KUIS–95–0009

Unateness, Symmetry and Self-Duality of Boolean Functions Satisfying the Propagation Criterion

HIROSE Shouichi IKEDA Katsuo

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

May 29, 1995

Abstract

Nonlinearity is an important concept for the design of conventional cryptosystems. The propagation criterion(PC) is a nonlinearity criteria of Boolean functions. The aim of this paper is to investigate the relationships between the PC and each one of the unateness, the symmetry and the self-duality. The latter three properties are not desirable for the components of cryptosystems.

First, relationships are presented between the unateness and the degree of the PC. It is shown that every Boolean function with four or more variables satisfying the PC of degree 1 is unate in at most two of its variables and that every Boolean function with four or more variables satisfying the PC of degree 2 is not unate in any one of its variables. These results show the incompatibility of the PC and the unateness. Second, relationships between the PC and the symmetry are investigated. It is shown that there exist symmetric functions satisfying the PC of maximum degree. Finally, compatibility of the PC and the self-duality is discussed. For every odd $n \geq 3$, the existence of self-dual functions with n variables satisfying the PC of degree $n-1$ is shown, which has been implicitly shown before in a few literatures. It is also shown that, for every $n \geq 2$, The degree of the PC of every self-dual function with n variables is at most $n/2-1$.

1 Introduction

Nonlinearity is an important concept for the design of conventional cryptosystems. Several nonlinearity criteria have been proposed as design principles of good conventional cryptosystems[Rue91]. The propagation criterion(PC)[PLLGV91], which is a generalized notion of the strict avalanche criterion[WT86] and the perfect nonlinearity[MS90], is a nonlinearity criteria of Boolean functions.

In the study of Boolean functions, Boolean functions with some sort of properties, such as unateness, symmetry, self-duality, and so on, have been investigated. These properties are not desirable for the components of cryptosystems. The aim of this paper is to investigate the relationships between the PC and each one of the unateness, the symmetry and the self-duality.

First, relationships are presented between the unateness and the degree of the PC. It is shown that every Boolean function with four or more variables satisfying the PC of degree 1 is unate in at most two of its variables and that there exist Boolean functions with four or more variables that satisfy the PC of degree 1 and that are unate in two of their variables. It is also shown that every Boolean function with four or more variables satisfying the PC of degree 2 is not unate in any one of its variables. These results show the incompatibility of the PC and the unateness.

Second, relationships between the PC and the symmetry are investigated. It is shown that there exist symmetric functions satisfying the PC of maximum degree. These functions are also identified.

Finally, compatibility of the PC and the self-duality is discussed. For every odd $n \geq 3$, the existence of self-dual functions with n variables satisfying the PC of degree $n-1$ is shown and an exact characterization of these functions is achieved. These results are shown implicitly in [SZZ93] and [HI95b]. It is also shown that, for every $n \geq 2$, The degree of the PC of every self-dual function with n variables is at most $n/2-1$. The optimality of the result is also shown.

Section 2 gives basic concepts and discusses Boolean functions satisfying the PC. Relationships between the PC and the unateness are discussed in Section 3. Section 4 is devoted to the symmetric Boolean functions satisfying the PC. The self-duality of Boolean functions satisfying the PC is discussed in Section 5.

2 Preliminaries

2.1 Walsh transform and Boolean functions

Let $\mathbf{R}$ and $\mathbf{N}$ denote the set of reals and the set of integers, respectively.

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 $\omega \cdot x = \omega_1 x_1 \oplus \cdots \oplus \omega_n x_n$. □

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 in 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 $f : \{0,1\}^n \to \{0,1\}$. Let B_n be the set of Boolean functions.

The Walsh transform can be applied to Boolean functions 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 $\hat{f}(x) \stackrel{\text{def}}{=} (-1)^{f(x)}$. The Walsh transform of $\hat{f}$ is

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

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

Definition 2 The autocorrelation function of a Boolean function $f \in \mathrm{B}_n$ 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 $x \oplus z$ denotes $(x_1 \oplus z_1, \ldots, x_n \oplus z_n)$. □

Proposition 2 shows a relationship between the autocorrelation function and the Walsh transform.

Proposition 2 For every $f \in \mathrm{B}_n$, $C_f = \mathcal{W}^{-1}(\hat{F}^2)$. □

2.2 The propagation criterion

For a set S, let $|\mathrm{S}|$ denote the number of elements in S. For $f \in \mathrm{B}_n$ and $c \in \{0,1\}$, let $f^{-1}(c) = \{x \mid f(x) = c\}$.

Definition 3 A Boolean function $f \in \mathrm{B}_n$ is balanced if and only if $|f^{-1}(c)| = 2^{n-1}$ for every $c \in \{0,1\}$. □

For every $\{0,1\}$-vector a, let $W(a)$ be the Hamming weight of a, that is, the number of 1's in a.

Definition 4 $f \in \mathrm{B}_n$ 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 every $a \in \{0,1\}^n$ such that $1 \le W(a) \le k$. f is perfectly nonlinear if and only if f satisfies the PC of degree n. □

Let $\mathrm{PC}_n(k)$ denote the set of Boolean functions in B_n satisfying the PC of degree k.

The condition of the above definition states that

$$\Pr(f(x) \oplus f(x \oplus a) = c) = 1/2$$

for every $a \in \{0,1\}^n$ such that $1 \le W(a) \le k$ and every $c \in \{0,1\}$. This means that the value of f changes with probability $1/2$ if at most any k of input variables change. This sensitivity of the value to the input variables is desirable for cryptographic transformations.

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

Proposition 3 Let $f \in \mathrm{B}_n$. f satisfies the PC of degree k if and only if $C_f(a) = 0$ for every $a \in \{0,1\}^n$ such that $1 \leq W(a) \leq k$. □

For perfectly nonlinear Boolean functions, the following proposition was proved[MS90].

Proposition 4 Let $f \in \mathrm{B}_n$. $f \in \mathrm{PC}_n(n)$ if and only if $\left|\hat{F}(\omega)\right| = 2^{n/2}$ for every $\omega \in \{0,1\}^n$. □

Let $\mathrm{V}_n = \{0,1\}^n - \{(0,\ldots,0)\}$.

Definition 5 Let $f \in \mathrm{B}_n$ and $a \in \mathrm{V}_n$. f is said to satisfy the PC with respect to a if $f(x) \oplus f(x \oplus a)$ is balanced. □

2.3 Unateness, Symmetry, and Self-Duality

We begin by defining the unate functions[Koh78].

Definition 6 A Boolean function $f(x_1,\ldots,x_n) \in \mathrm{B}_n$ is said to be positive(negative) in a variable x_i if and only if there exists a disjunctive expression of f in which x_i appears only in uncomplemented(complemented) form. If f is positive(negative) in all of its variables, then f is simply said to be positive(negative). □

Definition 7 A Boolean function $f(x_1,\ldots,x_n) \in \mathrm{B}_n$ is said to be unate in a variable x_i if and only if f is positive or negative in x_i. If f is unate in all of its variables, then f is simply said to be unate. □

For example, $f(x_1,x_2,x_3) = x_1\,x_2 \vee \overline{x_2}\,\overline{x_3}$ is unate in x_1 and x_3 and not unate in x_2.

Proposition 5 Let $f \in \mathrm{B}_n$. $f(x_1,\ldots,x_n)$ is positive in x_i if and only if $f|_{x_i=0} \leq f|_{x_i=1}$. □

Proposition 6 Let $f \in \mathrm{B}_n$. $f(x_1,\ldots,x_n)$ is negative in x_i if and only if $f|_{x_i=0} \geq f|_{x_i=1}$. □

Next, symmetry of Boolean functions is defined.

