}^2+2^{2e_4}{q_4}^2 &=& 2^m \\ {q_1}^2+2^{2(e_2-e_1)}{q_2}^2+2^{2(e_3-e_1)}{q_3}^2+2^{2(e_4-e_1)}{q_4}^2 &=& 2^{m-2e_1} \end{array}$$

Since the left-hand side of the above equation is greater than 4, $m-2e_1\geqslant 2$. Since the left-hand side is even, $e_2-e_1=0$. Thus,

$${q_1}^2+{q_2}^2+2^{2(e_3-e_1)}{q_3}^2+2^{2(e_4-e_1)}{q_4}^2=2^{m-2e_1}.$$

Since ${q_1}^2+{q_2}^2$ is a multiple of 2 but not of 4 and 2^{m-2e_1} is a multiple of 4, $e_3-e_1=e_4-e_1=0$ and

$${q_1}^2+{q_2}^2+{q_3}^2+{q_4}^2=2^{m-2e_1}.$$

For $i=1,2,3,4$, q_i can be represented as $q_i=2r_i+1$, where $r_i\geqslant 0$ is an integer. Hence,

$$4\left(\sum_{i=1}^{4}r_i(r_i+1)+1\right)=2^{m-2e_1}.$$

Because $\sum_{i=1}^{4}r_i(r_i+1)+1$ is odd, $m-2e_1=2$ and $r_1=r_2=r_3=r_4=0$. Hence, m is even and $w=x=y=z=2^{(m-2)/2}$. □

The following theorem presents a necessary and sufficient condition for $f\in \mathrm{B}_n$ to satisfy the PC with respect to all but three linearly dependent elements in V_n for even $n\geqslant 4$.

Theorem 5 Let $n\geqslant 4$ be even and $f\in\mathrm{B}_n$. Let b_1, b_2, b_3 be different elements in V_n and be linearly dependent. $f\notin \mathrm{PC}_n(n)$ satisfies the PC with respect to $\mathrm{V}_n-\{b_1,b_2,b_3\}$ if and only if

$$|\hat{F}(\omega)|=\begin{cases} 2^{n/2+1} & \text{if } b_1\cdot\omega=b_2\cdot\omega=b_3\cdot\omega=0 \\ 0 & \text{otherwise,}\end{cases}$$

or

$$|\hat{F}(\omega)|=\begin{cases} 2^{n/2+1} & \text{if } b_i\cdot\omega=0,\ b_j\cdot\omega=b_k\cdot\omega=1 \text{ for different } i,\ j,\ k \\ 0 & \text{otherwise.}\end{cases}$$

(Proof) $f\in\mathrm{B}_n$ satisfies the PC with respect to $\mathrm{V}_n-\{b_1,\ldots,b_k\}$ if and only if $C_f(a)=0$ for every $a\in\mathrm{V}_n-\{b_1,b_2,b_3\}$. From Lemma 2, $\left[\hat{F}^2\right]$ can be represented as

$$\left[\hat{F}^2\right]=C_f(0){v_0}^{\mathrm{T}}+C_f(b_1){v_{b_1}}^{\mathrm{T}}+C_f(b_2){v_{b_2}}^{\mathrm{T}}+C_f(b_3){v_{b_3}}^{\mathrm{T}},$$

Let

$$\begin{array}{rcl} u_0 &=& {v_0}^{\mathrm{T}}, \\ u_i &=& ({v_0}^{\mathrm{T}}+{v_{b_i}}^{\mathrm{T}})/2 \text{ for } i=1,2,3, \end{array}$$

then we can rewrite $\left[\hat{F}^2\right]$ as

$$\left[\hat{F}^2\right]=c_0u_0+c_1u_1+c_2u_2+c_3u_3,$$

where

$$\begin{aligned} c_0 &= C_f(0) - (C_f(b_1) + C_f(b_2) + C_f(b_3)) \\ c_i &= 2C_f(b_i). \end{aligned}$$

Since

$$\begin{aligned} u_0 &= [1, \ldots, 1], \\ u_i &= [1 \oplus l_{b_i}(0), \ldots, 1 \oplus l_{b_i}(2^n - 1)] \text{ for } i = 1, 2, 3, \end{aligned}$$

and l_{b_i} is balanced for every $b_i \in \mathrm{V}_n$,

$$\sum_{\omega \in \{0,1\}^n} \hat{F}^2(\omega) = 2^n c_0 + 2^{n-1}(c_1 + c_2 + c_3) = 2^{2n}.$$

Thus,

$$(c_0 + c_1 + c_2 + c_3) + (c_0 + c_1) + (c_0 + c_2) + (c_0 + c_3) = 2^{n+2}.$$

Since

$$\hat{F}^2(\omega) = \begin{cases} c_0 + c_i & \text{if } b_i = 0 \text{ and } b_j \cdot \omega = 1 \\ & \text{ for } i = 1, 2, 3 \text{ and } j \in \{1, 2, 3\} - \{i\} \\ c_o + c_1 + c_2 + c_3 & \text{if } b_i \cdot \omega = 0 \text{ for } i = 1, 2, 3, \end{cases}$$

from Lemma 1, 5, 6, there are following two cases:

Case 1 $c_0 + c_1 + c_2 + c_3 = c_0 + c_1 = c_0 + c_2 = c_0 + c_3 = 2^n$,

Case 2 only one of $c_0 + c_1 + c_2 + c_3$, $c_0 + c_1$, $c_0 + c_2$ and $c_0 + c_3$ is 2^{n+2} and the others are 0.

For Case 1, $f \in \mathrm{PC}_n(n)$.

For Case 2, if $c_0 + c_1 + c_2 + c_3 = 2^{n+2}$, then $\hat{F}^2(\omega) = 2^{n+2}$ when $b_1 \cdot \omega = b_2 \cdot \omega = b_3 \cdot \omega = 0$. If $c_0 + c_i = 2^{n+2}$, then $\hat{F}^2(\omega) = 2^{n+2}$ when $b_i \cdot \omega = 0$ and $b_j \cdot \omega = b_k \cdot \omega = 1$ for different i, j, k.

Hence, the theorem has been proved. □

The next corollary can be proved in the same way as Corollary 3.

Corollary 8 Let $n \geqslant 4$ be even. Let b_1, b_2, b_3 be different elements in V_n and be linearly dependent. If $f \in \mathrm{B}_n$ is balanced and satisfies the PC with respect to $\mathrm{V}_n - \{b_1, b_2, b_3\}$, then, for each of $i \in \{1, 2, 3\}$,

$$f(x) \oplus f(x \oplus b_i) \equiv 0 \text{ or } 1.$$

(Proof) For even $n \geqslant 4$, if $f \in \mathrm{B}_n - \mathrm{PC}_n(n)$ satisfies the PC with respect to $\mathrm{V}_n - \{b_1, b_2, b_3\}$, then, from the proof of Theorem 5,

$$\begin{aligned} C_f(0) + C_f(b_1) + C_f(b_2) + C_f(b_3) &= 2^{n+2} \\ C_f(0) + C_f(b_1) - C_f(b_2) - C_f(b_3) &= 0 \\ C_f(0) - C_f(b_1) + C_f(b_2) - C_f(b_3) &= 0 \\ C_f(0) - C_f(b_1) - C_f(b_2) + C_f(b_3) &= 0 \text{ for different } i, j, k \in \{1, 2, 3\}, \end{aligned}$$

or, for different $i, j, k \in \{1, 2, 3\}$,

$$\begin{aligned} C_f(0) + C_f(b_1) + C_f(b_2) + C_f(b_3) &= 0 \\ C_f(0) + C_f(b_i) - C_f(b_j) - C_f(b_k) &= 2^{n+2} \\ C_f(0) - C_f(b_i) + C_f(b_j) - C_f(b_k) &= 0 \\ C_f(0) - C_f(b_i) - C_f(b_j) + C_f(b_k) &= 0 \end{aligned}$$

For the former case, $C_f(b_1) = C_f(b_2) = C_f(b_3) = 2^n$, and for the latter case, $C_f(b_i) = 2^n$ and $C_f(b_j) = C_f(b_k) = -2^n$. $C_f(b) = 2^n$ and $C_f(b) = -2^n$ implies that $f(x) \oplus f(x \oplus b) \equiv 0$ and $f(x) \oplus f(x \oplus b) \equiv 1$, respectively. □

The following corollary can be easily derived from Theorem 5. This presents a spectral property of the balanced Boolean functions satisfying the PC with respect to all but three elements in V_n for every even $n \geqslant 4$.

Corollary 9 Let $n \geqslant 4$ be even. Let b_1, b_2, $b_3 \in \mathrm{V}_n$ be different and linearly dependent. $f \in \mathrm{B}_n$ is balanced and satisfies the PC with respect to $\mathrm{V}_n - \{b_1, b_2, b_3\}$ if and only if

$$\left|\hat{F}(\omega)\right| = \begin{cases} 2^{n/2+1} & \text{if } b_i \cdot \omega = 0,\ b_j \cdot \omega = b_k \cdot \omega = 1 \text{ for different } i,\ j,\ k \\ 0 & \text{otherwise.} \end{cases}$$

□

Corollary 10 Let $n \geqslant 4$ be even. The nonlinearity of any balanced Boolean function in B_n satisfying the PC with respect to all but three elements in V_n is $2^{n-1} - 2^{n/2}$.

(Proof) This corollary directly follows from Proposition 3 and Theorem 5. □

Seberry, et al.[SZZ93] proved that the nonlinearities of balanced Boolean functions satisfying the PC with respect to all but three nonzero vectors are at least $2^{n-1} - 2^{n/2}$. Corollary 10 determines the nonlinearity of balanced Boolean functions satisfying the PC with respect to all but three nonzero vectors uniquely, and shows that the lower bound of nonlinearity of Seberry, et al. is optimal.

In the following, it is shown that, for every even $n \geqslant 4$, one can construct all Boolean functions that satisfy the PC with respect to all but three linearly dependent vectors in V_n from all Boolean functions in $\mathrm{PC}_{n-2}(n-2)$.

A lemma is firstly proved for the basis of the following discussion.

Lemma 7 Let $n \geqslant 2$, $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in \mathrm{V}_n$ such that $a \neq b$ and $c, d \in \{0, 1\}$. Let $K_n(a, c; b, d)$ be a $2^{n-2} \times 2^n$ matrix that is constructed by removing all $(dec(\omega) + 1)$-th rows of H_n, where $a \cdot \omega \neq c$ or $b \cdot \omega \neq d$. Then,

- for each column v of H_{n-2}, $K_n(a, c; b, d)$ has four columns that is equal to v if $c = d = 0$, and has two columns that is equal to v and two columns that is equal to $-v$ if $c \neq 0$ or $d \neq 0$,
- for every i such that $1 \leqslant i \leqslant 2^n$,

$$\begin{aligned} col(K_n(a, c; b, d), i) &= col(K_n(a, c'; b, d'), i) \text{ or} \\ col(K_n(a, c; b, d), i) &= -col(K_n(a, c'; b, d'), i), \end{aligned}$$

  and, for $\{(c_1, d_1), (c_2, d_2), (c_3, d_3), (c_4, d_4)\} = \{0, 1\}^2$,

$$\begin{aligned} col(K_n(a, c_1; b, d_1), i) &= col(K_n(a, c_2; b, d_2), i) \\ &\Updownarrow \\ col(K_n(a, c_3; b, d_3), i) &= col(K_n(a, c_4; b, d_4), i). \end{aligned}$$

(Proof) This lemma can be proved by induction.

