Research Article

Jing Zhang*, Yuan Li, and John O. Adeyeye

Sensitivities and block sensitivities of elementary symmetric Boolean functions

<https://doi.org/10.1515/jmc-2020-0042>

received October 10, 2020; accepted March 5, 2021

Abstract: Boolean functions have important applications in molecular regulatory networks, engineering, cryptography, information technology, and computer science. Symmetric Boolean functions have received a lot of attention in several decades. Sensitivity and block sensitivity are important complexity measures of Boolean functions. In this paper, we study the sensitivity of elementary symmetric Boolean functions and obtain many explicit formulas. We also obtain a formula for the block sensitivity of symmetric Boolean functions and discuss its applications in elementary symmetric Boolean functions.

Keywords: Boolean functions, Lucas theorem

MSC 2020: 05A05, 05A15

1 Introduction

In 1938, Shannon [28] recognized that symmetric functions had efficient switch network implementation. Since then, a lot of research has been carried out on symmetric or partially symmetric Boolean functions, and detection of symmetry has become important in logic synthesis, technology mapping, binary decision diagram minimization, and testing [1,10,22].

For the applications of symmetric Boolean functions in cryptography, Canteaut and Videau [3] presented an extensive study in 2005, and more results on (totally) symmetric Boolean functions can be found in other papers [2,5,8,17,21,23,27].

It is clear that any symmetric Boolean function can be written as a sum of some elementary symmetric Boolean functions. Hence, it is a fundamental question to have a comprehensive understanding about elementary symmetric Boolean functions. In ref. [8], the authors studied the balancedness of elementary symmetric Boolean functions and they proposed a conjecture which has received a lot of attention [4–6,8,9,13,14,31].

In ref. [7], Cook et al. introduced the definition of sensitivity as a combinatorial measure for Boolean functions by providing lower bounds on the time needed by CREW PRAM (Concurrent Read Exclusive Write, Parallel Random Access Machine). The concept was extended by Nisan [24] to block sensitivity. The study of sensitivity and block sensitivity of Boolean functions has been an active research topic for many years [11,12,16,18,19,25,26,29,30,32].

Recently, Huang proved the long standing Sensitivity Conjecture [15]: for any Boolean function f , $bs(f) \leq 2s(f)^4$, where $bs(f)$ is the block sensitivity of f and $s(f)$ is the sensitivity of f .

* **Corresponding author: Jing Zhang**, Mathematics Department, Governors State University, IL, 60484, USA, e-mail: jzhang@govst.edu

Yuan Li: Department of Mathematics, Winston-Salem State University, NC, 27110, USA, e-mail: liyu@wssu.edu

John O. Adeyeye: Department of Mathematics, Winston-Salem State University, NC, 27110, USA, e-mail: adeyeyej@wssu.edu

In Section 2 of this paper, we introduce the algebraic normal form (ANF) of Boolean functions and the definition of symmetric Boolean functions. In Section 3, we first recall definitions used in the paper, then obtain many explicit formulas of the sensitivities of elementary symmetric Boolean functions by using some elementary combinatorial results. The main idea of Section 3 is motivated by ref. [8,33]. In Section 4, we prove a formula for the block sensitivity of symmetric Boolean functions. Based on our knowledge, this is the first study about the block sensitivity of symmetric Boolean functions. We apply this formula to elementary symmetric Boolean functions and show that the block sensitivity can be strictly greater than the sensitivity for some elementary symmetric Boolean functions. The conclusion is included in Section 5.

2 Preliminaries

In this section, we introduce the definitions and notations. Let $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$. If $f: \mathbb{F}^n \rightarrow \mathbb{F}$ is a function with n variables and values in $\mathbb{F}$, it is well known [20] that f can be expressed as a polynomial, called the ANF:

$$f(x_1, \dots, x_n) = \bigoplus_{0 \leq k_i \leq 1, i=1, \dots, n} a_{k_1 \dots k_n} x_1^{k_1} \cdots x_n^{k_n},$$

where each coefficient $a_{k_1 \dots k_n} \in \mathbb{F}$. The symbol $\oplus$ stands for addition modulo 2. The number $k_1 + \dots + k_n$ is the multivariate degree of the term $a_{k_1 \dots k_n} x_1^{k_1} \cdots x_n^{k_n}$ with nonzero coefficient $a_{k_1 \dots k_n}$. The greatest degree of all the terms of f is called the algebraic degree, denoted by $\deg(f)$.