Definition 8 Let $f \in \mathrm{B}_n$. f is said to be symmetric if and only if $(W(a) = W(b)) \Rightarrow (f(a) = f(b))$ for every $a, b \in \{0,1\}^n$. □

The value of symmetric Boolean functions is determined by the number of 1's in the input variables. Let S_n be the set of symmetric Boolean functions. For $f \in \mathrm{S}_n$, let $f^{(w)}$ denote the value of f to the input variables containing w 1's. Let $\mathrm{I} \subseteq \{0,1,\ldots,n\}$. S_n^{I} represents the symmetric function $f \in \mathrm{S}_n$ such that $f^{(w)} = 1$ if and only if $w \in \mathrm{I}$.

Self-duality of Boolean functions is defined below.

Definition 9 Let $f \in \mathrm{B}_n$. f is said to be self-dual if and only if $f(x_1,\ldots,x_n) = 1 \oplus f(1 \oplus x_1,\ldots,1 \oplus x_n)$. □

Let D_n denote the set of self-dual $f \in \mathrm{B}_n$.

The following proposition is immediate from the definition of the self-duality and that of the autocorrelation function.

Proposition 7 Let $f \in \mathrm{B}_n$. $f \in \mathrm{D}_n$ if and only if $C_f(1,\ldots,1) = -2^n$. □

$x_1\,x_2$	$x_1 \vee x_2$
$\overline{x_1}\,x_2$	$\overline{x_1} \vee x_2$
$x_1\,\overline{x_2}$	$x_1 \vee \overline{x_2}$
$\overline{x_1}\,\overline{x_2}$	$\overline{x_1} \vee \overline{x_2}$

Figure 1: Boolean functions in $\mathrm{PC}_2(2)$

$x_1\,x_2 \vee x_1\,x_3 \vee x_2\,x_3$	$\overline{x_1}\,\overline{x_2} \vee \overline{x_1}\,\overline{x_3} \vee \overline{x_2}\,\overline{x_3}$
$x_1\,x_2 \vee x_1\,\overline{x_3} \vee x_2\,\overline{x_3}$	$\overline{x_1}\,\overline{x_2} \vee \overline{x_1}\,x_3 \vee \overline{x_2}\,x_3$
$x_1\,\overline{x_2} \vee x_1\,x_3 \vee \overline{x_2}\,x_3$	$\overline{x_1}\,x_2 \vee \overline{x_1}\,\overline{x_3} \vee x_2\,\overline{x_3}$
$\overline{x_1}\,x_2 \vee \overline{x_1}\,x_3 \vee x_2\,x_3$	$x_1\,\overline{x_2} \vee x_1\,\overline{x_3} \vee \overline{x_2}\,\overline{x_3}$
$x_1\,\overline{x_2}\,\overline{x_3} \vee \overline{x_1}\,x_2\,x_3$	$\overline{x_1}\,\overline{x_2} \vee x_1\,x_3 \vee x_2\,\overline{x_3}$
$x_1\,\overline{x_2}\,x_3 \vee \overline{x_1}\,x_2\,\overline{x_3}$	$\overline{x_1}\,\overline{x_2} \vee \overline{x_1}\,x_3 \vee x_1\,x_2$
$x_1\,x_2\,\overline{x_3} \vee \overline{x_1}\,\overline{x_2}\,x_3$	$\overline{x_1}\,x_2 \vee x_1\,x_3 \vee \overline{x_2}\,\overline{x_3}$
$\overline{x_1}\,\overline{x_2}\,\overline{x_3} \vee x_1\,x_2\,x_3$	$x_1\,\overline{x_2} \vee \overline{x_1}\,x_3 \vee x_2\,\overline{x_3}$

Figure 2: Boolean functions in $\mathrm{PC}_3(2)$

3 Unateness

Figures 1 and 2 give all Boolean functions in $\mathrm{PC}_2(2)$ and $\mathrm{PC}_3(2)$, respectively. From these figures, it is easily observed that both $\mathrm{PC}_2(2)$ and $\mathrm{PC}_3(2)$ contain unate functions.

Suppose that $f(x_1, \ldots, x_n) \in \mathrm{B}_n$ is unate in x_n. Then, for every $(a_1, \ldots, a_{n-1}) \in \{0,1\}^{n-1}$, $f(a_1, \ldots, a_{n-1}, 0) = 0$ if $f(a_1, \ldots, a_{n-1}, 1) = 0$ or $f(a_1, \ldots, a_{n-1}, 1) = 0$ if $f(a_1, \ldots, a_{n-1}, 0) = 0$. This regularity does not seem compatible with the PC. In the following, this conjecture is shown to be correct for $f \in \mathrm{B}_n$ when $n \geq 4$. Before showing the results, several lemmas are presented.

Lemma 1 [HI95a] Let w, x, y, z and m be integers such that $w \geq x \geq y \geq z \geq 0$ and $m \geq 0$. Let $w^2 + x^2 + y^2 + z^2 = 2^m$. Then,

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

□

Lemma 2 Let $n \geq 2$ and $f \in \mathrm{PC}_n(1)$. Then, for every i such that $1 \leq i \leq n$, $f(x_1, \ldots, x_n)$ is positive in x_i if and only if $\hat{F}(0, \ldots, 0, \overset{i}{\check{1}}, 0, \ldots, 0) = 2^{n-1}$.

(Proof) Suppose that $i = n$. Since $f \in \mathrm{PC}_n(1)$, $f(x_1, \ldots, x_{n-1}, 0) \oplus f(x_1, \ldots, x_{n-1}, 1)$ is balanced,that is, $|\{\langle x \rangle_{n-1} \mid f|_{x_n=0} \neq f|_{x_n=1}\}| = 2^{n-2}$. Thus,

$$
\begin{aligned}
\hat{F}(0, \ldots, 0, 1) &= \sum_{x \in \{0,1\}^n} \hat{f}(x)(-1)^{x_n} \\
&= \sum_{\langle x \rangle_{n-1} \in \{0,1\}^{n-1}} (\hat{f}|_{x_n=0} - \hat{f}|_{x_n=1}) \\
&= 2|\{\langle x \rangle_{n-1} \mid f|_{x_n=0} = 0, f|_{x_n=1} = 1\}| - 2|\{\langle x \rangle_{n-1} \mid f|_{x_n=0} = 1, f|_{x_n=1} = 0\}| \\
&= 2^{n-1} - 4|\{\langle x \rangle_{n-1} \mid f|_{x_n=0} = 1, f|_{x_n=1} = 0\}|.
\end{aligned}
$$

Hence, $\hat{F}(0,\ldots,0,1) = 2^{n-1}$ if and only if $f(x)$ is positive in x_n. The same argument can be applied to the case where $1 \leq i \leq n-1$. □

The following lemma can be proved in the same way as Lemma 2.

Lemma 3 Let $n \geq 2$ and $f \in \mathrm{PC}_n(1)$. Then, for every i such that $1 \leq i \leq n$, $f(x_1,\ldots,x_n)$ is negative in x_i if and only if $\hat{F}(0,\ldots,0,\overset{i}{\check{1}},0,\ldots,0) = -2^{n-1}$. □

From Lemmas 2 and 3, if $f(x_1,\ldots,x_n) \in \mathrm{PC}_n(1)$ is unate in x_i, then

$$\hat{F}^2(0,\cdots,0,\overset{i}{\check{1}},0,\ldots,0) = 2^{2n-2} = \frac{1}{4}\sum_{\omega\in\{0,1\}^n}\hat{F}^2(\omega).$$

From this fact, it is immediately derived that every Boolean function satisfying the PC of degree 1 is unate in at most 4 of its variables. A more strict result is given in the following.

Lemma 4 Let $f \in \mathrm{B}_n$. Then, $f \in \mathrm{PC}_n(k)$ if and only if

$$\sum_{a\cdot\omega=0}\hat{F}^2(\omega) = \sum_{a\cdot\omega=1}\hat{F}^2(\omega) = 2^{2n-1}$$

for every $a \in \{0,1\}^n$ such that $1 \leq W(a) \leq k$.