For every (a, c) and (b, d), $K_n(a, c; b, d) = K_n(b, d; a, c)$. When $n = 2$, since

$$H_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

$$\begin{aligned} K_n((1,0), 0; (0,1), 0) &= \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} \\ K_n((1,0), 0; (0,1), 1) &= \begin{bmatrix} 1 & -1 & 1 & -1 \end{bmatrix} \\ K_n((1,0), 1; (0,1), 0) &= \begin{bmatrix} 1 & 1 & -1 & -1 \end{bmatrix} \\ K_n((1,0), 1; (0,1), 1) &= \begin{bmatrix} 1 & -1 & -1 & 1 \end{bmatrix}, \end{aligned}$$

and, for $a = (1,0), b = (1,1)$ and $a = (0,1), b = (1,1)$,

$$\begin{aligned}
K_n(a,0;b,0) &= \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} \\
K_n(a,1;b,0) &= \begin{bmatrix} 1 & -1 & 1 & -1 \end{bmatrix} \\
K_n(a,0;b,1) &= \begin{bmatrix} 1 & -1 & -1 & 1 \end{bmatrix} \\
K_n(a,1;b,1) &= \begin{bmatrix} 1 & 1 & -1 & -1 \end{bmatrix}.
\end{aligned}$$

Thus the theorem is proved for $n = 2$ because $H_0 = [1]$.

For $a_n = b_n = 0$. Since

$$\begin{aligned}
a \cdot (\omega_1, \ldots, \omega_{n-1}, 0) &= a \cdot (\omega_1, \ldots, \omega_{n-1}, 1), \\
b \cdot (\omega_1, \ldots, \omega_{n-1}, 0) &= b \cdot (\omega_1, \ldots, \omega_{n-1}, 1),
\end{aligned}$$

and

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$$

$$K_n(a,c;b,d) = \begin{bmatrix} K_{n-1}(\langle a \rangle_{n-1}, c; \langle b \rangle_{n-1}, d) & K_{n-1}(\langle a \rangle_{n-1}, c; \langle b \rangle_{n-1}, d) \\ K_{n-1}(\langle a \rangle_{n-1}, c; \langle b \rangle_{n-1}, d) & -K_{n-1}(\langle a \rangle_{n-1}, c; \langle b \rangle_{n-1}, d) \end{bmatrix}.$$

From the inductive assumption, for every column v' of H_{n-3}, $K_{n-1}(\langle a \rangle_{n-1}, c; \langle b \rangle_{n-1}, d)$ has four columns that are equal to v' if $c = d = 0$, and has two columns that are equal to v and two columns that are equal to $-v'$ if $c = 1$ or $d = 1$. Thus, for every column v of H_{n-2}, $K_n(a,c;b,d)$ has four columns that are equal to v if $c = d = 0$, and has two columns that are equal to v and two columns that are equal to $-v$ if $c = 1$ or $d = 1$.

It is apparent from the inductive assumption that, for every i such that $1 \leqslant i \leqslant 2^n$,

$$\begin{aligned}
col(K_n(a,c;b,d),i) &= col(K_n(a,c';b,d'),i) \text{ or} \\
col(K_n(a,c;b,d),i) &= -col(K_n(a,c';b,d'),i).
\end{aligned}$$

It is also apparent that and, for $\{(c_1,d_1),(c_2,d_2),(c_3,d_3),(c_4,d_4)\} = \{0,1\}^2$,

$$\begin{aligned}
col(K_n(a,c_1;b,d_1),i) &= col(K_n(a,c_2;b,d_2),i) \\
&\Updownarrow \\
col(K_n(a,c_3;b,d_3),i) &= col(K_n(a,c_4;b,d_4),i).
\end{aligned}$$

For $a_n = 1, b_n = 0$.

$$\begin{aligned}
a \cdot (\omega_1, \ldots, \omega_{n-1}, 0) &= \langle a \rangle_{n-1} \cdot \langle \omega \rangle_{n-1} \\
a \cdot (\omega_1, \ldots, \omega_{n-1}, 1) &= \langle a \rangle_{n-1} \cdot \langle \omega \rangle_{n-1} \oplus 1.
\end{aligned}$$

(i) When $a = (0, \ldots, 0, 1)$,

$$\begin{aligned}
K_n(a,0;b,0) &= \begin{bmatrix} K_{n-1}(\langle b \rangle_{n-1}, 0) & K_{n-1}(\langle b \rangle_{n-1}, 0) \end{bmatrix}, \\
K_n(a,0;b,1) &= \begin{bmatrix} K_{n-1}(\langle b \rangle_{n-1}, 1) & K_{n-1}(\langle b \rangle_{n-1}, 1) \end{bmatrix}, \\
K_n(a,1;b,0) &= \begin{bmatrix} K_{n-1}(\langle b \rangle_{n-1}, 0) & -K_{n-1}(\langle b \rangle_{n-1}, 0) \end{bmatrix}, \\
K_n(a,1;b,1) &= \begin{bmatrix} K_{n-1}(\langle b \rangle_{n-1}, 1) & -K_{n-1}(\langle b \rangle_{n-1}, 1) \end{bmatrix}.
\end{aligned}$$

From Lemma 4, for every column v of H_{n-2}, $K_{n-1}(\langle b\rangle_{n-1}, 0)$ has two columns that are equal to v, and $K_{n-1}(\langle b\rangle_{n-1}, 1)$ has v and $-v$. Thus, $K_n(a, c; b, d)$ has four columns equal to v if $c = d = 0$, and has two columns equal to v and two columns equal to $-v$ if $c = 1$ or $d = 1$.

Since, for every j such that $1 \leqslant j \leqslant 2^{n-1}$,

$$\begin{array}{rcl} col(K_{n-1}(\langle b\rangle_{n-1}, 0), j) & = & col(K_{n-1}(\langle b\rangle_{n-1}, 1), j) \text{ or} \\ col(K_{n-1}(\langle b\rangle_{n-1}, 0), j) & = & -col(K_{n-1}(\langle b\rangle_{n-1}, 1), j), \end{array}$$

for every i such that $1 \leqslant i \leqslant 2^n$,

$$\begin{array}{rcl} col(K_n(a, c; b, d), i) & = & col(K_n(a, c'; b, d'), i) \text{ or} \\ col(K_n(a, c; b, d), i) & = & -col(K_n(a, c'; b, d'), i), \end{array}$$

and also, for $\{(c_1, d_1), (c_2, d_2), (c_3, d_3), (c_4, d_4)\} = \{0, 1\}^2$,

$$\begin{array}{rcl} col(K_n(a, c_1; b, d_1), i) & = & col(K_n(a, c_2; b, d_2), i) \\ & \Updownarrow & \\ col(K_n(a, c_3; b, d_3), i) & = & col(K_n(a, c_4; b, d_4), i). \end{array}$$

(ii) When $a \neq (0, \ldots, 0, 1)$,

$$K_n(a, c; b, d) = \left[\begin{array}{cc} K_{n-1}(\langle a\rangle_{n-1}, c; \langle b\rangle_{n-1}, d) & K_{n-1}(\langle a\rangle_{n-1}, c; \langle b\rangle_{n-1}, d) \\ K_{n-1}(\langle a\rangle_{n-1}, 1 \oplus c; \langle b\rangle_{n-1}, d) & -K_{n-1}(\langle a\rangle_{n-1}, 1 \oplus c; \langle b\rangle_{n-1}, d) \end{array} \right].$$

From the inductive assumption, for every i such that $1 \leqslant i \leqslant 2^{n-1}$,

$$\begin{array}{rcl} col(K_{n-1}(\langle a\rangle_{n-1}, c; \langle b\rangle_{n-1}, d), i) & = & col(K_{n-1}(\langle a\rangle_{n-1}, 1 \oplus c; \langle b\rangle_{n-1}, d), i) \text{ or} \\ col(K_{n-1}(\langle a\rangle_{n-1}, c; \langle b\rangle_{n-1}, d), i) & = & -col(K_{n-1}(\langle a\rangle_{n-1}, 1 \oplus c; \langle b\rangle_{n-1}, d), i), \end{array}$$

and, for every $(c_1, d_1), (c_2, d_2) \in \{0, 1\}^2$ such that $(c_1, d_1) \neq (c_2, d_2)$,

$$\begin{array}{rcl} col(K_{n-1}(\langle a\rangle_{n-1}, c_1; \langle b\rangle_{n-1}, d_1), i) & = & col(K_{n-1}(\langle a\rangle_{n-1}, 1 \oplus c_1; \langle b\rangle_{n-1}, d_1), i) \\ & \Updownarrow & \\ col(K_{n-1}(\langle a\rangle_{n-1}, c_2; \langle b\rangle_{n-1}, d_2), i) & = & col(K_{n-1}(\langle a\rangle_{n-1}, 1 \oplus c_2; \langle b\rangle_{n-1}, d_2), i). \end{array}$$

Thus, there exists some $2^n \times 2^n$-matrix Π, which permutes the columns of matrices, such that, for every c and d,

$$K_n(a, c; b, d)\, \Pi = \left[\begin{array}{cc} K_{n-1}(\langle a\rangle_{n-1}, c; \langle b\rangle_{n-1}, d) & K_{n-1}(\langle a\rangle_{n-1}, c; \langle b\rangle_{n-1}, d) \\ K_{n-1}(\langle a\rangle_{n-1}, c; \langle b\rangle_{n-1}, d) & -K_{n-1}(\langle a\rangle_{n-1}, c; \langle b\rangle_{n-1}, d) \end{array} \right].$$

Thus, this case can be proved in the same way as the case where $a_n = b_n = 0$.

For $a_n = b_n = 1$.

(i) When $a = (0, \ldots, 0, 1)$,

$$\begin{array}{rcl} K_n(a, 0; b, 0) & = & \left[\begin{array}{cc} K_{n-1}(\langle b\rangle_{n-1}, 0) & K_{n-1}(\langle b\rangle_{n-1}, 0) \end{array} \right], \\ K_n(a, 0; b, 1) & = & \left[\begin{array}{cc} K_{n-1}(\langle b\rangle_{n-1}, 1) & K_{n-1}(\langle b\rangle_{n-1}, 1) \end{array} \right], \\ K_n(a, 1; b, 0) & = & \left[\begin{array}{cc} K_{n-1}(\langle b\rangle_{n-1}, 1) & -K_{n-1}(\langle b\rangle_{n-1}, 1) \end{array} \right], \\ K_n(a, 1; b, 1) & = & \left[\begin{array}{cc} K_{n-1}(\langle b\rangle_{n-1}, 0) & -K_{n-1}(\langle b\rangle_{n-1}, 0) \end{array} \right]. \end{array}$$

This case can be proved in the same way as the case where $a = (0, \ldots, 0, 1)$ and b such that $b_n \neq 0$.