The number of non-zeros in $\mathbf{x} = (x_1, \dots, x_n)$, denoted by $W(\mathbf{x})$, is called the Hamming weight of $\mathbf{x}$.

Let S_n be the symmetric group of degree n , i.e., the set of all the permutations over the set $\{1, \dots, n\}$. If for any permutation $\pi \in S_n$,

$$f(x_1, \dots, x_n) = f(x_{\pi(1)}, \dots, x_{\pi(n)}),$$

then the function $f(x_1, \dots, x_n)$ is called a symmetric function. Obviously, the value of symmetric functions $f(x_1, \dots, x_n)$ depends only on the Hamming weight of $(x_1, \dots, x_n)$. In other words, $f(x_1, \dots, x_n)$ is symmetric if and only if

$$W(\mathbf{x}) = W(\mathbf{y}) \Rightarrow f(\mathbf{x}) = f(\mathbf{y}).$$

Let $v_k = f(\mathbf{x})$ with $W(\mathbf{x}) = k$, we call $v(f) = \langle v_0, \dots, v_n \rangle$ the value vector of $f(\mathbf{x})$. It is clear that there are 2^{n+1} symmetric Boolean functions.

3 Sensitivity of elementary symmetric Boolean functions

In this section, we calculate the sensitivities of elementary symmetric Boolean functions. More precisely, we present explicit formulas for the sensitivities of $X(d, n)$ when d is odd and $d = 2^k, 2^{k+t} \pm 2^t$. We show that $s(X(d, n))$ and $s(X(n-d, n))$ are computable for fixed d and that the explicit formulas of $s(X(d \times 2^k, n))$ can be obtained once we obtain the sequence $\left\{ \frac{1 - (-1)^{C(j,d)}}{2} \right\}_{j=0}^{\infty}$.

Definition 3.1. For integers n and d , $1 \leq d \leq n$, we define the elementary symmetric Boolean function by

$$X(d, n) = \bigoplus_{1 \leq i_1 < \dots < i_d \leq n} x_{i_1} \cdots x_{i_d}.$$

Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}^n$. We use $\mathbf{x}^i$ to denote the word obtained by flipping the i -th bit of $\mathbf{x}$.

Definition 3.2. [16,26] The sensitivity $s(f; \mathbf{x})$ of f at $\mathbf{x}$ is the number of indices i such that $f(\mathbf{x}) \neq f(\mathbf{x}^i)$. The sensitivity of f , denoted by $s(f)$, is $\max_{\mathbf{x}} s(f; \mathbf{x})$. The average sensitivity of f , denoted by $\bar{s}(f)$, is $\frac{1}{2^n} \sum_{\mathbf{x} \in \{0,1\}^n} s(f, \mathbf{x})$.

In the above definition,

$$s(f) = \max_{\mathbf{x}} s(f; \mathbf{x}) = \max_{\mathbf{x} \in \{0,1\}^n} s(f; \mathbf{x}).$$

Example 3.3. In Table 1, we list the sensitivities of $X(1, 3)$, $X(2, 3)$, and $X(3, 3)$ on every word. Their sensitivities are 3, 2, 3, respectively, and the average sensitivities are $3, \frac{3}{2}, \frac{3}{4}$, respectively.

Definition 3.4. The function $f(x_1, \dots, x_n)$ is essential in the variable x_i if there exist $r, s \in \mathbb{F}$ and $x_1^*, \dots, x_{i-1}^*, x_{i+1}^*, \dots, x_n^*$ such that

$$f(x_1^*, \dots, x_{i-1}^*, r, x_{i+1}^*, \dots, x_n^*) \neq f(x_1^*, \dots, x_{i-1}^*, s, x_{i+1}^*, \dots, x_n^*).$$

First, we will calculate the sensitivities and average sensitivities of $X(1, n)$ and $X(n, n)$.

Lemma 3.5. For every $\mathbf{x}$ in $\mathbb{F}^n$, $s(f; \mathbf{x}) = n$ is equivalent to $f(x_1, \dots, x_n) = x_1 \oplus \dots \oplus x_n \oplus a$, where $a \in \mathbb{F}$.