(Proof) Since $f \in \mathrm{B}_n$, $f \in \mathrm{PC}_n(k)$ if and only if, for every $a \in \{0,1\}^n$ such that $1 \leq W(a) \leq k$, $C_f(a) = \frac{1}{2^n}\sum_{\omega\in\{0,1\}^n}\hat{F}^2(\omega)(-1)^{a\cdot\omega} = 0$. Thus, $\sum_{a\cdot\omega=0}\hat{F}^2(\omega) = \sum_{a\cdot\omega=1}\hat{F}^2(\omega)$. The lemma holds because $\sum_{\omega\in\{0,1\}^n}\hat{F}^2(\omega) = 2^{2n}$ for every $f \in \mathrm{B}_n$. □

Theorem 1 Let $n \geq 4$. If $f \in \mathrm{PC}_n(1)$, then f is unate at most two of its variables.

(Proof) Without loss of generality, it can be assumed that $f(x_1,\ldots,x_n) \in \mathrm{PC}_n(1)$ is unate in x_1, x_2 and x_3. Then, from Lemmas 2 and 3,

$$\begin{aligned}&\hat{F}^2(1,0,0,0,\ldots,0) + \hat{F}^2(0,1,0,0,\ldots,0) + \hat{F}^2(0,0,1,0,\ldots,0)\\ &= 2^{2(n-1)} + 2^{2(n-1)} + 2^{2(n-1)}\\ &= 2^{2n-1} + 2^{2n-2}.\end{aligned}$$

Since $f(x_1,\ldots,x_n) \in \mathrm{PC}_n(1)$, from Lemma 4, $\sum_{\omega_4=0}\hat{F}^2(\omega) = 2^{2n-1}$, which causes a contradiction. □

The optimality of the above result can also be proved. In the following, we present an exact characterization of a Boolean function in $\mathrm{PC}_n(1)$ that is unate in two of its variables.

Theorem 2 Let $n \geq 4$ and $f \in \mathrm{PC}_n(1)$. $f(x_1,\ldots,x_n)$ is unate in x_i and x_j if and only if f satisfies one of the following two conditions:

- $\hat{F}(k) = 0$ if $k \notin \{2^{i-1}, 2^{j-1}, 2^n - 2^{i-1} - 1, 2^n - 2^{j-1} - 1\}$, and an odd number of $\hat{F}(2^{i-1})$, $\hat{F}(2^{j-1})$, $\hat{F}(2^n - 2^{i-1} - 1)$ and $\hat{F}(2^n - 2^{j-1} - 1)$ are equal to 2^{n-1} and the others are equal to -2^{n-1}.
- $\hat{F}(k) = 0$ if $k \notin \{2^{i-1}, 2^{j-1}, 2^n - 1, 2^n - 2^{i-1} - 2^{j-1} - 1\}$, and an odd number of $\hat{F}(2^{i-1})$, $\hat{F}(2^{j-1})$, $\hat{F}(2^n - 1)$ and $\hat{F}(2^n - 2^{i-1} - 2^{j-1} - 1)$ are equal to 2^{n-1} and the others are equal to -2^{n-1}.

(Proof) We prove the theorem only for the first condition. It can be proved in the same way for the second condition.

Suppose that $f \in \mathrm{PC}_n(1)$ is unate in x_1 and x_2. Then,

$$\hat{F}^2(1,0,0,\ldots,0) + \hat{F}^2(0,1,0,\ldots,0) = 2^{2(n-1)} + 2^{2(n-1)} = 2^{2n-1}.$$

Since $\sum_{\omega_i=0} \hat{F}^2(\omega) = 2^{2n-1}$ for every i such that $3 \le i \le n$,

$$\omega \neq \left\{ \begin{array}{ll} (1,0,0,\ldots,0), & (0,1,0,\ldots,0), \\ (1,0,1,\ldots,1), & (0,1,1,\ldots,1), \\ (0,0,1,\ldots,1), & (1,1,1,\ldots,1) \end{array} \right\} \Rightarrow \hat{F}(\omega) = 0.$$

Let

$$\begin{array}{ll} \hat{F}(1,0,0,\ldots,0) = \hat{F}_1, & \hat{F}(0,1,0,\ldots,0) = \hat{F}_0, \\ \hat{F}(1,0,1,\ldots,1) = \hat{F}_{10}, & \hat{F}(0,1,1,\ldots,1) = \hat{F}_{01}, \\ \hat{F}(0,0,1,\ldots,1) = \hat{F}_{00}, & \hat{F}(1,1,1,\ldots,1) = \hat{F}_{11}. \end{array}$$

Since $\sum_{\omega_i=0} \hat{F}^2(\omega) = \sum_{\omega_i=1} \hat{F}^2(\omega) = 2^{2n-1}$ for $i = 1, 2$,

$$\hat{F}_{00}^2 + \hat{F}_{01}^2 = \hat{F}_{10}^2 + \hat{F}_{11}^2 = \hat{F}_{00}^2 + \hat{F}_{10}^2 = \hat{F}_{01}^2 + \hat{F}_{11}^2 = 2^{2(n-1)}.$$

From Lemma 1, there are following two cases:

C-1. $\left|\hat{F}_{10}\right| = \left|\hat{F}_{01}\right| = 2^{n-1}$, $\left|\hat{F}_{00}\right| = \left|\hat{F}_{11}\right| = 0$,

C-2. $\left|\hat{F}_{00}\right| = \left|\hat{F}_{11}\right| = 2^{n-1}$, $\left|\hat{F}_{10}\right| = \left|\hat{F}_{01}\right| = 0$.

For C-1, let $b_1 = (1,0,0,\ldots,0)$, $b_2 = (0,1,0,\ldots,0)$ $b_3 = (1,0,1,\ldots,1)$, and $b_4 = (0,1,1,\ldots,1)$. Then, $\left[\hat{f}\right]$ can be represented as

$$\left[\hat{f}\right] = \frac{1}{2^n}\left[\hat{F}\right] H_n = \frac{1}{2^n}\left(\hat{F}_1\left[\hat{l}_{b_1}\right] + \hat{F}_0\left[\hat{l}_{b_2}\right] + \hat{F}_{10}\left[\hat{l}_{b_3}\right] + \hat{F}_{01}\left[\hat{l}_{b_4}\right]\right).$$

Since $b_1 \oplus b_2 \oplus b_3 \oplus b_4 = (0,\ldots,0)$, for every $x \in \{0,1\}^n$, an even number of $\hat{l}_{b_1}(x)$, $\hat{l}_{b_2}(x)$, $\hat{l}_{b_3}(x)$ and $\hat{l}_{b_4}(x)$ are equal to 1, and the others are equal to -1. Thus, an odd number of $\hat{F}_1$, $\hat{F}_0$, $\hat{F}_{10}$ and $\hat{F}_{01}$ must be equal to 2^{n-1} and the others must be equal to -2^{n-1} since $f \in \mathrm{B}_n$.

Conversely, if an odd number of $\hat{F}_1$, $\hat{F}_0$, $\hat{F}_{10}$ and $\hat{F}_{01}$ are equal to 2^{n-1} and the others are equal to -2^{n-1}, then $f \in \mathrm{PC}_n(1)$ and f is unate in x_1 and x_2.

The same argument as the above one can be applicable to C-2. □

Corollary 1 Let $n \ge 4$. For every i, j such that $1 \le i < j \le n$, there are 16 $f(x_1,\ldots,x_n)$'s in $\mathrm{PC}_n(1)$ that are unate in x_i and x_j. □

The proof of Theorem 2 gives a method of construction for Boolean functions satisfying the PC of degree 1 and are unate in two of their variables. This method can construct every such functions.