(ii) When $a \neq (0, \ldots, 0, 1)$ and $b \neq (0, \ldots, 0, 1)$,

$$K_n(a, c; b, d) = \\ \begin{bmatrix} K_{n-1}(\langle a \rangle_{n-1}, c; \langle b \rangle_{n-1}, d) & K_{n-1}(\langle a \rangle_{n-1}, c; \langle b \rangle_{n-1}, d) \\ K_{n-1}(\langle a \rangle_{n-1}, 1 \oplus c; \langle b \rangle_{n-1}, 1 \oplus d) & -K_{n-1}(\langle a \rangle_{n-1}, 1 \oplus c; \langle b \rangle_{n-1}, 1 \oplus d) \end{bmatrix}.$$

In the same way as for the above case, it can be shown that there exists some $2^n \times 2^n$-matrix Π, which permutes the columns of matrices, such that, for every c and d,

$$K_n(a, c; b, d)\, \Pi = \\ \begin{bmatrix} K_{n-1}(\langle a \rangle_{n-1}, c; \langle b \rangle_{n-1}, d) & K_{n-1}(\langle a \rangle_{n-1}, c; \langle b \rangle_{n-1}, d) \\ K_{n-1}(\langle a \rangle_{n-1}, c; \langle b \rangle_{n-1}, d) & -K_{n-1}(\langle a \rangle_{n-1}, c; \langle b \rangle_{n-1}, d) \end{bmatrix}.$$

This case can be proved in the same way as the case where $a_n = b_n = 0$.

This completes the proof. □

Example 2 Let $n = 4$ and $a = (0, 1, 0, 1)$, $b = (1, 0, 0, 1)$. Let $H_4 = [v_1^4, \ldots, v_{16}^4]$ and $H_2 = [v_1, v_2, v_3, v_4]$. Then,

$$\begin{aligned} K_4(a, 0; b, 0) &= \begin{bmatrix} v_1^4 & v_5^4 & v_{12}^4 & v_{16}^4 \end{bmatrix}^{\mathrm{T}} \\ &= \big[\; v_1 \;\; v_3 \;\; v_3 \;\; v_1 \;\; v_2 \;\; v_4 \;\; v_4 \;\; v_2 \\ &\qquad v_3 \;\; v_1 \;\; v_1 \;\; v_3 \;\; v_4 \;\; v_2 \;\; v_2 \;\; v_4 \;\big] \end{aligned}$$

$$\begin{aligned} K_4(a, 0; b, 1) &= \begin{bmatrix} v_2^4 & v_6^4 & v_{11}^4 & v_{15}^4 \end{bmatrix}^{\mathrm{T}} \\ &= \big[\; v_1 \;\; -v_3 \;\; v_3 \;\; -v_1 \;\; v_2 \;\; -v_4 \;\; v_4 \;\; -v_2 \\ &\qquad v_3 \;\; -v_1 \;\; v_1 \;\; -v_3 \;\; v_4 \;\; -v_2 \;\; v_2 \;\; -v_4 \;\big] \end{aligned}$$

$$\begin{aligned} K_4(a, 1; b, 0) &= \begin{bmatrix} v_3^4 & v_7^4 & v_{10}^4 & v_{14}^4 \end{bmatrix}^{\mathrm{T}} \\ &= \big[\; v_1 \;\; v_3 \;\; -v_3 \;\; -v_1 \;\; v_2 \;\; v_4 \;\; -v_4 \;\; -v_2 \\ &\qquad v_3 \;\; v_1 \;\; -v_1 \;\; -v_3 \;\; v_4 \;\; v_2 \;\; -v_2 \;\; -v_4 \;\big] \end{aligned}$$

$$\begin{aligned} K_4(a, 1; b, 1) &= \begin{bmatrix} v_4^4 & v_8^4 & v_9^4 & v_{13}^4 \end{bmatrix}^{\mathrm{T}} \\ &= \big[\; v_1 \;\; -v_3 \;\; -v_3 \;\; v_1 \;\; v_2 \;\; -v_4 \;\; -v_4 \;\; v_2 \\ &\qquad v_3 \;\; -v_1 \;\; -v_1 \;\; v_3 \;\; v_4 \;\; -v_2 \;\; -v_2 \;\; v_4 \;\big] \end{aligned}$$

For each column v_i of H_2, $K_4(a, 0; b, 0)$ has four columns that are equal to v_i, and each of $K_4(a, 0; b, 1)$, $K_4(a, 1; b, 0)$ and $K_4(a, 1; b, 1)$ has two columns that are equal to v_i and two columns that are equal to $-v_i$. □

The following theorem implies an injective mapping from the set of Boolean functions in B_n that satisfy the PC with respect to all but three linearly dependent nonzero vectors to $\mathrm{PC}_{n-2}(n-2)$ for even $n \geqslant 4$.

Theorem 6 Let $n \geqslant 4$ be even. Let $f \in \mathrm{B}_n$ and $b_1, b_2, b_3 \in \{0, 1\}^n$ such that b_1, b_2, b_3 are different and linearly dependent. Suppose f satisfies the PC with respect to $\mathrm{V}_n - \{b_1, b_2, b_3\}$ and is not perfectly nonlinear. For $\alpha_1, \ldots, \alpha_{2^{n-2}} \in \{0,1\}^n$ such that $1 \leqslant dec(\alpha_1) < \cdots < dec(\alpha_{2^{n-2}}) \leqslant 2^n - 1$ and $\hat{F}(\alpha_i) \neq 0$ for $1 \leqslant i \leqslant 2^{n-2}$, let $f_W \in \mathrm{B}_{n-1}$ be defined as

$$\left[\hat{f}_W(0), \ldots, \hat{f}_W(2^{n-2}-1)\right] = \frac{1}{2^{\frac{n}{2}+1}} \left[\hat{F}(\alpha_1), \ldots, \hat{F}(\alpha_{2^{n-2}})\right].$$

Then f_W is perfectly nonlinear.

(Proof) Since f satisfies the PC with respect to $\mathrm{V}_n - \{b_1, b_2, b_3\}$ and is not perfectly nonlinear,

$$|\hat{F}(\omega)| = \begin{cases} 2^{n/2+1} & \text{if } b_1 \cdot \omega = b_2 \cdot \omega = b_3 \cdot \omega = 0 \\ 0 & \text{otherwise,} \end{cases}$$

or

$$|\hat{F}(\omega)| = \begin{cases} 2^{n/2+1} & \text{if } b_i \cdot \omega = 0,\ b_j \cdot \omega = b_k \cdot \omega = 1 \text{ for different } i,\ j,\ k \\ 0 & \text{otherwise.} \end{cases}$$

Without loss of generality, we can fix $i = 1$, $j = 2$, $k = 3$. Thus,

$$\begin{aligned} \frac{1}{2^n}\left[\hat{F}(0), \ldots, \hat{F}(2^n-1)\right] H_n &= \left[\hat{f}(0), \ldots, \hat{f}(2^n-1)\right] \\ \frac{1}{2^n}\left[\hat{F}(\alpha_1), \ldots, \hat{F}(\alpha_{2^{n-2}})\right] K_n(b_1, 0; b_2, c) &= \left[\hat{f}(0), \ldots, \hat{f}(2^n-1)\right] \\ \left[\hat{f}_W(0), \ldots, \hat{f}_W(2^{n-2}-1)\right] K_n(b_1, 0; b_2, c) &= 2^{\frac{n}{2}-1}\left[\hat{f}(0), \ldots, \hat{f}(2^n-1)\right], \end{aligned}$$

where $c = 0$ and $c = 1$, respectively. From Lemma 7, there exists a nondegenerate $2^n \times 2^n$-matrix Π such that

$$K_n(b_1, 0; b_2, c) = \left[\begin{array}{cccc} H_{n-2} & H_{n-2} & (-1)^c H_{n-2} & (-1)^c H_{n-2} \end{array}\right].$$

Π exchanges columns of $K_n(b_1, 0; b_2, c)$. Hence,

$$\begin{aligned} &\left[\hat{f}_W(0), \ldots, \hat{f}_W(2^{n-2}-1)\right]\left[\begin{array}{cccc} H_{n-2} & H_{n-2} & (-1)^c H_{n-2} & (-1)^c H_{n-2} \end{array}\right] = \\ &\qquad 2^{\frac{n}{2}-1}\left[\hat{f}(0), \ldots, \hat{f}(2^n-1)\right]\Pi, \end{aligned}$$

which shows that

$$\left|\left(\mathcal{W}(\hat{f}_W)\right)(\omega)\right| = 2^{\frac{n}{2}-1}$$

for every $\omega \in \{0,1\}^{n-2}$. This completes the proof. □

The following theorem states that the mapping in Theorem 6 is surjective.

Theorem 7 Let $n \geqslant 4$ be even and $g \in \mathrm{B}_{n-2}$. Let $\alpha_1, \ldots, \alpha_{2^{n-2}} \in \{0,1\}^n$, $b_1, b_2, b_3 \in \mathrm{V}_n$ and $c, d \in \{0,1\}$ such that $0 \leqslant dec(\alpha_1) < \cdots < dec(\alpha_{2^{n-2}}) \leqslant 2^n - 1$ and $b_1 \cdot \alpha_i = c$, $b_2 \cdot \alpha_i = d$ and $b_3 \cdot \alpha_i = c \oplus d$ for $1 \leqslant i \leqslant 2^{n-2}$. Let $\hat{F} : \{0,1\}^n \to \mathbf{N}$ be defined as

$$\hat{F}(\omega) = \begin{cases} 2^{n/2+1}\hat{g}(i-1) & \text{if } \omega = \alpha_i, \\ 0 & \text{otherwise,} \end{cases}$$

and $\hat{f} = \mathcal{W}^{-1}(\hat{F})$. If g is perfectly nonlinear, then $\hat{f} : \{0,1\}^n \to \{-1,1\}$ and f satisfies the PC with respect to $\mathrm{V}_n - \{b_1, b_2, b_3\}$.