Proof. The sufficiency is obvious. We show the necessity in the following.

Since for every word $\mathbf{x}$ in $\mathbb{F}^n$, $s(f; \mathbf{x}) = n$, we know that every variable x_i is essential in f . If $\deg(f) > 1$, without loss of generality, we may assume that the term with degree $\deg(f)$ contains variable x_1 . Hence, we can write f as

$$f(x_1, \dots, x_n) = x_1 g(x_2, \dots, x_n) \oplus h(x_2, \dots, x_n),$$

where $\deg(g) = \deg(f) - 1 \geq 1$. Hence, function g is not a constant function. We can find $(b_2, \dots, b_n)$ such that $g(b_2, \dots, b_n) = 0$. Then, we have

$$f(1, b_2, \dots, b_n) = f(0, b_2, \dots, b_n) = h(b_2, \dots, b_n),$$

which means that the sensitivity of f over the word $(1, b_2, \dots, b_n)$ is at most $n - 1$. This contradiction shows $\deg(f) = 1$. Since every variable is essential, we have $f(x_1, \dots, x_n) = x_1 \oplus \dots \oplus x_n \oplus a$. For $a \in \mathbb{F}$. $\square$

From Lemma 3.5, we immediately have

Corollary 3.6. The sensitivity and average sensitivity of $X(1, n) = x_1 + \dots + x_n$ are both n . In other words, $s(X(1, n)) = \bar{s}(X(1, n)) = n$.

For the sensitivity of $X(n, n) = x_1 \cdots x_n$, we have $s(X(n, n), (1, \dots, 1)) = n$, $s(X(n, n), \mathbf{x}) = 1$ with $W(\mathbf{x}) = n - 1$ and $s(X(n, n), \mathbf{x}) = 0$ with $W(\mathbf{x}) \leq n - 2$. So we have

Proposition 3.7. The sensitivity of $X(n, n)$ is n , and the average sensitivity of $X(n, n)$ is $\frac{n}{2^{n-1}}$. In other words, $s(X(n, n)) = n$ and $\bar{s}(X(n, n)) = \frac{n}{2^{n-1}}$.

Table 1: Example 3.3, $s(X(1, 3)) = 3$, $s(X(2, 3)) = 2$, $s(X(3, 3)) = 3$

$\mathbf{x}$	$X(1, 3)(\mathbf{x})$	$s(X(1, 3), \mathbf{x})$	$X(2, 3)(\mathbf{x})$	$s(X(2, 3), \mathbf{x})$	$X(3, 3)(\mathbf{x})$	$s(X(3, 3), \mathbf{x})$
(0,0,0)	0	3	0	0	0	0
(0,0,1)	1	3	0	2	0	0
(0,1,0)	1	3	0	2	0	0
(0,1,1)	0	3	1	2	0	1
(1,0,0)	1	3	0	2	0	0
(1,0,1)	0	3	1	2	0	1
(1,1,0)	0	3	1	2	0	1
(1,1,1)	1	3	1	0	1	3

Remark 3.8. Function $X(n, n)$ is a nested canalizing function and the above proposition also appeared in [18, 19].

We need some lemmas to calculate the sensitivities of $X(d, n)$ for $2 \leq d \leq n - 1$.

Lemma 3.9. [33] Let $v(f) = \langle v_0, v_1, \dots, v_n \rangle$ be the value vector of symmetric Boolean function $f(\mathbf{x})$. If for some i , $(v_{i-1}, v_i, v_{i+1}) \in \{(0, 1, 0), (1, 0, 1)\}$, then the sensitivity of f is n . Otherwise, $s(f) = \max\{k + 1, n - k | v_k \neq v_{k+1}\}$.

Lemma 3.10. If $v_0 \neq v_1$ or $v_{n-1} \neq v_n$, then $s(f) = n$.