Example 1 Four Boolean functions are given that are in $\mathrm{PC}_4(1)$ and that are positive in x_1 and x_2. Let

$$\begin{aligned} \left[\hat{F}_0\right] &= [0,8,8,0,0,0,0,0,0,0,0,0,0,-8,8,0], \\ \left[\hat{F}_1\right] &= [0,8,8,0,0,0,0,0,0,0,0,0,0,8,-8,0]. \end{aligned}$$

Then,

$$\left[\hat{f_0}\right] = \frac{1}{2^4}\left[\hat{F_0}\right] H_4 = [1,1,-1,-1,1,-1,1,-1,1,-1,1,-1,1,1,-1,-1],$$

$$\left[\hat{f_1}\right] = \frac{1}{2^4}\left[\hat{F_1}\right] H_4 = [1,-1,1,-1,1,1,-1,-1,1,1,-1,-1,1,-1,1,-1].$$

Thus,

$$f_0(x_1,x_2,x_3,x_4) = x_1\overline{x_3}x_4 \vee x_1x_3\overline{x_4} \vee x_2x_3x_4 \vee x_2\overline{x_3}\,\overline{x_4} = x_1(x_3 \oplus x_4) \vee x_2(x_3 \oplus x_4 \oplus 1),$$

$$f_1(x_1,x_2,x_3,x_4) = x_1x_3x_4 \vee x_1\overline{x_3}\,\overline{x_4} \vee x_2\overline{x_3}x_4 \vee x_2x_3\overline{x_4} = x_1(x_3 \oplus x_4 \oplus 1) \vee x_2(x_3 \oplus x_4).$$

The other two functions can be constructed in the same way as the above. They are

$$g_0(x_1,x_2,x_3,x_4) = x_1x_2 \vee x_1\overline{x_3}x_4 \vee x_1x_3\overline{x_4} \vee x_2\overline{x_3}x_4 \vee x_2x_3\overline{x_4} = x_1x_2 \vee (x_1 \vee x_2)(x_3 \oplus x_4),$$

$$g_1(x_1,x_2,x_3,x_4) = x_1x_2 \vee x_1x_3x_4 \vee x_1\overline{x_3}\,\overline{x_4} \vee x_2x_3x_4 \vee x_2\overline{x_3}\,\overline{x_4} = x_1x_2 \vee (x_1 \vee x_2)(x_3 \oplus x_4 \oplus 1).$$

The truth tables of the above functions are presented in Figure 3. □

The observation in Example 1 can be generalized to the following corollary of Theorem 2.

Corollary 2 Let $n \geq 4$ and $f \in \mathrm{PC}_n(1)$. $f(x_1,\ldots,x_n)$ is unate in x_i and x_j if and only if f can be represented in one of the following formulas:

- $(c_1 \oplus x_i)L_{\{i,j\}}(x_1,\ldots,x_n) \vee (c_2 \oplus x_j)(1 \oplus L_{\{i,j\}}(x_1,\ldots,x_n))$,
- $(c_1 \oplus x_i)(1 \oplus L_{\{i,j\}}(x_1,\ldots,x_n)) \vee (c_2 \oplus x_j)L_{\{i,j\}}(x_1,\ldots,x_n)$,
- $(c_1 \oplus x_i)(c_2 \oplus x_j) \vee ((c_1 \oplus x_i) \vee (c_2 \oplus x_j))L_{\{i,j\}}(x_1,\ldots,x_n)$,
- $(c_1 \oplus x_i)(c_2 \oplus x_j) \vee ((c_1 \oplus x_i) \vee (c_2 \oplus x_j))(1 \oplus L_{\{i,j\}}(x_1,\ldots,x_n))$,

where $L_{\{i,j\}}(x_1,\ldots,x_n) = \bigoplus_{k\in\{1,\ldots,n\}-\{i,j\}} x_k$ and $c_1, c_2 \in \{0,1\}$. □

The following theorem is on non-unateness of the Boolean functions satisfying the PC of degree 2.

Theorem 3 Let $n \geq 4$. If $f \in \mathrm{PC}_n(2)$, then f is not unate in any one of its variables.

(Proof) Suppose that $f \in \mathrm{PC}_n(2)$ is unate in x_1. Then, $\hat{F}^2(1,0,\ldots,0) = 2^{2(n-1)}$. Let i, j be any integers such that $2 \leq i < j \leq n$. Since $f \in \mathrm{PC}_n(2)$, $\sum_{\omega_i=0} \hat{F}^2(\omega) = 2^{2n-1}$, $\sum_{\omega_j=0} \hat{F}^2(\omega) = 2^{2n-1}$, and $\sum_{\omega_i\oplus\omega_j=1} \hat{F}^2(\omega) = 2^{2n-1}$. Thus,

$$\sum_{\omega_i=0} \hat{F}^2(\omega) + \sum_{\omega_j=0} \hat{F}^2(\omega) - 2\hat{F}^2(1,0,\ldots,0) - \sum_{\omega_i\oplus\omega_j=1} \hat{F}^2(\omega) = 0.$$

From this equation, if $\hat{F}(\omega) \neq 0$, then at most one of $\omega_2,\ldots,\omega_n$ is 0 or $\omega = (1,0,\ldots,0)$.

If $n = 4$, then, for every $f \in \mathrm{PC}_4(2)$, f is perfectly nonlinear and $\hat{F}^2(\omega) = 16$ for every $\omega \in \{0,1\}^4$, which is a contradiction.