(Proof) Since $\hat{F}(\omega) = 0$ when $\omega \neq \alpha_i$ and $b_1 \cdot \alpha_i = c$ and $b_2 \cdot \alpha_i = d$ for $1 \leqslant i \leqslant 2^{n-2}$,

$$\begin{aligned} \left[\hat{f}\right] &= \frac{1}{2^n}\left[\hat{F}(0), \ldots, \hat{F}(2^n-1)\right] H_n \\ &= \frac{1}{2^n}\left[\hat{F}(\alpha_1), \ldots, \hat{F}(\alpha_{2^{n-2}})\right] K_n(b_1, c; b_2, d) \\ &= \frac{1}{2^{\frac{n-1}{2}}}\left[[\hat{g}(0), \ldots, \hat{g}(2^{n-2}-1)\right] K_n(b_1, c; b_2, d) \end{aligned}$$

From Lemma 7, for $K_n(b_1, c; b_2, d)$, there exists a nondegenerate $2^n \times 2^n$-matrix Π such that

$$K_n(b_1, c; b_2, d)\, \Pi = \left[\begin{array}{cccc} H_{n-2} & H_{n-2} & (-1)^{c\vee d} H_{n-2} & (-1)^{c\vee d} H_{n-2} \end{array}\right]$$

Π exchanges columns of $K_n(b_1, c; b_2, d)$. Hence,

$$\begin{aligned} \left[\hat{f}\right]\, \Pi &= \frac{1}{2^{\frac{n}{2}-1}} \left[\hat{g}(0), \ldots, \hat{g}(2^{n-1}-1)\right] \left[\begin{array}{cccc} H_{n-2} & H_{n-2} & (-1)^{c\vee d} H_{n-2} & (-1)^{c\vee d} H_{n-2} \end{array}\right] \\ &= \frac{1}{2^{\frac{n}{2}-1}} \left[\begin{array}{cccc} \hat{G} & \hat{G} & (-1)^{c\vee d}\hat{G} & (-1)^{c\vee d}\hat{G} \end{array}\right]. \end{aligned}$$

Since $\left|\hat{G}(\omega)\right| = 2^{\frac{n}{2}-1}$ for every $\omega \in \{0,1\}^{n-2}$, $\hat{f} : \{0,1\}^n \to \{-1,1\}$ and, from Theorem 5, f satisfies the PC with respect to $\mathrm{V}_n - \{b_1, b_2, b_3\}$. □

From Theorem 6 and 7, it is obvious that the algorithm below generates all the Boolean functions in B_n that satisfy the PC with respect to all but three nonzero vectors and that is not perfectly nonlinear from all the Boolean functions in $\mathrm{PC}_{n-2}(n-2)$ for even $n \geqslant 4$.

Algorithm 2

input $p \in \mathrm{PC}_{n-2}(n-2)$, $b_1, b_2 \in \mathrm{V}_n$ for even $n \geqslant 4$.

output $f_{(0,0)}, f_{(0,1)}, f_{(1,0)}, f_{(1,1)} \in \mathrm{B}_n$ that satisfy the PC with respect to $V_n - \{b_1, b_2, b_1 \oplus b_2\}$.

procedure

1. Let $(c,d) \in \{0,1\}^2$ and $\alpha_1^{(c,d)}, \ldots, \alpha_{2^{n-2}}^{(c,d)} \in \{0,1\}^n$ such that

   $$0 \leqslant dec(\alpha_1^{(c,d)}) < \cdots < dec(\alpha_{2^{n-2}}^{(c,d)}) \leqslant 2^n - 1,$$

   and, for every i such that $1 \leqslant i \leqslant 2^{n-2}$,

   $$b_1 \cdot \alpha_i^{(c,d)} = c,\ b_2 \cdot \alpha_i^{(c,d)} = d$$

2. Let

   $$\hat{F}_{(c,d)}(\omega) = \begin{cases} 2^{n/2+1}\hat{p}(i-1) & \text{if } \omega = \alpha_i^{(c,d)} \\ 0 & \text{otherwise,} \end{cases}$$

   where $\hat{F}_{(c,d)} = \mathcal{W}(\hat{f}_{(c,d)})$.

3. Let

   $$\left[\hat{f}_{(c,d)}\right] = \frac{1}{2^n}\left[\hat{F}_{(c,d)}\right] H_n.$$

□

For Algorithm 2, $\hat{F}_{(c,d)}(0) = 0$ only if $(c,d) = (0,0)$. Thus, $f_{(c,d)}$ is balanced if $(c,d) = (0,0)$ and not balanced otherwise.

The following corollary presents the relationship between the number of balanced Boolean functions satisfying the PC with respect to all but three elements in V_n and that of perfectly nonlinear Boolean functions in B_{n-2}.

Corollary 11 Let $n \geqslant 4$ be even. The number of balanced Boolean functions in B_n satisfying the PC with respect to all but three elements in V_n is $\begin{pmatrix} 2^n - 1 \\ 2 \end{pmatrix} |\mathrm{PC}_{n-2}(n-2)|$. □

4.3 Examples

This section gives examples of Algorithm 1 and Algorithm2.

Example 3 Two Boolean functions in B_5 are constructed that satisfy the PC with respect to all but one nonzero vectors.

Let $p \in \mathrm{PC}_4(4)$ be

$$p(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_3x_4.$$

Let $b = (0, 1, 1, 1, 1)$.

The elements ω's in $\{0,1\}^5$ that satisfy $b \cdot \omega = 0$ are

$$0, 1, 6, 7, 10, 11, 12, 13, 18, 19, 20, 21, 24, 25, 30, 31,$$

where each of the numbers represents $dec(\omega)$. Thus,

$$\left[\hat{F_0}\right] = [0, 0, 8, 8, 8, -8, 0, 0, 8, 8, 0, 0, 0, 0, 8, -8, 8, 8, 0, 0, 0, 0, 8, -8, 0, 0, -8, -8, -8, 8, 0, 0].$$

$$\begin{aligned} \left[\hat{f_0}\right] &= \frac{1}{2^5}\left[\hat{F_0}\right] H_5 \\ &= [1, 1, 1, -1, 1, -1, 1, 1, 1, 1, -1, 1, 1, -1, -1, -1, \\ &\quad 1, 1, -1, 1, 1, -1, -1, -1, -1, -1, -1, 1, -1, 1, -1, -1]. \end{aligned}$$

The algebraic normal form of f_0 is

$$f_0(x_1, \ldots, x_5) = x_1x_2 \oplus x_1x_3 \oplus x_2x_4 \oplus x_2x_5 \oplus x_4x_5.$$

f_1 can be generated in the same way as the above.

$$f_1(x_1, \ldots, x_5) = x_2 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_4 \oplus x_2x_5 \oplus x_4x_5.$$

The truth tables of f_1 and f_2 are shown in Figure 1. f_0 is balanced, while f_1 is not balanced. $f_0, f_1 \in \mathrm{PC}_5(4)$ since they satisfy the PC with respect to $\mathrm{V}_5 - \{(0, 1, 1, 1, 1)\}$. For $b = (0, 1, 1, 1, 1)$,

$$\begin{aligned} f_0(x) \oplus f_0(x \oplus b) &\equiv 1 \\ f_1(x) \oplus f_1(x \oplus b) &\equiv 0 \end{aligned}$$

□

Example 4 Four Boolean functions in B_6 are constructed that satisfy the PC with respect to all but three nonzero vectors.

Let $p \in \mathrm{PC}_4(4)$ be

$$p(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_3x_4.$$

Let $b_1 = (1, 1, 1, 1, 0, 0)$, $b_2 = (0, 0, 1, 1, 1, 1)$ and $b_3 = (1, 1, 0, 0, 1, 1)$.

The elements ω's in $\{0,1\}^6$ that satisfy $b_1 \cdot \omega = b_2 \cdot \omega = b_3 \cdot \omega = 0$ are

$$0, 3, 12, 15, 21, 22, 25, 26, 37, 38, 41, 42, 48, 51, 60, 63$$

where each of the numbers represents $dec(\omega)$. Thus,

$$\begin{aligned} \left[\hat{F}_{(0,0)}\right] &= [16, 0, 0, 16, 0, 0, 0, 0, 0, 0, 0, 0, 16, 0, 0, -16, 0, 0, 0, 0, 0, 16, 16, 0, 0, 16, -16, 0, 0, 0, 0, 0, \\ &\quad 0, 0, 0, 0, 0, 16, 16, 0, 0, 16, -16, 0, 0, 0, 0, 0, -16, 0, 0, -16, 0, 0, 0, 0, 0, 0, 0, 0, -16, 0, 0, 16] \end{aligned}$$

$x_3x_4x_5$ x_1x_2	000	001	011	010	110	111	101	100
00			**1**			**1**		
01		**1**	**1**	**1**	**1**	**1**	**1**	
11	**1**				**1**	**1**	**1**	
10			**1**		**1**		**1**	**1**

$f_0(x_1, \ldots, x_5)$

$x_3x_4x_5$ x_1x_2	000	001	011	010	110	111	101	100
00			**1**			**1**		
01	**1**							**1**
11		**1**	**1**	**1**				**1**
10			**1**		**1**		**1**	**1**

$f_1(x_1, \ldots, x_5)$

Figure 1: Truth tables of f_0 and f_1.

$$\begin{aligned}\left[\hat{f}_0\right] &= \frac{1}{2^6}\left[\hat{F}_{(0,0)}\right] H_6 \\ &= [1,-1,1,-1,-1,-1,1,1,1,1,-1,-1,-1,1,-1,1,1,1,1,1,1,-1,-1,1,1,-1,-1,1,1,1,1,1, \\ &\quad 1,1,1,1,1,-1,-1,1,1,-1,-1,1,1,1,1,1,-1,1,-1,1,1,1,-1,-1,-1,-1,1,1,1,-1,1,-1]\end{aligned}$$

The algebraic normal form of $f_{(0,0)}$ is

$$f_{(0,0)}(x_1,\ldots,x_6) \;=\; x_1 \oplus x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_1x_5 \oplus x_3x_5 \oplus x_1x_6 \oplus x_3x_6 \oplus x_5x_6$$

$f_{(0,1)}$, $f_{(1,0)}$ and $f_{(1,1)}$ can be generated in the same way as the above.

$$\begin{aligned} f_{(0,1)}(x_1,\ldots,x_6) &= x_1x_3 \oplus x_2x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_1x_5 \oplus x_3x_5 \oplus x_1x_6 \oplus x_3x_6 \oplus x_5x_6. \\ f_{(1,0)}(x_1,\ldots,x_6) &= x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_1x_5 \oplus x_3x_5 \oplus x_1x_6 \oplus x_3x_6 \oplus x_5x_6. \\ f_{(1,1)}(x_1,\ldots,x_6) &= x_1 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_1x_5 \oplus x_3x_5 \oplus x_1x_6 \oplus x_3x_6 \oplus x_5x_6. \end{aligned}$$

$f_{(0,1)}$ $f_{(1,0)}$ and $f_{(1,1)}$ are balanced, while $f_{(0,0)}$ is not balanced. The truth table of $f_{(1,1)}$ is presented in Figure 2. $f_{(0,0)}$, $f_{(0,1)}$, $f_{(1,0)}$, $f_{(1,1)} \in \mathrm{PC}_6(3)$ since they satisfy the PC with respect to $\mathrm{V}_6 - \{b_1, b_2, b_3\}$ and the Hamming weights of b_1, b_2, b_3 are all 4. Table 1 shows the values of $f_{(c_1,c_2)}(x) \oplus f_{(c_1,c_2)}(x \oplus b_i)$ for $(c_1, c_2) \in \{0,1\}^2$ and $i = 1, 2, 3$. □

5 Boolean functions satisfying the PC of degree $n-2$

5.1 Boolean functions with even number of variables

In this section, it is proved that, for every even $n \geqslant 4$, $\mathrm{PC}_n(n-2) = \mathrm{PC}_n(n)$.

Firstly, we present a simple lemma. For $u \in \{0,1\}^{2^n}$ and $\alpha \in \{0,1\}^n$, let $[u]_\alpha$ denote the $dec(\alpha)+1$-th element of u. For $b \in \{0,1\}^n$, let v_b denote the $dec(b)+1$-th column vector of the Hadamard matrix H_n.