Proof. Because $v_0 \neq v_1$ implies $s(f, (0, \dots, 0)) = n$ and $v_{n-1} \neq v_n$ implies $s(f, (1, \dots, 1)) = n$, we have $s(f) = n$. $\square$

Let $C(n, k) = \frac{n!}{k!(n-k)!}$ if $0 \leq k \leq n$ and 0 otherwise, then we have

Lemma 3.11. [8] Let $X(d, n)(j)$ be the value of $X(d, n)$ when $\mathbf{x}$ has Hamming weight j , then

$$X(d, n)(j) = \frac{1 - (-1)^{C(j, d)}}{2}.$$

Lemma 3.12. (Lucas theorem) Let $n = a_m p^m + a_{m-1} p^{m-1} + \dots + a_1 p + a_0$ and $k = b_m p^m + b_{m-1} p^{m-1} + \dots + b_1 p + b_0$, where $a_i, b_i \in \mathbb{N}$, $0 \leq a_i \leq p - 1$, $0 \leq b_i \leq p - 1$, and p is a prime, then

$$C(n, k) \equiv C(a_m, b_m) \cdots C(a_1, b_1) \pmod{p}.$$

From the Lucas theorem, we immediately have

Lemma 3.13. For any prime p and natural number t , $C(n, k) \equiv C(p^t n, p^t k) \pmod{p}$. Particularly, we have $C(n, k) \equiv C(2^t n, 2^t k) \pmod{2}$.

Lemma 3.14. [3, 8] For any integer $k \geq 2$, the sequence $\{(-1)^{C(j, k)}\}_{j=0}^{\infty}$ is periodic and the least period is $2^{\lceil \log_2 k \rceil + 1}$.

By Lemmas 3.12 and 3.14, we get the following computing results.

Lemma 3.15. [8] If we write the infinite periodic string $a_1 a_2 \cdots a_k a_1 a_2 \cdots a_k \cdots$ as $\overline{a_1 a_2 \cdots a_k}$, then

$$\begin{aligned} \left\{ \frac{1 - (-1)^{C(j, 2)}}{2} \right\}_{j=0}^{\infty} &= \overline{0011} \\ \left\{ \frac{1 - (-1)^{C(j, 3)}}{2} \right\}_{j=0}^{\infty} &= \overline{0001} \\ \left\{ \frac{1 - (-1)^{C(j, 4)}}{2} \right\}_{j=0}^{\infty} &= \overline{00001111} \\ \left\{ \frac{1 - (-1)^{C(j, 5)}}{2} \right\}_{j=0}^{\infty} &= \overline{00000101} \\ \left\{ \frac{1 - (-1)^{C(j, 6)}}{2} \right\}_{j=0}^{\infty} &= \overline{00000011} \\ \left\{ \frac{1 - (-1)^{C(j, 7)}}{2} \right\}_{j=0}^{\infty} &= \overline{00000001} \\ \left\{ \frac{1 - (-1)^{C(j, 8)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000011111111} \\ \left\{ \frac{1 - (-1)^{C(j, 9)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000001010101} \\ \left\{ \frac{1 - (-1)^{C(j, 10)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000000110011} \end{aligned}$$

$$\begin{aligned}
\left\{ \frac{1 - (-1)^{C(j,11)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000000010001} \\
\left\{ \frac{1 - (-1)^{C(j,12)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000000001111} \\
\left\{ \frac{1 - (-1)^{C(j,13)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000000000101} \\
\left\{ \frac{1 - (-1)^{C(j,14)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000000000011} \\
\left\{ \frac{1 - (-1)^{C(j,15)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000000000001} \\
\left\{ \frac{1 - (-1)^{C(j,16)}}{2} \right\}_{j=0}^{\infty} &= \overline{00000000000000001111111111111111} \\
\left\{ \frac{1 - (-1)^{C(j,17)}}{2} \right\}_{j=0}^{\infty} &= \overline{000000000000000001010101010101} \\
\left\{ \frac{1 - (-1)^{C(j,18)}}{2} \right\}_{j=0}^{\infty} &= \overline{00000000000000000011001100110011} \\
\left\{ \frac{1 - (-1)^{C(j,19)}}{2} \right\}_{j=0}^{\infty} &= \overline{00000000000000000001000100010001} \\
\left\{ \frac{1 - (-1)^{C(j,20)}}{2} \right\}_{j=0}^{\infty} &= \overline{00000000000000000000111100001111}.
\end{aligned}$$

Using Lemma 3.12 for $p = 2$ and Lemma 3.14, a straightforward calculation shows

Lemma 3.16. When $d = 2^k$, $k \in \mathbb{N}$, we have

$$\left\{ \frac{1 - (-1)^{C(j,d)}}{2} \right\}_{j=0}^{\infty} = \left\{ \frac{1 - (-1)^{C(j,2^k)}}{2} \right\}_{j=0}^{\infty} = \overbrace{0 \cdots 0}^{2^k} \overbrace{1 \cdots 1}^{2^k}.$$

We first consider the sensitivities of $X(d, n)$ for odd d .