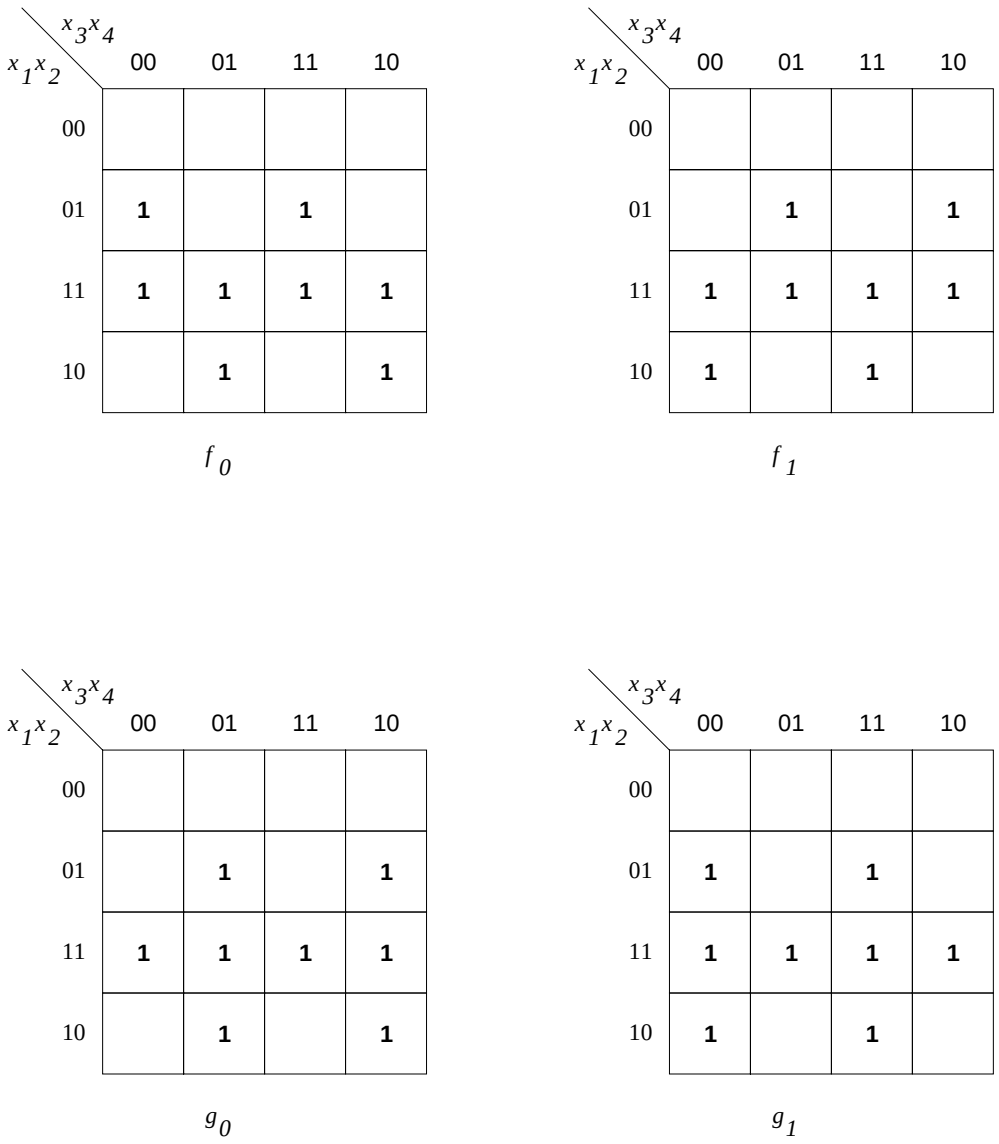

Figure 3: Functions in $\mathrm{PC}_4(1)$ and positive in x_1 and x_2

For $n \geq 5$,

$$\begin{aligned}
&\sum_{\omega_i \oplus \omega_j = 1} \hat{F}^2(\omega) \\
&= \hat{F}^2(0,1,\ldots,1,\overset{i}{\check{0}},1,\ldots,1) + \hat{F}^2(0,1,\ldots,1,\overset{j}{\check{0}},1,\ldots,1) + \\
&\quad \hat{F}^2(1,1,\ldots,1,\overset{i}{\check{0}},1,\ldots,1) + \hat{F}^2(1,1,\ldots,1,\overset{j}{\check{0}},1,\ldots,1) \\
&= 2^{2n-1}.
\end{aligned}$$

Thus, from Lemma 1, for every $\omega \in \{0,1\}^n$ such that only one of $\omega_2,\ldots,\omega_n$ is 0 and $\hat{F}(\omega) \neq 0$, $\hat{F}^2(\omega) = 2^{2n-2}$. For every $\omega \in \{0,1\}^n$ such that only one of $\omega_2,\ldots,\omega_n$ is 0, since

$$\sum_{\omega_1=0} \hat{F}^2(\omega) = \sum_{\omega_1=1} \hat{F}^2(\omega) = 2^{2n-1},$$

$$\hat{F}^2(1,0,\ldots,0) = 2^{2(n-1)},$$

at most three of $\hat{F}^2(\omega)$'s are 2^{2n-2}, while, since

$$\sum_{\omega_2 \oplus \omega_3 = 1} \hat{F}^2(\omega) = \sum_{\omega_4 \oplus \omega_5 = 1} \hat{F}^2(\omega) = 2^{2n-1},$$

at least four of $\hat{F}^2(\omega)$'s are 2^{2n-2}. This causes a contradiction. Thus, the theorem has been proved. □

4 Symmetry

In this section, relationships between the symmetry and the PC are presented.

The following lemma shows a necessary condition for the Boolean functions satisfying the PC of degree 2 to be symmetric.

Lemma 5 Let $n \geq 2$. If $f \in \mathrm{PC}_n(2) \cap \mathrm{S}_n$, then$f^{(w+2)} = \overline{f^{(w)}}$ for every w such that $0 \leq w \leq n-2$.

(Proof) Let p be $1 \leq p \leq n-1$. Let $b^p = (b_1^p, \ldots, b_n^p) \in \{0,1\}^n$ such that $b_p^p = b_{p+1}^p = 1$ and $b_i^p = 0$ if $i \neq p, p+1$.

Since $f \in \mathrm{PC}_n(2)$, $f(x) \oplus f(x \oplus b^p)$ is balanced for every p such that $1 \leq p \leq n-1$. Since $f \in \mathrm{S}_n$,

$$f|_{x_p=0, x_{p+1}=1} \equiv f|_{x_p=1, x_{p+1}=0}$$

for every p such that $1 \leq p \leq n-1$. Thus,

$$f|_{x_p=0, x_{p+1}=0} \oplus f|_{x_p=1, x_{p+1}=1} \equiv 1$$

for every p such that $1 \leq p \leq n-1$. Thus, $f^{(w+2)} = \overline{f^{(w)}}$ for every w such that $0 \leq w \leq n-2$. □

The following lemma shows that there exist symmetric functions satisfying the PC of maximum degree.

Lemma 6 Let $n \geq 2$ and $f \in \mathrm{S}_n$. If $f^{(w+2)} = \overline{f^{(w)}}$ for every w such that $0 \leq w \leq n-2$, then

$$f \in \begin{cases} \mathrm{PC}_n(n) & \text{for even } n, \\ \mathrm{PC}_n(n-1) & \text{for odd } n. \end{cases}$$

(Proof) Let $W(a) = r$ and $\mathrm{I}(a) = \{i \mid a_i = 1, 1 \leq i \leq n\}$. Let $\mathrm{R}_j = \{4k + j \mid k = 0, 1, \ldots, \lfloor (n-j)/4 \rfloor\}$ for $j = 0, 1, 2, 3$.

f is any one of $S_n^{\mathrm{R}_0 \cup \mathrm{R}_1}$, $S_n^{\mathrm{R}_0 \cup \mathrm{R}_3}$, $S_n^{\mathrm{R}_2 \cup \mathrm{R}_3}$ and $S_n^{\mathrm{R}_1 \cup \mathrm{R}_2}$. Since $S_n^{\mathrm{R}_2 \cup \mathrm{R}_3} = \overline{S_n^{\mathrm{R}_0 \cup \mathrm{R}_1}}$ and $S_n^{\mathrm{R}_0 \cup \mathrm{R}_3} = \overline{S_n^{\mathrm{R}_1 \cup \mathrm{R}_2}}$, it is sufficient to prove for $S_n^{\mathrm{R}_0 \cup \mathrm{R}_1}$ and $S_n^{\mathrm{R}_1 \cup \mathrm{R}_2}$.

For the case where $f = S_n^{\mathrm{R}_0 \cup \mathrm{R}_1}$:

(i) Suppose that $r \equiv 0 \pmod 4$.

For every $x \in \{0,1\}^n$ such that $|\mathrm{I}(a) \cap I(x)| = 2k$ for some k such that $0 \leq k \leq r/2$,

$$|W(x) - W(x \oplus a)| \equiv 0 \pmod 4.$$

Thus, in this case, $f(x) \oplus f(x \oplus a) = 0$.

For every $x \in \{0,1\}^n$ such that $|\mathrm{I}(a) \cap I(x)| = 2k+1$ for some k such that $0 \leq k \leq r/2 - 1$,

$$|W(x) - W(x \oplus a)| \equiv 2 \pmod 4.$$

Thus, in this case, $f(x) \oplus f(x \oplus a) = 1$.

From the above discussion,

$$\{x \mid f(x) \oplus f(x \oplus a) = 1\} = \{x \mid |\mathrm{I}(a) \cap I(x)| \text{ is odd}\}.$$

Hence,

$$|\{x \mid f(x) \oplus f(x \oplus a) = 1\}| = 2^{n-r} \sum_{k=0}^{r/2-1} {}_r\mathrm{C}_{2k+1} = 2^{n-1}.$$

(ii) Suppose that $r \equiv 1 \pmod 4$.

For every $x \in \{0,1\}^n$ such that $|\mathrm{I}(a) \cap I(x)| = 2k$ for some k such that $0 \le k \le (r-1)/2$,

$$|W(x) - W(x \oplus a)| = \begin{cases} r - 4k \equiv 1 \pmod 4 & \text{if } r - 2k \ge 2k \\ 4k - r \equiv 3 \pmod 4 & \text{if } r - 2k < 2k. \end{cases}$$

Thus, in this case, $f(x) \oplus f(x \oplus a) = 1$ if and only if $W(x)$ is odd.

For every $x \in \{0,1\}^n$ such that $|\mathrm{I}(a) \cap I(x)| = 2k+1$ for some k such that $0 \le k \le (r-1)/2$,

$$|W(x) - W(x \oplus a)| = \begin{cases} r - (4k+2) \equiv 3 \pmod 4 & \text{if } W(x \oplus a) \ge W(x) \\ (4k+2) - r \equiv 1 \pmod 4 & \text{if } W(x \oplus a) < W(x). \end{cases}$$

Thus, in this case, $f(x) \oplus f(x \oplus a) = 1$ if and only if $W(x)$ is even.