Lemma 8 Let $n \geqslant 2$. Let $b_i = (0,\ldots,0,\overset{i}{1},0,\ldots,0)$ for every i such that $1 \leqslant i \leqslant n$ and $b_{n+1} = (1,\ldots,1)$. For $v_{b_1},\ldots,v_{b_{n+1}}$ and $\alpha = (\alpha_1,\ldots,\alpha_n) \in \{0,1\}^n$,

- if $W(\alpha)$ is even, then

$$[v_{b_{n+1}}]_\alpha = 1,$$

$$[v_{b_i}]_\alpha = \begin{cases} 1 & \text{if } \alpha_i = 0 \\ -1 & \text{if } \alpha_i = 1, \end{cases}$$

- if $W(\alpha)$ is odd, then

$$[v_{b_{n+1}}]_\alpha = -1,$$

$$[v_{b_i}]_\alpha = \begin{cases} 1 & \text{if } \alpha_i = 1 \\ -1 & \text{if } \alpha_i = 0, \end{cases}$$

Table 1: The value of $f_{(c_1,c_2)}(x) \oplus f_{(c_1,c_2)}(x \oplus b_i)$.

	b_1	b_2	b_3
$f_{(0,0)}$	0	0	0
$f_{(0,1)}$	0	1	1
$f_{(1,0)}$	1	0	1
$f_{(1,1)}$	1	1	0

$x_4x_5x_6$ $x_1x_2x_3$	000	001	011	010	110	111	101	100
000			**1**			**1**		
001		**1**	**1**	**1**	**1**	**1**	**1**	
011	**1**				**1**	**1**	**1**	
010			**1**		**1**		**1**	**1**
110	**1**							**1**
111	**1**	**1**		**1**	**1**		**1**	**1**
101			**1**		**1**		**1**	**1**
100	**1**				**1**	**1**	**1**	

Figure 2: Truth table of $f_{(1,1)}$.

(Proof) This lemma can be proved from the fact that,

$$[v_{b_{n+1}}]_\alpha = (-1)^{\alpha_1 \oplus \cdots \oplus \alpha_n},$$

and, for each i such that $1 \leqslant i \leqslant n$,

$$[v_{b_i}]_\alpha = (-1)^{\alpha_1 \oplus \cdots \oplus \alpha_{i-1} \oplus \alpha_{i+1} \oplus \cdots \oplus \alpha_n}.$$

□

Theorem 8 For every even $n \geqslant 4$, $\mathrm{PC}_n(n-2) = \mathrm{PC}_n(n)$.

(Proof) Suppose that $f \in \mathrm{PC}_n(n-2)$. Then, $C_f(a) = 0$ for any $a \in \{0,1\}^n$ such that $1 \leqslant W(a) \leqslant n-2$. Thus, $\left[\hat{F}^2\right]$ is able to be represented as

$$\left[\hat{F}^2\right] = C_f(0){v_0}^{\mathrm{T}} + C_f(b_1){v_{b_1}}^{\mathrm{T}} + \cdots + C_f(b_n){v_{b_n}}^{\mathrm{T}} + C_f(b_{n+1}){v_{b_{n+1}}}^{\mathrm{T}}.$$

Let

$$\begin{aligned} u_0 &= {v_0}^{\mathrm{T}}, \\ u_i &= ({v_0}^{\mathrm{T}} + {v_{b_i}}^{\mathrm{T}})/2, \end{aligned}$$

for every $1 \leqslant i \leqslant n+1$. Then, $\left[\hat{F}^2\right]$ can be represented as

$$\left[\hat{F}^2\right] = c_0 u_0 + c_1 u_1 + \cdots + c_{n+1} u_{n+1},$$

where

$$\begin{aligned} c_0 &= C_f(0) - (C_f(b_1) + \cdots + C_f(b_{n+1})), \\ c_i &= 2C_f(b_i). \end{aligned}$$

From Lemma 8, for any odd s such that $1 \leqslant s \leqslant n$ and $i_1, \ldots, i_s$ such that $0 \leqslant i_1 < \cdots < i_s \leqslant n-1$,

$$\left[\hat{F}^2(\sum_{k=1}^{s} 2^{i_k})\right] = c_0 + \sum_{k=1}^{s} c_{i_k+1},$$

and, for any even t such that $1 \leqslant t \leqslant n$ and $j_1, \ldots, j_t$ such that $0 \leqslant j_1 < \cdots < j_t \leqslant n-1$,

$$\left[\hat{F}^2(\sum_{k=1}^{t} 2^{j_k})\right] = c_0 + c_1 + \cdots + c_{n+1} - \sum_{k=1}^{t} c_{j_k+1}.$$

Thus, for every pair of odd integers s and t such that $1 \leqslant s, t \leqslant n$ and $s+t \leqslant n$ and $i_1, \ldots, i_s$ and $j_1, \ldots, j_t$ such that $\{i_1, \ldots, i_s\} \cap \{j_1, \ldots, j_t\} = \emptyset$ and $0 \leqslant i_1 < \cdots < i_s \leqslant n-1$ and $0 \leqslant j_1 < \cdots < j_t \leqslant n-1$,

$$\begin{aligned} &\hat{F}^2(0) + \hat{F}^2(\sum_{k=1}^{s} 2^{i_k}) + \hat{F}^2(\sum_{l=1}^{t} 2^{j_l}) + \hat{F}^2(\sum_{k=1}^{s} 2^{i_k} + \sum_{l=1}^{t} 2^{j_l}) \\ &= 4c_0 + 2(c_1 + \cdots + c_{n+1}) \\ &= 2^{n+2}. \end{aligned}$$

Since $n+2$ is even, from Lemma 1, 5, 6, all of $\hat{F}^2(0)$, $\hat{F}^2(\sum_{k=1}^{s} 2^{i_k})$, $\hat{F}^2(\sum_{l=1}^{t} 2^{j_l})$, $\hat{F}^2(\sum_{k=1}^{s} 2^{i_k} + \sum_{l=1}^{t} 2^{j_l})$ are equal to 2^n, or only one of them is equal to 2^{n+2} and the others are equal to 0.

In the former case, f is perfectly nonlinear.

In the latter case, if $\hat{F}^2(0) = 2^{n+2}$, then $\hat{F}(\omega) = 0$ for every $\omega \neq 0$, which contradicts that $\sum_{\omega \in \{0,1\}^n} \hat{F}^2(\omega) = 2^{2n}$.

If $\hat{F}^2(0) = c_0 + c_1 + \cdots + c_{n+1} = 0$, then $c_0 = 2^{n+1}$. For this case,

$$\begin{aligned}
&\hat{F}^2(1,0,\ldots,0) + \hat{F}^2(0,1,0,\ldots,0) + \hat{F}^2(1,1,0,\ldots,0)\\
&= (c_0 + c_1) + (c_0 + c_2) + (c_0 + c_3 + \cdots + c_{n+1})\\
&= 2c_0 + (c_0 + c_1 + \cdots + c_{n+1})\\
&= 2^{n+2}.
\end{aligned}$$

From Lemma 1, 5, and $c_0 = 2^{n+1}$, there are following three cases:

(Case 1) $c_1 = 2^{n+1}$, $c_2 = -2^{n+1}$, $c_0 + c_3 + \cdots + c_{n+1} = 0$,

(Case 2) $c_1 = -2^{n+1}$, $c_2 = 2^{n+1}$, $c_0 + c_3 + \cdots + c_{n+1} = 0$,

(Case 3) $c_1 = -2^{n+1}$, $c_2 = -2^{n+1}$, $c_0 + c_3 + \cdots + c_{n+1} = 2^{n+2}$.

For Case 1. Since

$$\begin{aligned}
&\hat{F}^2(0,0,1,0,\ldots,0) + \hat{F}^2(0,0,0,1,0,\ldots,0) + \hat{F}^2(1,1,1,1,0,\ldots,0)\\
&= (c_0 + c_3) + (c_0 + c_4) + (c_0 + c_5 + \cdots + c_{n+1})\\
&= 2c_0 + (c_0 + c_3 + \cdots + c_{n+1})\\
&= 2^{n+2},
\end{aligned}$$

the same argument as the above one shows that

(Case 1.1) $c_3 = 2^{n+1}$, $c_4 = -2^{n+1}$, $c_0 + c_5 + \cdots + c_{n+1} = 0$.

(Case 1.2) $c_3 = -2^{n+1}$, $c_4 = 2^{n+1}$, $c_0 + c_5 + \cdots + c_{n+1} = 0$.

(Case 1.3) $c_3 = -2^{n+1}$, $c_4 = -2^{n+1}$, $c_0 + c_5 + \cdots + c_{n+1} = 2^{n+2}$.

For Case 1.1, 1.2 and 1.3, the following three equations can be derived, respectively,

$$\hat{F}^2(1,0,1,0,0,\ldots,0) = c_0 + c_1 + \cdots + c_{n+1} - (c_1 + c_3) = -2^{n+2},$$

$$\hat{F}^2(1,0,0,1,0,\ldots,0) = c_0 + c_1 + \cdots + c_{n+1} - (c_1 + c_4) = -2^{n+2},$$

$$\hat{F}^2(0,1,1,1,0,\ldots,0) = c_0 + c_2 + c_3 + c_4 = -2^{n+2},$$

which are contradictions.

For Case 2. This case can be proved in the same way as Case 1.

For Case 3. Since $c_0 + c_3 + \cdots + c_{n+1} = 2^{n+2}$,

$$\begin{aligned}
&\hat{F}^2(0,0,1,0,\ldots,0) + \hat{F}^2(0,0,0,1,0,\ldots,0) + \hat{F}^2(1,1,1,1,0,\ldots,0)\\
&= (c_0 + c_3) + (c_0 + c_4) + (c_0 + c_5 + \cdots + c_{n+1})\\
&= 2c_0 + (c_0 + c_3 + \cdots + c_{n+1})\\
&= 2^{n+3}.
\end{aligned}$$

From Lemma 1, 5, there are following three cases:

(Case 3.1) $c_3 = 2^{n+1}$, $c_4 = -2^{n+1}$, $c_0 + c_5 + \cdots + c_{n+1} = 2^{n+2}$,

(Case 3.2) $c_3 = -2^{n+1}$, $c_4 = 2^{n+1}$, $c_0 + c_5 + \cdots + c_{n+1} = 2^{n+2}$,

(Case 3.3) $c_3 = 2^{n+1}$, $c_4 = 2^{n+1}$, $c_0 + c_5 + \cdots + c_{n+1} = 0$.

Table 2: Bounds of the degree of the PC of balanced Boolean functions

number of variables	4	6	8	10	12	14	16	18	20	22	24	26
upper bound	1	3	5	7	9	11	13	15	17	19	21	23
lower bound	1	3	4	5	7	8	9	11	12	13	15	16

For Case 3.1, 3.2 and 3.3, the following three equations can be derived, respectively,

$$\hat{F}^2(1,1,0,1,0,\ldots,0) = c_0 + c_1 + c_2 + c_4 = -2^{n+2},$$

$$\hat{F}^2(1,1,1,0,0,\ldots,0) = c_0 + c_1 + c_2 + c_3 = -2^{n+2},$$

$$\hat{F}^2(0,0,1,1,0,\ldots,0) = c_0 + c_1 + \cdots + c_{n+1} - (c_3 + c_4) = -2^{n+2},$$

which are contradictions. Hence, the theorem has been proved. □

Since perfectly nonlinear Boolean functions are not balanced, the following corollary can be derived. It presents an upper bound of the degree of the PC of a balanced Boolean functions with the even number of inputs.