Theorem 3.17. For $d = 1, 3, 5, \dots, 2 \left\lfloor \frac{n-1}{2} \right\rfloor + 1$, the sensitivity of $X(d, n)$ is n :

$$s(X(d, n)) = n.$$

Proof. If n is odd, we already know $s(X(n, n)) = n$. For $0 < d < n$ and d odd, we have

$$X(d, n)(d-1) = v_{d-1} = \frac{1 - (-1)^{C(d-1,d)}}{2} = 0,$$

$$X(d, n)(d) = v_d = \frac{1 - (-1)^{C(d,d)}}{2} = 1,$$

and

$$X(d, n)(d+1) = v_{d+1} = \frac{1 - (-1)^{C(d+1,d)}}{2} = 0.$$

Hence, $(v_{d-1}, v_d, v_{d+1}) = (0, 1, 0)$ and by Lemma 3.9, we have

$$s(X(d, n)) = n. \quad \square$$

In order to compute the sensitivities of $X(d, n)$ for even d , we need to improve Lemma 3.9.

Lemma 3.18. Let $v(f) = \langle v_0, \dots, v_n \rangle$ be the value vector of $X(d, n)$ for even d , $k_{\min} = \min\{k | v_k \neq v_{k+1}\}$ and $k_{\max} = \max\{k | v_k \neq v_{k+1}\}$, then $s(X(d, n)) = \max\{k_{\max} + 1, n - k_{\min}\}$.

Proof. We first show that there is no i such that $(v_{i-1}, v_i, v_{i+1}) \in \{(0, 1, 0), (1, 0, 1)\}$.

Let $d = 2k$, $k \in \mathbb{N}$, we have

$$(i - 2k)C(i, 2k) = iC(i - 1, 2k), \quad (3.1)$$

$$(i + 1 - 2k)C(i + 1, 2k) = (i + 1)C(i, 2k). \quad (3.2)$$

Case 1. If there exists i such that

$$(v_{i-1}, v_i, v_{i+1}) = \left(\frac{1 - (-1)^{C(i-1, 2k)}}{2}, \frac{1 - (-1)^{C(i, 2k)}}{2}, \frac{1 - (-1)^{C(i+1, 2k)}}{2} \right) = (0, 1, 0),$$

then $2|C(i - 1, 2k)$, $2 \nmid C(i, 2k)$, and $2|C(i + 1, 2k)$. By equation (3.1), $2|(i - 2k)$, hence $2|i$. But by equation (3.2), $2|(i + 1)$, which is a contradiction.

Case 2. If there exists i such that

$$(v_{i-1}, v_i, v_{i+1}) = \left(\frac{1 - (-1)^{C(i-1, 2k)}}{2}, \frac{1 - (-1)^{C(i, 2k)}}{2}, \frac{1 - (-1)^{C(i+1, 2k)}}{2} \right) = (1, 0, 1),$$

then $2 \nmid C(i - 1, 2k)$, $2|C(i, 2k)$ and $2 \nmid C(i + 1, 2k)$. By equation (3.1), $2|i$. Again by equation (3.2), $2|(i + 1 - 2k)$ and $2|(i + 1)$, we receive a contradiction.

We show that there is no i such that

$$(v_{i-1}, v_i, v_{i+1}) \in \{(0, 1, 0), (1, 0, 1)\}.$$

On the other hand, let

$$\{k | v_k \neq v_{k+1}\} = \{k_{\min} = k_1, k_2, \dots, k_t = k_{\max}\}$$

with $k_1 < k_2 < \dots < k_t$. Since $s(X(d, n)) = \max\{k + 1, n - k | v_k \neq v_{k+1}\}$, we have

$$s(X(d, n)) = \max\{k_1 + 1, n - k_1, k_2 + 1, n - k_2, \dots, k_t + 1, n - k_t\} = \max\{k_{\max} + 1, n - k_{\min}\}. \quad \square$$

To simplify the notation, sometimes, we write the value vector $\langle v_0, \dots, v_n \rangle$ as $\langle v_0 \dots v_n \rangle$ and word $(x_1, \dots, x_n)$ as $(x_1 \dots x_n)$.