From the above discussion,

$$\{x \mid f(x) \oplus f(x \oplus a) = 1\} =$$
$$\{x \mid |\mathrm{I}(a) \cap I(x)| \text{ is even and } W(x) \text{ is odd}\} \cup \{x \mid |\mathrm{I}(a) \cap I(x)| \text{ is odd and } W(x) \text{ is even}\}.$$

Hence, unless $n \equiv 1 \pmod 4$ and $a = (1, \ldots, 1)$, then

$$\begin{aligned} |\{x \mid f(x) \oplus f(x \oplus a) = 1\}| &= \sum_{k=0}^{\frac{r-1}{2}} {}_r\mathrm{C}_{2k} \sum_{j=0}^{\lfloor \frac{n-r-1}{2} \rfloor} {}_{n-r}\mathrm{C}_{2j+1} + \sum_{k=0}^{\frac{r-1}{2}} {}_r\mathrm{C}_{2k+1} \sum_{j=0}^{\lfloor \frac{n-r-1}{2} \rfloor} {}_{n-r}\mathrm{C}_{2j+1} \\ &= 2^{n-1}, \end{aligned}$$

and $f(x) \oplus f(x \oplus a)$ is balanced. If $n \equiv 1 \pmod 4$ and $a = (1, \ldots, 1)$, then

$$\begin{aligned} \{x \mid |\mathrm{I}(a) \cap I(x)| \text{ is even and } W(x) \text{ is odd}\} &= \emptyset, \\ \{x \mid |\mathrm{I}(a) \cap I(x)| \text{ is odd and } W(x) \text{ is even}\} &= \emptyset. \end{aligned}$$

Thus, in this case, $f(x) \oplus f(x \oplus a) \equiv 0$.

(iii) Suppose that $r \equiv 2 \pmod 4$. In this case, we can prove in the same way as (i) that

$$\{x \mid f(x) \oplus f(x \oplus a) = 1\} = \{x \mid |\mathrm{I}(a) \cap I(x)| \text{ is even}\}.$$

Hence,

$$|\{x \mid f(x) \oplus f(x \oplus a) = 1\}| = 2^{n-r} \sum_{k=0}^{r/2} {}_r\mathrm{C}_{2k} = 2^{n-1}.$$

(iv) Suppose that $r \equiv 3 \pmod 4$. It can be obtained in the same way as (ii) that

$$\{x \mid f(x) \oplus f(x \oplus a) = 1\} =$$
$$\{x \mid |\mathrm{I}(a) \cap I(x)| \text{ and } W(x) \text{ are even}\} \cup \{x \mid |\mathrm{I}(a) \cap I(x)| \text{ and } W(x) \text{ are odd}\}.$$

Hence, unless $n \equiv 3 \pmod 4$ and $a = (1, \ldots, 1)$, then

$$\begin{aligned} |\{x \mid f(x) \oplus f(x \oplus a) = 1\}| &= \sum_{k=0}^{\frac{r-1}{2}} {}_r\mathrm{C}_{2k} \sum_{j=0}^{\lceil \frac{n-r-1}{2} \rceil} {}_{n-r}\mathrm{C}_{2j} + \sum_{k=0}^{\frac{r-1}{2}} {}_r\mathrm{C}_{2k+1} \sum_{j=0}^{\lceil \frac{n-r-1}{2} \rceil} {}_{n-r}\mathrm{C}_{2j} \\ &= 2^{n-1}, \end{aligned}$$

and $f(x) \oplus f(x \oplus a)$ is balanced. If $n \equiv 3 \pmod 4$ and $a = (1, \ldots, 1)$, then

$$\begin{aligned} \{x \,|\, |\mathrm{I}(a) \cap I(x)| \text{ is even and } W(x) \text{ is odd}\} &= \{x \,|\, W(x) \text{ is odd}\} \\ \{x \,|\, |\mathrm{I}(a) \cap I(x)| \text{ is odd and } W(x) \text{ is even}\} &= \{x \,|\, W(x) \text{ is even}\}. \end{aligned}$$

Thus, in this case, $f(x) \oplus f(x \oplus a) \equiv 1$.

For the case where $f = S_n^{\mathrm{R}_1 \cup \mathrm{R}_2}$:

(v) Suppose that $r \equiv 0 \pmod 4$. It is obtained that

$$\{x \,|\, f(x) \oplus f(x \oplus a) = 1\} = \{x \,|\, |\mathrm{I}(a) \cap I(x)| \text{ is odd}\}.$$

Hence, $f(x) \oplus f(x \oplus a)$ is balanced.

(vi) Suppose that $r \equiv 1 \pmod 4$. It can be obtained that

$$\begin{aligned} &\{x \,|\, f(x) \oplus f(x \oplus a) = 1\} = \\ &\quad \{x \,|\, |\mathrm{I}(a) \cap I(x)| \text{ and } W(x) \text{ are even}\} \cup \{x \,|\, |\mathrm{I}(a) \cap I(x)| \text{ and } W(x) \text{ are odd}\}. \end{aligned}$$

Hence, unless $n \equiv 1 \pmod 4$ and $a = (1, \ldots, 1)$, then $f(x) \oplus f(x \oplus a)$ is balanced. If $n \equiv 1 \pmod 4$ and $a = (1, \ldots, 1)$, then $f(x) \oplus f(x \oplus a) \equiv 1$.

(vii) Suppose that $r \equiv 2 \pmod 4$. In this case, we can prove in the same way as (i) that

$$\{x \,|\, f(x) \oplus f(x \oplus a) = 1\} = \{x \,|\, |\mathrm{I}(a) \cap I(x)| \text{ is even}\}.$$

Hence, $f(x) \oplus f(x \oplus a)$ is balanced.

(viii) Suppose that $r \equiv 3 \pmod 4$. It is obtained that

$$\begin{aligned} &\{x \,|\, f(x) \oplus f(x \oplus a) = 1\} = \\ &\quad \{x \,|\, |\mathrm{I}(a) \cap I(x)| \text{ is even and } W(x) \text{ is odd}\} \cup \{x \,|\, |\mathrm{I}(a) \cap I(x)| \text{ is odd and } W(x) \text{ is even}\}. \end{aligned}$$

Hence, unless $n \equiv 3 \pmod 4$ and $a = (1, \ldots, 1)$, then $f(x) \oplus f(x \oplus a)$ is balanced. If $n \equiv 3 \pmod 4$ and $a = (1, \ldots, 1)$, then $f(x) \oplus f(x \oplus a) \equiv 0$. □

From the above two lemmas, the following theorem is obtained.

Theorem 4 Let $n \geq 2$.

- If n is even, then, for every k such that $2 \leq k \leq n$,

$$\mathrm{PC}_n(k) \cap \mathrm{S}_n = \{f \in \mathrm{S}_n \,|\, f^{(w+2)} = \overline{f^{(w)}} \text{ for every } w \text{ such that } 0 \leq w \leq n-2\}.$$

- If n is odd, then, for every k such that $2 \leq k \leq n-1$,

$$\mathrm{PC}_n(k) \cap \mathrm{S}_n = \{f \in \mathrm{S}_n \,|\, f^{(w+2)} = \overline{f^{(w)}} \text{ for every } w \text{ such that } 0 \leq w \leq n-2\}.$$

□

The number of symmetric Boolean functions with n variables satisfying the PC of degree more than 1 is 4 for $n \geq 4$.