Corollary 12 For every even $n \geqslant 4$, the degree of the PC of balanced Boolean functions is less than $n-2$. □

As for the lower bound, the following has been proved.

Proposition 8 [SZZ93] Let $n \geqslant 4$ be even. Suppose that $n = 3t + c$, where $c = 0, 1$, or 2. Then there exist balanced Boolean functions in B_n that satisfy the PC of degree $2t-1$ when $c = 0, 1$ or $2t$ when $c = 2$. □

Table 2 shows the bounds of the degree of the PC of balanced Boolean functions. The bounds are tight for $n = 4, 6$.

5.2 Boolean functions with odd number of variables

In this section, it is shown that, for every odd $n \geqslant 3$, every $f \in \mathrm{PC}_n(n-2)$ satisfies the PC with respect to all but one elements in V_n.

Lemma 9 Let $x, y, z \geqslant 0$ be integers and $m \geqslant 0$ be an even integer. $x^2 + y^2 + z^2 = 3 \cdot 2^m$ if and only if $x = y = z = 2^{m/2}$.

(Proof) x, y, z can be represented as

$$x = 2^{e_1} q_1,\ y = 2^{e_2} q_2,\ z = 2^{e_3} q_3,$$

where $e_1, e_2, e_3 \geqslant 0$, and each of q_1, q_2, q_3 is 0 or odd. We may assume that $x \geqslant y \geqslant z \geqslant 0$.

(i) If we assume that $y = z = 0$, then $x^2 = 3 \cdot 2^m$, which contradicts that x is an integer.

(ii) Suppose that $x \neq 0$, $y \neq 0$, $z = 0$. Then, $2^{2e_1} {q_1}^2 + 2^{2e_2} {q_2}^2 = 3 \cdot 2^m$. Since, without loss of generality, we can assume that $e_2 \geqslant e_1 \geqslant 0$,

$${q_1}^2 + 2^{2(e_2 - e_1)} {q_2}^2 = 3 \cdot 2^{m - 2e_1}.$$

If $e_1 = e_2$, then ${q_1}^2 + {q_2}^2$ is a multiple of 2 but not of 4. This implies that $m - 2e_1 = 1$, which contradicts that m is even.

If $e_1 < e_2$, then the left-hand side is odd and $m - 2e_1 = 0$. Thus, ${q_1}^2 + 2^{2(e_2-e_1)} {q_2}^2 = 3$, which implies that $2(e_2 - e_1) = 1$. This contradicts that e_1 and e_2 are integers.

(iii) Suppose that none of x, y, z is 0. Without loss of generality, we may assume that $0 \leqslant e_1 \leqslant e_2 \leqslant e_3$.

$$\begin{aligned} 2^{2e_1}{q_1}^2 + 2^{2e_2}{q_2}^2 + 2^{2e_3}{q_3}^2 &= 3 \cdot 2^m \\ {q_1}^2 + 2^{2(e_2-e_1)}{q_2}^2 + 2^{2(e_3-e_1)}{q_3}^2 &= 3 \cdot 2^{m-2e_1}. \end{aligned}$$

If we assume that $e_1 \neq e_2$ and $e_1 \neq e_3$, or $e_1 = e_2 = e_3$, then the left-hand side is odd. This implies that $m - 2e_1 = 0$ and

$$ {q_1}^2 + 2^{2(e_2-e_1)}{q_2}^2 + 2^{2(e_3-e_1)}{q_3}^2 = 3. $$

Since $q_1, q_2, q_3 \geqslant 1$, $e_1 = e_2 = e_3 = m/2$ and $q_1 = q_2 = q_3 = 1$.
If we assume that $e_1 = e_2$ and $e_1 \neq e_3$, then ${q_1}^2 + {q_2}^2 = 3 \cdot 2^{m-2e_1} - 2^{2(e_3-e_1)}{q_3}^2$. Since ${q_1}^2 + {q_2}^2$ is a multiple of 2 but not of 4, $m - 2e_1 = 1$ or $2(e_3 - e_1) = 1$. This situation cannot occur because m is even.

Hence, the lemma has been proved. □

Theorem 9 For every odd $n \geqslant 3$, if $f \in \mathrm{PC}_n(n-2)$, then, for some $b \in \{0,1\}^n$ such that $W(b) \geqslant n-1$, f satisfies the PC with respect to $\mathrm{V}_n - \{b\}$.

(Proof) Suppose that $f \in \mathrm{PC}_n(n-2)$. Then, $C_f(a) = 0$ for every $a \in \{0,1\}^n$ whose Hamming weight is at least $n-1$. $\left[\hat{F}^2\right]$ is able to be represented as

$$ \left[\hat{F}^2\right] = c_0 u_0 + c_1 u_1 + \cdots + c_{n+1} u_{n+1}, $$

where for every $1 \leqslant i \leqslant n+1$,

$$\begin{aligned} u_0 &= {v_0}^{\mathrm{T}}, \\ u_i &= ({v_0}^{\mathrm{T}} + {v_{b_i}}^{\mathrm{T}})/2, \\ c_0 &= C_f(0) - (C_f(b_1) + \cdots + C_f(b_{n+1})), \\ c_i &= 2C_f(b_i). \end{aligned}$$

Hence, from Lemma 8, for every i, j such that $0 \leqslant i, j \leqslant n-1$ and $i \neq j$,

$$ \hat{F}^2(2^i) = c_0 + c_{i+1}, $$

$$ \hat{F}^2(2^i + 2^j) = c_0 + c_1 + \cdots + c_{n+1} - (c_{i+1} + c_{j+1}). $$

Thus, for every i, j such that $0 \leqslant i, j \leqslant n-1$ and $i \neq j$,

$$\begin{aligned} &\hat{F}^2(0) + \hat{F}^2(2^i) + \hat{F}^2(2^j) + \hat{F}^2(2^i + 2^j) \\ &= 4c_0 + 2(c_1 + \cdots + c_{n+1}) \\ &= 2^{n+2} \end{aligned}$$

Since $n+2$ is odd, from Lemma 1, 5, 6, two of $\hat{F}^2(0)$, $\hat{F}^2(2^i)$, $\hat{F}^2(2^j)$ and $\hat{F}^2(2^i + 2^j)$ are equal to 0, and two of them are equal to 2^{n+1}.

If $\hat{F}^2(0) = c_0 + c_1 + \cdots + c_{n+1} = 0$, then $c_0 = 2^{n+1}$. For every i, j such that $0 \leqslant i, j \leqslant n-1$ and $i \neq j$, since

$$\begin{aligned} &\hat{F}^2(2^i) + \hat{F}^2(2^j) + \hat{F}^2(2^i + 2^j) \\ &= 2c_0 + (c_0 + c_1 + \cdots + c_{n+1}) \\ &= 2^{n+2}, \end{aligned}$$

each of $\hat{F}^2(2^i)$, $\hat{F}^2(2^j)$ and $\hat{F}^2(2^i + 2^j)$ is equal to 0 or 2^{n+1}. Thus, each of $c_1, \ldots, c_n$ is equal to 0 or -2^{n+1}. Since, for every i, j such that $0 \leqslant i, j \leqslant n-1$ and $i \neq j$,

$$ \hat{F}^2(2^i + 2^j) = -(c_{i+1} + c_{j+1}) $$

is equal to 0 or 2^{n+1}, at most only one of $c_1, \ldots, c_n$ is equal to -2^{n+1}, and the others are equal to 0. If one of $c_1, \ldots, c_n$ is equal to -2^{n+1}, then $c_{n+1} = 0$, otherwise, $c_{n+1} = -2^{n+1}$, because $c_0 = 2^{n+1}$ and $c_0 + c_1 + \cdots + c_{n+1} = 0$. Hence, one of $c_1, \ldots, c_{n+1}$ is equal to -2^{n+1} and the others are equal to 0.

If $\hat{F}^2(0) = c_0 + c_1 + \cdots + c_{n+1} = 2^{n+1}$, then $c_0 = 0$. Thus, for every i such that $0 \leqslant i \leqslant n-1$, $\hat{F}^2(2^i) = c_{i+1}$, and c_{i+1} is equal to 0 or 2^{n+1}. Since, for every i, j such that $0 \leqslant i, j \leqslant n-1$ and $i \neq j$,

$$\hat{F}^2(2^i + 2^j) = 2^{n+1} - (c_{i+1} + c_{j+1}),$$

at most one of $c_1, \ldots, c_n$ is 2^{n+1}. If one of $c_1, \ldots, c_n$ is equal to 2^{n+1}, then $c_{n+1} = 0$, otherwise, $c_{n+1} = 2^{n+1}$, because $c_0 = 0$ and $c_0 + c_1 + \cdots + c_{n+1} = 2^{n+1}$.

From the above discussion, there exist some i such that $1 \geqslant i \geqslant n+1$ and $C_f(a) = 0$ for every $a \in \mathrm{V}_n - \{b_i\}$. Hence, f satisfies the PC with respect to all but one elements in V_n. □

The following corollaries can be derived from the above two theorems.

Corollary 13 For every odd $n \geqslant 3$,

$$|\mathrm{PC}_n(n-2)| = 2(n+1)|\mathrm{PC}_{n-1}(n-1)|,$$

and the number of balanced Boolean functions in $\mathrm{PC}_n(n-2)$ is $(n+1)|\mathrm{PC}_{n-1}(n-1)|$.

(Proof) There exist $n+1$ elements in V_n whose Hamming weight is at least $n-1$. For each $b \in \mathrm{V}_n$, there exist $2|\mathrm{PC}_{n-1}(n-1)|$ Boolean functions that satisfy the PC with respect to $\mathrm{V}_n - \{b\}$, and half of them are balanced. □

Corollary 14 For every odd $n \geqslant 3$, the nonlinearities of Boolean functions in $\mathrm{PC}_n(n-2)$ is $2^{n-1} - 2^{(n-1)/2}$. □

6 Relationships Between the PC and the SAC

This section presents some relationships between $\mathrm{PC}_n(k)$ and $\mathrm{SAC}_n(m)$.

Rothaus[Rot76] presented a few methods for constructing Boolean bent functions. One of them gives Boolean bent functions of the form

$$f(x_1, \ldots, x_n) = \bigoplus_{i=1}^{m} x_i x_{m+i} \oplus g(x_1, \ldots, x_m),$$

where $n = 2m$ and g is an arbitrary m-input Boolean function.

It is apparent, from definitions of the SAC and the PC, that Boolean functions satisfying the PC of degree at least one also satisfy the SAC of order zero. We show the relationships between $\mathrm{SAC}_n(1)$ and $\mathrm{PC}_n(k)$.

The following theorem shows that perfectly nonlinear Boolean functions do not necessarily satisfy the SAC of order 1.