Theorem 3.19. For $n \geq 2^k$, $k \in \mathbb{N}$, the sensitivity of $X(2^k, n)$ is

$$s(X(2^k, n)) = 2^k \left\lfloor \frac{n}{2^k} \right\rfloor.$$

Proof. By Lemma 3.16, the value vector is the first $n + 1$ numbers of the sequence

$$\left\{ \frac{1 - (-1)^{C(j, d)}}{2} \right\}_{j=0}^{\infty} = \left\{ \frac{1 - (-1)^{C(j, 2^k)}}{2} \right\}_{j=0}^{\infty} = \overbrace{0 \dots 0}^{2^k} \overbrace{1 \dots 1}^{2^k}.$$

Let $n = 2^k q + r$, $0 \leq r \leq 2^k - 1$, $k \in \mathbb{N}$.

When q is even, we have

$$\langle v_0 \dots v_n \rangle = \langle \overbrace{0 \dots 0}^{2^k} \overbrace{1 \dots 1}^{2^k} \dots \overbrace{0 \dots 0}^{2^k} \overbrace{1 \dots 1}^{2^k} \overbrace{10 \dots 0}^{r+1} \rangle.$$

It is clear that $k_{\min} = 2^k - 1$ and $k_{\max} = 2^k q - 1$. By Lemma 3.18, we have

$$s(X(2^k, n)) = \max\{k_{\max} + 1, n - k_{\min}\} = \max\{2^k q, n - 2^k + 1\} = \max\{2^k q, 2^k(q - 1) + r + 1\} = 2^k q = 2^k \left\lfloor \frac{n}{2^k} \right\rfloor.$$

When q is odd, we have $\langle v_0 \cdots v_n \rangle = \langle \overbrace{0 \cdots 0}^{2^k} \overbrace{1 \cdots 1}^{2^k} \cdots \overbrace{0 \cdots 0}^{2^k} \overbrace{1 \cdots 1}^{r+1} \rangle$. The calculation is identical to the case when q is even. We are done. $\square$

A bound for the sensitivities of elementary symmetric Boolean functions can be received by Lemma 3.18.

Proposition 3.20. For any $1 \leq d \leq n$, $d \in \mathbb{N}$, we have $\left\lfloor \frac{n+1}{2} \right\rfloor \leq s(X(d, n)) \leq n$.

Proof. First, we have $s(X(d, n)) \leq n$ by definition. From Lemma 3.18, for even d , we have

$$s(X(d, n)) = \max\{k_{\max} + 1, n - k_{\min}\} \geq \max\{k_{\min} + 1, n - k_{\min}\} \geq \left\lfloor \frac{n+1}{2} \right\rfloor.$$

By Theorem 3.17, $s(X(d, n)) = n$ for odd d , we are done. $\square$

Remark 3.21. The upper bound in the Proposition 3.20 is tight. In Theorem 3.19, let $n = 2^{k+1} - 1$, then $s(X(2^k, n)) = \left\lfloor \frac{n+1}{2} \right\rfloor$. It shows that the lower bound can also be reached sometimes.

To understand and prove more general formulas, we will first calculate the sensitivities of $X(d, n)$ for some small even d . The same techniques will be used to obtain more general formulas later.

Lemma 3.22. For $n \geq 6$, the sensitivity of $X(6, n)$ is

$$s(X(6, n)) = \begin{cases} 8 \left\lfloor \frac{n}{8} \right\rfloor, & n = 8q + r, \ 0 \leq r \leq 5 \\ n, & n = 8q + 6 \\ n - 1, & n = 8q + 7. \end{cases}$$

Proof. By Lemma 3.15, the value vector $\langle v_0 \cdots v_n \rangle$ is the first $n + 1$ number of $\left\{ \frac{1 - (-1)^{C(j,6)}}{2} \right\}_{j=0}^{\infty} = \overline{00000011}$.