Theorem 5 Let $n \geq 2$ be even and $f \in \mathrm{S}_n$. $f \in \mathrm{PC}_n(1)$ if, for every w such that $0 \leq w \leq n/2-1$,

$$f^{(w+1)} = f^{(w)} \text{ and } f^{(n-w)} = \overline{f^{(n-w-1)}},$$

or

$$f^{(w+1)} = \overline{f^{(w)}} \text{ and } f^{(n-w)} = f^{(n-w-1)}.$$

(Proof) $f(x_1, \ldots, x_{n-1}, x_n) \oplus f(x_1, \ldots, x_{n-1}, x_n \oplus 1)$ is balanced if and only if $f(x_1, \ldots, x_{n-1}, 0) \oplus f(x_1, \ldots, x_{n-1}, 1)$ is balanced. Suppose that $f^{(w+1)} = f^{(w)}$ and $f^{(n-w)} = \overline{f^{(n-w-1)}}$, or $f^{(w+1)} = \overline{f^{(w)}}$ and $f^{(n-w)} = f^{(n-w-1)}$. Then, for every k such that $0 \leq k \leq n/2-1$,

$$\begin{aligned}&|\{\langle x\rangle_{n-1} \mid f(\langle x\rangle_{n-1}, 0) \oplus f(\langle x\rangle_{n-1}, 1) = 1, \text{ and } W(\langle x\rangle_{n-1}) = k \text{ or } W(\langle x\rangle_{n-1}) = n-1-k\}| \\ &\quad = {}_{n-1}\mathrm{C}_k.\end{aligned}$$

Thus,

$$|\{\langle x\rangle_{n-1} \mid f(\langle x\rangle_{n-1}, 0) \oplus f(\langle x\rangle_{n-1}, 1) = 1\}| = \sum_{k=0}^{n/2-1} {}_{n-1}\mathrm{C}_k = 2^{n-2}.$$

This implies that $f(x_1, \ldots, x_{n-1}, x_n) \oplus f(x_1, \ldots, x_{n-1}, x_n \oplus 1)$ is balanced.

It can be proved in the same way that $f(x_1, \ldots, x_n) \oplus f(x_1, \ldots, x_{i-1}, \overline{x_i}, x_{i+1}, \ldots, x_n)$ is balanced for every i such that $1 \leq i \leq n-1$. □

From the above theorem, it follows that $|\mathrm{PC}_n(1) \cap \mathrm{S}_n| \geq 2^{n/2+1}$ for every even $n \geq 2$.

Corollary 3 For every even $n \geq 4$, $\mathrm{PC}_n(1) \cap \mathrm{S}_n \neq \mathrm{PC}_n(2) \cap \mathrm{S}_n = \cdots = \mathrm{PC}_n(n) \cap \mathrm{S}_n$. □

5 Self-Duality

Self-duality of Boolean functions satisfying the PC is discussed in this section. First, two lemmas are presented on the properties of self-dual Boolean functions.

Lemma 7 If $f \in \mathrm{D}_n$, then

$$\hat{F}(\omega) = \begin{cases} 0 & \text{if } W(\omega) \text{ is even} \\ 2\hat{F}_0(\langle\omega\rangle_{n-1}) & \text{if } W(\omega) \text{ is odd,} \end{cases}$$

where $\hat{F}_0(\langle\omega\rangle_{n-1}) = \sum_{\langle x\rangle_{n-1}} \hat{f}(\langle x\rangle_{n-1}, 0)(-1)^{\langle\omega\rangle_{n-1}\cdot\langle x\rangle_{n-1}}$.

(Proof) Since $f(x_1, \ldots, x_n) = 1 \oplus f(1 \oplus x_1, \ldots, 1 \oplus x_n)$, $f(x_1, \ldots, x_{n-1}, 1) = 1 \oplus f(1 \oplus x_1, \ldots, 1 \oplus x_{n-1}, 0)$.

$$\begin{aligned}
\hat{F}(\omega) &= \sum_x \hat{f}(x)(-1)^{\omega\cdot x} \\
&= \sum_{\langle x\rangle_{n-1}} \hat{f}(\langle x\rangle_{n-1}, 0)(-1)^{\langle\omega\rangle_{n-1}\cdot\langle x\rangle_{n-1}} + \sum_{\langle x\rangle_{n-1}} \hat{f}(\langle x\rangle_{n-1}, 1)(-1)^{\langle\omega\rangle_{n-1}\cdot\langle x\rangle_{n-1}\oplus\omega_n} \\
&= \sum_{\langle x\rangle_{n-1}} \hat{f}(\langle x\rangle_{n-1}, 0)(-1)^{\langle\omega\rangle_{n-1}\cdot\langle x\rangle_{n-1}} - \sum_{\langle x\rangle_{n-1}} \hat{f}(1 \oplus x_1, \ldots, 1 \oplus x_{n-1}, 0)(-1)^{\langle\omega\rangle_{n-1}\cdot\langle x\rangle_{n-1}\oplus\omega_n} \\
&= \sum_{\langle x\rangle_{n-1}} \hat{f}(\langle x\rangle_{n-1}, 0)(-1)^{\langle\omega\rangle_{n-1}\cdot\langle x\rangle_{n-1}} - \sum_{\langle y\rangle_{n-1}} \hat{f}(\langle y\rangle_{n-1}, 0)(-1)^{\omega_1(1\oplus y_1)\oplus\cdots\oplus\omega_{n-1}(1\oplus y_{n-1})\oplus\omega_n} \\
&= \sum_{\langle x\rangle_{n-1}} \hat{f}(\langle x\rangle_{n-1}, 0)(-1)^{\langle\omega\rangle_{n-1}\cdot\langle x\rangle_{n-1}} - \sum_{\langle y\rangle_{n-1}} \hat{f}(\langle y\rangle_{n-1}, 0)(-1)^{\langle\omega\rangle_{n-1}\cdot\langle y\rangle_{n-1}\oplus(\omega_1\oplus\cdots\oplus\omega_n)} \\
&= \begin{cases} 0 & \text{if } W(\omega) \text{ is even} \\ 2\displaystyle\sum_{\langle x\rangle_{n-1}} \hat{f}(\langle x\rangle_{n-1}, 0)(-1)^{\langle\omega\rangle_{n-1}\cdot\langle x\rangle_{n-1}} & \text{if } W(\omega) \text{ is odd.} \end{cases}
\end{aligned}$$

□

Lemma 8 Let $f \in \mathrm{D}_n$. Then,

$$C_f(a) = \begin{cases} 2C_{f|_{x_n=0}}(a_1, \ldots, a_{n-1}) & \text{if } a_n = 0 \\ -2C_{f|_{x_n=0}}(a_1 \oplus 1, \ldots, a_{n-1} \oplus 1) & \text{if } a_n = 1. \end{cases}$$

(Proof)

$$\begin{aligned} C_f(a) &= \frac{1}{2^n} \sum_{\omega} \hat{F}^2(\omega)(-1)^{\omega \cdot a} \\ &= \frac{1}{2^n} \left(\sum_{\langle \omega \rangle_{n-1}} \hat{F}^2(\langle \omega \rangle_{n-1}, 0)(-1)^{\langle \omega \rangle_{n-1} \cdot \langle a \rangle_{n-1}} + \sum_{\langle \omega \rangle_{n-1}} \hat{F}^2(\langle \omega \rangle_{n-1}, 1)(-1)^{\langle \omega \rangle_{n-1} \cdot \langle a \rangle_{n-1} \oplus a_n} \right). \end{aligned}$$

From Lemma 7,

$$\hat{F}(\langle \omega \rangle_{n-1}, 0) = \begin{cases} 0 & \text{if } W(\langle \omega \rangle_{n-1}) \text{ is even} \\ 2\hat{F}_0(\langle \omega \rangle_{n-1}) & \text{if } W(\langle \omega \rangle_{n-1}) \text{ is odd,} \end{cases}$$

$$\hat{F}(\langle \omega \rangle_{n-1}, 1) = \begin{cases} 2\hat{F}_0(\langle \omega \rangle_{n-1}) & \text{if } W(\langle \omega \rangle_{n-1}) \text{ is even} \\ 0 & \text{if } W(\langle \omega \rangle_{n-1}) \text{ is odd.} \end{cases}$$