Theorem 10 For every even $n \geqslant 2$, $\mathrm{PC}_n(n) \not\subseteq \mathrm{SAC}_n(1)$.

(Proof) Let $n = 2m$ and

$$f(x_1, \ldots, x_n) = \bigoplus_{i=1}^{m} x_i x_{m+i}.$$

Then $f \in \mathrm{PC}_n(n)$, and

$$f|_{x_n=1}(x_1, \ldots, x_{n-1}) = \bigoplus_{i=1}^{m-1} x_i x_{m+i} \oplus x_m.$$

Thus,

$$f|_{x_n=1}(x_1,\ldots,x_{n-1}) \oplus f|_{x_n=1}(x_1,\ldots,x_{m-1},x_m \oplus 1, x_{m+1},\ldots,x_{n-1}) \equiv 1,$$

This implies that $f \notin \mathrm{SAC}_n(1)$. □

The following theorem shows that, for every odd $n \geqslant 3$, all the Boolean functions with n inputs satisfying the PC of degree $n-1$ satisfy the SAC of order 1, while those satisfying the PC of degree $n-2$ necessarily not. We prove the theorem by using the following lemma.

Lemma 10 [For90] For any $f \in \mathrm{B}_n$, $f \in \mathrm{SAC}_n(1)$ if and only if, $f \in \mathrm{SAC}_n(0)$ and

$$\sum_{\omega\in\{0,1\}^n} \hat{F}(\omega)\hat{F}(\omega \oplus a)(-1)^{\omega_i} = 0$$

for every $a \in \{0,1\}^n$ whose Hamming weight is 1 and every i such that the i-th bit of a is 0, □

Theorem 11 For every odd $n \geqslant 3$,

1. $\mathrm{PC}_n(n-1) \subseteq \mathrm{SAC}_n(1)$,
2. $\mathrm{PC}_n(n-2) \not\subseteq \mathrm{SAC}_n(1)$.

(Proof) 1. Suppose that $f \in \mathrm{PC}_n(n-1)$. It is clear from the definition that $f \in \mathrm{SAC}_n(0)$. If n is odd, then $\hat{F}(\omega) = 0$ either for every $\omega \in \{0,1\}^n$ whose Hamming weight is even or for every $\omega \in \{0,1\}^n$ whose Hamming weight is odd. For any $a \in \{0,1\}^n$ whose Hamming weight is 1, $\hat{F}(\omega) = 0$ or $\hat{F}(\omega \oplus a) = 0$, because the Hamming weight of either ω or $\omega \oplus a$ is odd. Thus,

$$\sum_{\omega\in\{0,1\}^n} \hat{F}(\omega)\hat{F}(\omega \oplus a)(-1)^{\omega_i} = 0,$$

which implies that $f \in \mathrm{SAC}_n(1)$.

2. Let $m = (n-1)/2$ and $p \in \mathrm{B}_{2m}$ such that

$$p(x_1,\ldots,x_{2m}) = x_1x_{2m} \oplus x_2x_{2m-1} \oplus \cdots \oplus x_mx_{m+1}.$$

For $b = (0,1,\ldots,1) \in \{0,1\}^n$ and $\alpha_1,\ldots,\alpha_{2^{n-1}} \in \{0,1\}^n$ such that $0 \leqslant dec(\alpha_1) < \cdots < dec(\alpha_{2^{n-1}}) \leqslant 2^n - 1$ and $b \cdot \alpha_i = 1$ for $1 \leqslant i \leqslant 2^{n-1}$,

$$\hat{F}(\omega) = \begin{cases} 2^{(n+1)/2}\hat{p}(i-1) & \text{if } \omega = \alpha_i \\ 0 & \text{othewise.} \end{cases}$$

Let $\hat{f} = \mathcal{W}^{-1}(\hat{F})$. Then, $f \in \mathrm{PC}_n(n-2)$, because $f \in \mathrm{B}_n$ and f satisfies the PC with respect to $\mathrm{V}_n - \{b\}$ from Theorem 4.

Since

$$p(0,x_2,\ldots,x_{2m}) \oplus p(1,x_2,\ldots,x_{2m}) = x_m$$

and

$$b \cdot (0,\omega_2,\ldots,\omega_n) = b \cdot (1,\omega_2,\ldots,\omega_n),$$

for $a = (1,0,\ldots,0) \in \{0,1\}^n$,

$$\begin{aligned} \hat{F}(\alpha_{2j-1})\hat{F}(\alpha_{2j} \oplus a) &= \hat{F}(\alpha_{2j-1})\hat{F}(\alpha_{2j}) \\ &= \begin{cases} 2^{n+1} & j = 1,\ldots,2^{n-3} \\ -2^{n+1} & j = 2^{n-3}+1,\ldots,2^{n-2}. \end{cases} \end{aligned}$$

The n-th bit of α_i is equal to 0 for $i = 1,\ldots,2^{n-2}$ and equal to 1 for $i = 2^{n-2}+1,\ldots,2^{n-1}$. Thus,

$$\begin{aligned} \sum_{\omega\in\{0,1\}^n} \hat{F}(\omega)\hat{F}(\omega \oplus a)(-1)^{\omega_n} &= 2^{n+1}2^{n-2} + (-2^{n+1})(-1)2^{n-2} \\ &= 2^{2n}. \end{aligned}$$

This implies that $f \notin \mathrm{SAC}_n(1)$. □

Table 3: $\hat{F}$ of Example 5

$(\omega_1, \omega_2, \omega_3, \omega_4, \omega_5)$	$\hat{F}$	$(\omega_1, \omega_2, \omega_3, \omega_4, \omega_5)$	$\hat{F}$
$(0,0,0,0,0)$	8	$(0,0,0,0,1)$	0
$(1,0,0,0,0)$	8	$(1,0,0,0,1)$	0
$(0,1,0,0,0)$	0	$(0,1,0,0,1)$	8
$(1,1,0,0,0)$	0	$(1,1,0,0,1)$	-8
$(0,0,1,0,0)$	0	$(0,0,1,0,1)$	8
$(1,0,1,0,0)$	0	$(1,0,1,0,1)$	-8
$(0,1,1,0,0)$	8	$(0,1,1,0,1)$	0
$(1,1,1,0,0)$	8	$(1,1,1,0,1)$	0
$(0,0,0,1,0)$	0	$(0,0,0,1,1)$	8
$(1,0,0,1,0)$	0	$(1,0,0,1,1)$	-8
$(0,1,0,1,0)$	8	$(0,1,0,1,1)$	0
$(1,1,0,1,0)$	8	$(1,1,0,1,1)$	0
$(0,0,1,1,0)$	-8	$(0,0,1,1,1)$	0
$(1,0,1,1,0)$	-8	$(1,0,1,1,1)$	0
$(0,1,1,1,0)$	0	$(0,1,1,1,1)$	-8
$(1,1,1,1,0)$	0	$(1,1,1,1,1)$	8

Example 5 We present an example of Boolean functions in B_n that satisfy the PC of degree $n-2$ and that do not satisfy the SAC of order 1.

Let $n = 5$. Let $p \in \mathrm{PC}_4(4)$ such that

$$p(x_1, x_2, x_3, x_4) = x_1 x_4 \oplus x_2 x_3,$$

and $b = (0,1,1,1,1)$. Let $\hat{F}(\omega_1, \ldots, \omega_5$ be defined as in the proof of Theorem 11. Table 3 shows the $\hat{F}(\omega_1, \ldots, \omega_5)$.

$$f(x_1, \ldots, x_5) = x_2 \oplus x_1 x_2 \oplus x_2 x_3 \oplus x_2 x_4 \oplus x_3 x_4 \oplus x_1 x_5.$$

$f \in \mathrm{PC}_5(3)$ because f satisfies the PC with respect to $\mathrm{V}_5 - \{(0,1,1,1,1)\}$. Let

$$\begin{aligned} f(1, x_2, x_3, x_4, x_5) &= x_2 x_3 \oplus x_2 x_4 \oplus x_3 x_4 \oplus x_5 \\ &\overset{\text{def}}{=} g(x_2, x_3, x_4, x_5). \end{aligned}$$

Then,

$$g(x_2, x_3, x_4, x_5) \oplus g(x_2, x_3, x_4, x_5 \oplus 1) \equiv 1,$$

and g does not satisfy the SAC. Thus, $f \notin \mathrm{SAC}_5(1)$. □

The following theorem shows that, for every odd $n \geqslant 3$, Boolean functions with n inputs satisfying the PC of degree $n-2$ do not necessarily satisfy the SAC of order 2. The proof of this theorem uses the following lemma.

Lemma 11 [For90] For any $f \in \mathrm{B}_n$, $f \in \mathrm{SAC}_n(2)$ if and only if $f \in \mathrm{SAC}_n(1)$ and

$$\sum_{\omega \in \{0,1\}^n} \hat{F}(\omega) \hat{F}(\omega \oplus a)(-1)^{\omega_i} = 0$$

for every $a \in \{0,1\}^n$ whose Hamming weight is 2 and every i such that the i-th bit of a is 0, □

Theorem 12 For every odd $n \geqslant 3$, $\mathrm{PC}_n(n-1) \not\subseteq \mathrm{SAC}_n(2)$.

(Proof) If $n = 3$, then $\mathrm{SAC}_3(2) = \phi$.

For $n \geqslant 5$, let $m = (n-1)/2$ and $p \in \mathrm{B}_{2m}$ such that

$$p(x_1, \dots, x_{2m}) = x_1 x_{2m} \oplus x_2 x_{2m-1} \oplus \cdots \oplus x_m x_{m+1}.$$

For $\alpha_1, \dots, \alpha_{2^{n-1}} \in \{0,1\}^n$ such that $0 \leqslant dec(\alpha_1) < \cdots < dec(\alpha_{2^{n-1}}) \leqslant 2^n - 1$ and the Hamming weights of them are odd,

$$\hat{F}(\omega) = \begin{cases} 2^{(n+1)/2}\hat{p}(i-1) & \text{if } \omega = \alpha_i \\ 0 & \text{othewise.} \end{cases}$$

Let $\hat{f} = \mathcal{W}^{-1}(\hat{F})$. Then, $f \in \mathrm{PC}_n(n-1)$, because $f \in \mathrm{B}_n$ and f satisfies the PC with respect to $\mathrm{V}_n - \{(1, \dots, 1)\}$ from Theorem 4.