Thus,

$$\begin{aligned} C_f(\langle a \rangle_{n-1}, 0) &= \frac{1}{2^n} \sum_{\langle \omega \rangle_{n-1}} \left(\hat{F}^2(\langle \omega \rangle_{n-1}, 0) + \hat{F}^2(\langle \omega \rangle_{n-1}, 1) \right) (-1)^{\langle \omega \rangle_{n-1} \cdot \langle a \rangle_{n-1}} \\ &= \frac{1}{2^{n-2}} \sum_{\langle \omega \rangle_{n-1}} \hat{F}_0^2(\langle \omega \rangle_{n-1})(-1)^{\langle \omega \rangle_{n-1} \cdot \langle a \rangle_{n-1}} \\ &= 2C_{f|_{x_n=0}}(a_1, \ldots, a_{n-1}). \end{aligned}$$

And,

$$\begin{aligned} C_f(\langle a \rangle_{n-1}, 1) &= \frac{1}{2^n} \sum_{\langle \omega \rangle_{n-1}} \left(\hat{F}^2(\langle \omega \rangle_{n-1}, 0) - \hat{F}^2(\langle \omega \rangle_{n-1}, 1) \right) (-1)^{\langle \omega \rangle_{n-1} \cdot \langle a \rangle_{n-1}} \\ &= \frac{1}{2^{n-2}} \sum_{\langle \omega \rangle_{n-1}} \hat{F}_0^2(\langle \omega \rangle_{n-1})(-1)^{\langle \omega \rangle_{n-1} \cdot \langle a \rangle_{n-1} \oplus (\omega_1 \oplus \cdots \oplus \omega_{n-1} \oplus 1)} \\ &= -\frac{1}{2^{n-2}} \sum_{\langle \omega \rangle_{n-1}} \hat{F}_0^2(\langle \omega \rangle_{n-1})(-1)^{\omega_1(a_1 \oplus 1) \oplus \cdots \oplus \omega_{n-1}(a_{n-1} \oplus 1)} \\ &= -2C_{f|_{x_n=0}}(a_1 \oplus 1, \ldots, a_{n-1} \oplus 1). \end{aligned}$$

□

The following results show that there exist self-dual Boolean functions satisfying the PC. The maximum degree of the PC of self-dual Boolean functions with an odd number of variables, however, is different from that of self-dual Boolean functions with an even number of variables.

First, Boolean functions with an odd number of variables are discussed. The following proposition gives a necessary and sufficient condition for Boolean functions with an odd number of variables satisfying the PC of maximum degree.

Proposition 8 Let $n \geq 3$ be odd and $f \in \mathrm{B}_n$. $f \in \mathrm{PC}_n(n-1)$ if and only if

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

□

It is shown in [HI95a], for every odd $n \geq 3$, that the number of Boolean functions in $\mathrm{PC}_n(n-1)$ is $2|\mathrm{PC}_{n-1}(n-1)|$, which is $\Omega(2^{2^{(n-1)/2}}2^{(n-1)/2}!)$[Rue91], and that, for the half of them, $\hat{F}(\omega) = 0$ for every ω such that $W(\omega)$ is even.

Theorem 6 Let $n \geq 3$ be odd and $f \in \mathrm{B}_n$. Then, $f \in \mathrm{PC}_n(n-1) \cap \mathrm{D}_n$ if and only if

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

(Proof) From Lemma 7 and Proposition 8, it is clear that

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

if $f \in \mathrm{PC}_n(n-1) \cap \mathrm{D}_n$.

If $f \in \mathrm{B}_n$ and

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

then, $f \in \mathrm{PC}_n(n-1)$ and

$$C_f(1,\ldots,1) = \frac{1}{2^n}\sum_{\omega}\hat{F}^2(\omega)(-1)^{\omega_1\oplus\cdots\oplus\omega_n} = 2\sum_{\omega, W(\omega) \text{ is odd}}(-1)^{\omega_1\oplus\cdots\oplus\omega_n} = -2^n.$$

Thus, from Proposition 7, $f \in \mathrm{D}_n$. □

Next, Boolean functions with an even number of variables is discussed. The following theorem indicates that, for every even $n \geq 2$, the degree of the PC of self-dual Boolean functions with n variables is at most $n/2-1$ and that there really exist self-dual Boolean functions with n variables satisfying the PC of degree $n/2-1$.

Corollary 4 Let $n \geq 3$ be odd. $\mathrm{PC}_n(n-1) \cap \mathrm{D}_n = \mathrm{PC}_n(n-1) \cap \{f \in \mathrm{B}_n \mid f \text{ is balanced}\}$. □

Theorem 7 Let $n \geq 2$ be even. Then,

1. $\mathrm{PC}_n(n/2) \cap \mathrm{D}_n = \emptyset$,
2. $\mathrm{PC}_n(n/2-1) \cap \mathrm{D}_n \neq \emptyset$.

(Proof) 1) Suppose that $f \in \mathrm{D}_n$. For $f|_{x_n=0} \in \mathrm{B}_{n-1}$, $C_{f|_{x_n=0}}(0,\ldots,0) \neq 0$. Since $f|_{x_n=0}$ does not satisfy the PC with respect to at least one element $(a_1,\ldots,a_{n-1}) \in \mathrm{V}_{n-1}$, $C_{f|_{x_n=0}}(a_1,\ldots,a_{n-1}) \neq 0$. Thus, from Lemma 8, $C_f(0,\ldots,0) \neq 0$, $C_f(1,\ldots,1) \neq 0$, and $C_f(a_1,\ldots,a_{n-1},0) \neq 0$, $C_f(a_1 \oplus 1,\ldots,a_{n-1}\oplus 1,1) \neq 0$, Let the Hamming weight of $(a_1,\ldots,a_{n-1})$ is k. Then, the Hamming weights of $(a_1,\ldots,a_{n-1},0)$ and $(a_1\oplus 1,\ldots,a_{n-1}\oplus 1,1)$ are k and $n-k$, respectively. Since $\min_{1\leq k\leq n-1}\max\{k,n-k\} = n/2$, f satisfies the PC of degree at most $n/2-1$.

2) Let $b = (b_1,\ldots,b_{n-1}) \in \{0,1\}^{n-1}$ and $b_i = 1$ if $1 \leq i \leq n/2$ and $b_i = 0$ if $n/2+1 \leq i \leq n-1$. Let $f \in \mathrm{D}_n$ and $f|_{x_n=0}$ satisfy the PC with respect to $\mathrm{V}_{n-1} - \{b\}$. Then, from Lemma 8, $C_f(a) \neq 0$ if and only if $a \in \{(0,\ldots,0),(1,\ldots,1),(b_1,\ldots,b_{n-1},0),(b_1\oplus 1,\ldots,b_{n-1}\oplus 1,1)\}$. Thus, $f \in \mathrm{PC}_n(n/2-1)$. □

6 Conclusion

This paper has discussed the relationships between the PC and each one of the unateness, the symmetry and the self-duality.

It has been presented that Boolean functions satisfying the PC of degree 2 are not unate in any one of its variables. This implies that the PC and the unateness are not compatible. The PC and the symmetry are not compatible, either, in the sense that there exist only four symmetric functions with a fixed number of variables that satisfy the PC of degree 2. The presented results on the unateness and the symmetry of Boolean functions satisfying the PC also show the difference between the PC of degree at most one and the PC of degree at least 2.

Relationships between the PC and the self-duality in this paper show a different behavior between Boolean functions with an even number of variables and those with an odd number of variables. There exist Boolean functions with an odd number of variables that satisfy the PC of maximum degree, while the degree of the PC of self-dual Boolean functions with an even number of variables is less than one half of the number of the variables.

One of the future works is to investigate the relationships between other nonlinearity criteria than the PC and each one of the unateness, the symmetry and the self-duality.

References

[HI95a] Hirose, S. and Ikeda, K., "Propagation characteristics of Boolean functions and their balancedness," IEICE Trans. Fundamentals, vol. E78–A, no. 1, pp. 11–18, 1995.

[HI95b] Hirose, S. and Ikeda, K., "Relationships among nonlinearity criteria of Boolean functions," IEICE Trans. Fundamentals, vol. E78–A, no. 2, pp. 235–243, 1995.

[Koh78] Kohavi, Z., Switching and finite automata theory, 2nd edition, Tata McGraw-Hill, 1978.

[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).