Since

$$p(0, x_2, \dots, x_{2m}) \oplus p(1, x_2, \dots, x_{2m}) = x_m$$

and

$$\begin{aligned} W((0,0,\omega_3,\dots,\omega_n)) &= W((1,1,\omega_2,\dots,\omega_n)), \\ W((0,1,\omega_3,\dots,\omega_n)) &= W((1,0,\omega_2,\dots,\omega_n)), \end{aligned}$$

for $a = (1, 1, \dots, 0) \in \{0,1\}^n$,

$$\begin{aligned} \hat{F}(\alpha_{2j-1})\hat{F}(\alpha_{2j} \oplus a) &= \hat{F}(\alpha_{2j-1})\hat{F}(\alpha_{2j}) \\ &= \begin{cases} 2^{n+1} & j = 1, \dots, 2^{n-3} \\ -2^{n+1} & j = 2^{n-3}+1, \dots, 2^{n-2}. \end{cases} \end{aligned}$$

The n-th bit of α_i is equal to 0 for $i = 1, \dots, 2^{n-2}$ and equal to 1 for $i = 2^{n-2}+1, \dots, 2^{n-1}$. Thus,

$$\begin{aligned} \sum_{\omega \in \{0,1\}^n} \hat{F}(\omega)\hat{F}(\omega \oplus a)(-1)^{\omega_n} &= 2^{n+1}2^{n-2} + (-2^{n+1})(-1)2^{n-2} \\ &= 2^{2n}. \end{aligned}$$

This implies that $f \notin \mathrm{SAC}_n(2)$. □

Example 6 We give an example of Boolean functions in B_n that satisfy the PC of degree $n-1$ and that do not satisfy the SAC of order 2.

Let $n = 5$. Let $p \in \mathrm{PC}_4(4)$ such that

$$p(x_1, x_2, x_3, x_4) = x_1 x_4 \oplus x_2 x_3.$$

Let $\hat{F}(\omega_1, \dots, \omega_5$ be defined as in the proof of Theorem 12. Table 4 shows the $\hat{F}(\omega_1, \dots, \omega_5)$.

$$f(x_1, \dots, x_5) = x_1 \oplus x_1 x_2 \oplus x_1 x_3 \oplus x_1 x_4 \oplus x_3 x_4 \oplus x_1 x_5 \oplus x_2 x_5$$

$f \in \mathrm{PC}_5(4)$ because f satisfies the PC with respect to $\mathrm{V}_5 - \{(1,1,1,1,1)\}$. Let

$$\begin{aligned} f(0, 1, x_3, x_4, x_5) &= x_3 x_4 \oplus x_5 \\ &\overset{\text{def}}{=} g(x_3, x_4, x_5). \end{aligned}$$

Then,

$$g(x_3, x_4, x_5) \oplus g(x_3, x_4, x_5 \oplus 1) \equiv 1,$$

and g does not satisfy the SAC. Thus, $f \notin \mathrm{SAC}_5(2)$. □

Table 4: $\hat{F}$ of Example 6

$(\omega_1, \omega_2, \omega_3, \omega_4, \omega_5)$	$\hat{F}$	$(\omega_1, \omega_2, \omega_3, \omega_4, \omega_5)$	$\hat{F}$
$(0,0,0,0,0)$	0	$(0,0,0,0,1)$	8
$(1,0,0,0,0)$	8	$(1,0,0,0,1)$	0
$(0,1,0,0,0)$	8	$(0,1,0,0,1)$	0
$(1,1,0,0,0)$	0	$(1,1,0,0,1)$	-8
$(0,0,1,0,0)$	8	$(0,0,1,0,1)$	0
$(1,0,1,0,0)$	0	$(1,0,1,0,1)$	8
$(0,1,1,0,0)$	0	$(0,1,1,0,1)$	-8
$(1,1,1,0,0)$	8	$(1,1,1,0,1)$	0
$(0,0,0,1,0)$	8	$(0,0,0,1,1)$	0
$(1,0,0,1,0)$	0	$(1,0,0,1,1)$	8
$(0,1,0,1,0)$	0	$(0,1,0,1,1)$	-8
$(1,1,0,1,0)$	8	$(1,1,0,1,1)$	0
$(0,0,1,1,0)$	0	$(0,0,1,1,1)$	-8
$(1,0,1,1,0)$	-8	$(1,0,1,1,1)$	0
$(0,1,1,1,0)$	-8	$(0,1,1,1,1)$	0
$(1,1,1,1,0)$	0	$(1,1,1,1,1)$	8

Lemma 12 [PLLGV91] Let $n \geqslant 3$ and $f \in \mathrm{B}_n$. Suppose that the nonlinear order of f is 2. f satisfies the SAC of order m such that $0 \leqslant m \leqslant n-2$ if and only if every variable x_i occurs in at least second order terms of the algebraic normal form of f. □

From Lemma 12,

$$\mathrm{SAC}_n(n-2) = \{f \in \mathrm{B}_n \mid f(x) = h(x) \oplus \bigoplus_{1 \leqslant i < j \leqslant n} x_i x_j, h \in \mathrm{A}_n\}.$$

Thus, $\mathrm{SAC}_n(n-2) \subset \mathrm{PC}_n(n)$ for every even $n \geqslant 2$ [AT90], and $\mathrm{SAC}_n(n-2) \subset \mathrm{PC}_n(n-1)$ for every odd $n \geqslant 3$.

It is obvious that $\mathrm{SAC}_n(n-3) \subsetneq \mathrm{SAC}_n(0) = \mathrm{PC}_n(1)$. It is implicitly described in [PLLGV91] that $\mathrm{SAC}_n(n-2) \subsetneq \mathrm{PC}_n(n-1)$. For $\mathrm{SAC}_n(n-3)$ and $\mathrm{PC}_n(2)$, the following theorem holds.

Theorem 13 $\mathrm{SAC}_n(n-3) \not\subseteq \mathrm{PC}_n(2)$ for every $n \geqslant 3$.

(Proof) Let

$$g(x_1, \ldots, x_n) = \bigoplus_{1 \leqslant i < j \leqslant n, i \leqslant n-2} x_i x_j.$$

It is sufficient to show that $g \notin \mathrm{PC}_n(2)$ because $g \in \mathrm{SAC}_n(n-3)$ from Lemma 12. Since

$$g(x_1, \ldots, x_n) = q_{n-2}(x_1, \ldots, x_{n-2}) \oplus \bigoplus_{1 \leqslant i \leqslant n-2} x_i(x_{n-1} \oplus x_n),$$

for $a = (0, \ldots, 0, 1, 1)$,

$$g(x_1, \ldots, x_n) \oplus g(x_1 \oplus a_1, \ldots, x_n \oplus a_n) \equiv 0.$$

Hence, $g \notin \mathrm{PC}_n(2)$. □

Figure 3 and 4 show the relationships between the PC and the SAC. In the two figures, if a directed path exists from the set A to the set B, then the set A contains the set B.

$$\begin{tikzcd}
\mathbf{PC_n\,(1)} \arrow[r, leftrightarrow] \arrow[d] & \mathbf{SAC_n\,(0)} \arrow[d] \\
\mathbf{PC_n\,(2)} \arrow[d] & \mathbf{SAC_n\,(1)} \arrow[d] \\
\vdots \arrow[d] & \vdots \arrow[d] \\
\mathbf{PC_n\,(n\text{-}3)} \arrow[d] & \mathbf{SAC_n\,(n\text{-}4)} \arrow[d] \\
\mathbf{PC_n\,(n\text{-}2)} \arrow[d, leftrightarrow] \arrow[dr] & \mathbf{SAC_n\,(n\text{-}3)} \arrow[d] \\
\mathbf{PC_n\,(n\text{-}1)} \arrow[d, leftrightarrow] & \mathbf{SAC_n\,(n\text{-}2)} \\
\mathbf{PC_n\,(n)} &
\end{tikzcd}$$

Figure 3: Relationships between the PC and the SAC(n is even).

$$\begin{tikzcd}
\mathbf{PC_n\,(1)} \arrow[r, leftrightarrow] \arrow[d] & \mathbf{SAC_n\,(0)} \arrow[d] \\
\mathbf{PC_n\,(2)} \arrow[d] & \mathbf{SAC_n\,(1)} \arrow[d] \arrow[ddddl] \\
\vdots \arrow[d] & \vdots \arrow[d] \\
\mathbf{PC_n\,(n\text{-}3)} \arrow[d] & \mathbf{SAC_n\,(n\text{-}4)} \arrow[d] \\
\mathbf{PC_n\,(n\text{-}2)} \arrow[d] & \mathbf{SAC_n\,(n\text{-}3)} \arrow[d] \\
\mathbf{PC_n\,(n\text{-}1)} \arrow[r] & \mathbf{SAC_n\,(n\text{-}2)}
\end{tikzcd}$$

Figure 4: Relationships between the PC and the SAC(n is odd).

7 Conclusion

This paper discusses the properties of nonlinearity criteria and the relationships among them. It focuses on the propagation criterion, the strict avalanche criterion, and the nonlinearity.

Firstly, we discussed Boolean functions with n variables satisfying the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$, and those satisfying the PC with respect to all but linearly independent elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. Secondly, we discussed the construction of Boolean functions satisfying the PC with respect to all but one or all but three elements in $\{0,1\}^n - \{(0,\ldots,0)\}$. Thirdly, we showed that the Boolean functions with n variables satisfying the PC of degree $n-2$ are perfectly nonlinear for every even $n \geqslant 4$, and that they satisfy the PC with respect to all but one elements in $\{0,1\}^n - \{(0,\ldots,0)\}$ for every odd $n \geqslant 3$. Lastly, Some relationships were presented between the PC and the SAC.

Note Many of the results presented in this report were obtained independently by Seberry, Zhang and Zheng [SZZ94].

References

[AT90] C. M. Adams, S. E. Tavares: "The use of bent sequences to achieve higher-order strict avalanche criterion," Tech. Rep. Queen's Univ., TR 90–013 (1990).

[For90] R. Forré: "The strict avalanche criterion: Spectral properties of Boolean functions and an extended definition," Proc. CRYPTO'88, LNCS no. 403, pp. 450–468 (1990).

[Llo91] S. Lloyd: "Properties of binary functions," Proc. EUROCRYPT'90, LNCS no. 473, pp. 124–139 (1991).

[MS90] W. Meier, O. Staffelbach: "Nonlinearity criteria for cryptographic functions," Proc. EUROCRYPT'89, LNCS no. 434, pp. 549–562 (1990).

[PLLGV91] B. Preneel, W. V. Leekwijk, L. V. Linden, R. Govaerts, J. Vandewalle: "Propagation characteristics of Boolean functions," Proc. EUROCRYPT'90, LNCS no. 473, pp. 161–173 (1991).

[PGV92] B. Preneel, R. Govaerts, J. Vandewalle: "Boolean functions satisfying higher order propagation criteria," Proc. EUROCRYPT'91, LNCS no. 547, pp. 141–152 (1992).

[Rot76] O. S. Rothaus: "On 'bent' functions," J. Combinatorial Theo. (A), **20**, pp. 300–305 (1976).

[Rue91] R. A. Rueppel: "Stream ciphers," in Contemporary cryptology: The science of information integrity, G. Simmons, ed., IEEE Press, pp. 65–134 (1991).

[SZZ93] J. Seberry, X. M. Zhang, Y. Zheng: "Highly nonlinear balanced Boolean functions satisfying high degree propagation criterion," Tech. Rep. The Univ. Wollongong, tr–93–1 (1993).

[SZZ94] J. Seberry, X. M. Zhang, Y. Zheng: "Characterizing the Structures of Highly Nonlinear Cryptographic Functions," Tech. Rep. The Univ. Wollongong, tr–94–15 (1994).

[WT86] A. F. Webster, S. E. Tavares: "On the design of S-boxes," Proc. CRYPTO'85, LNCS no. 218, pp. 523–534 (1986).