When $n = 8q + 6$, the value vector $\langle v_0 \cdots v_n \rangle$ ends with 01. By Lemma 3.10, $s(X(6, n)) = n$.

When $n = 8q + 7$, the value vector $\langle v_0 \cdots v_n \rangle$ is

$$\langle \overbrace{00000011}^8 \cdots \overbrace{00000011}^8 \rangle.$$

Since $k_{\min} = 5$ and $k_{\max} = n - 2$, we have $s(X(6, n)) = \max\{n - 2 + 1, n - 5\} = n - 1$.

When $n = 8q + r$, $0 \leq r \leq 5$,

$$\langle v_0 \cdots v_n \rangle = \langle \overbrace{00000011}^8 \cdots \overbrace{00000011}^8 \overbrace{0 \cdots 0}^{r+1} \rangle.$$

Since $k_{\min} = 5$ and $k_{\max} = 8q - 1$, we have

$$s(X(6, n)) = \max\{8q - 1 + 1, n - 5\} = \max\{8q, 8q + r - 5\} = 8q = 8 \left\lfloor \frac{n}{8} \right\rfloor. \quad \square$$

For $d = 10$, we have

Lemma 3.23. For $n \geq 10$, the sensitivity of $X(10, n)$ is

$$s(X(10, n)) = \begin{cases} 16 \left\lfloor \frac{n}{16} \right\rfloor, & n = 16q + r, \ 0 \leq r \leq 9 \\ n, & n = 16q + 10, \ 16q + 12, \ 16q + 14 \\ n - 1, & n = 16q + 11, \ 16q + 13, \ 16q + 15. \end{cases}$$

Proof. By Lemma 3.15, the value vector $\langle v_0 \cdots v_n \rangle$ is the first $n + 1$ number of $\left\{ \frac{1 - (-1)^{C(j,10)}}{2} \right\}_{j=0}^{\infty} = \overline{0000000000110011}$.

When $n = 16q + 10$, $16q + 12$, $16q + 14$, the value vectors $\langle v_0 \cdots v_n \rangle$ end with 01, 10, and 01, respectively. By Lemma 3.10, $s(X(10, n)) = n$.

When $n = 16q + 11$, $16q + 13$, $16q + 15$, the value vectors $\langle v_0 \cdots v_n \rangle$ are

$$\begin{aligned} & \overbrace{\langle \overbrace{0000000000110011}^{16} \cdots \overbrace{0000000000110011}^{16} \overbrace{000000000011}^{12} \rangle}^q, \\ & \overbrace{\langle \overbrace{0000000000110011}^{16} \cdots \overbrace{0000000000110011}^{16} \overbrace{00000000001100}^{14} \rangle}^q, \end{aligned}$$

and

$$\overbrace{\langle \overbrace{0000000000110011}^{16} \cdots \overbrace{0000000000110011}^{16} \rangle}^{q+1},$$

respectively. In any case, we always have $k_{\min} = 10$ and $k_{\max} = n - 2$, so

$$s(X(10, n)) = \max\{n - 2 + 1, n - 10\} = n - 1.$$

When $n = 16q + r$, $0 \leq r \leq 9$, the value vector $\langle v_0 \cdots v_n \rangle$ is

$$\overbrace{\langle \overbrace{0000000000110011}^{16} \cdots \overbrace{0000000000110011}^{16} \overbrace{0 \cdots 0}^{r+1} \rangle}^q.$$

Since $k_{\min} = 9$ and $k_{\max} = 16q - 1$,

$$s(X(10, n)) = \max\{16q - 1 + 1, n - 9\} = \max\{16q, 16q + r - 9\} = 16q = 16 \left\lfloor \frac{n}{16} \right\rfloor. \quad \square$$

For $d = 12$, we have

Lemma 3.24. For $n \geq 12$, the sensitivity of $X(12, n)$ is

$$s(X(12, n)) = \begin{cases} 16 \left\lfloor \frac{n}{16} \right\rfloor, & n = 16q + r, \quad 0 \leq r \leq 11 \\ 16 \left\lfloor \frac{n}{16} \right\rfloor + 12, & n = 16q + r, \quad 12 \leq r \leq 15. \end{cases}$$

Proof. By Lemma 3.15, the value vector $\langle v_0 \cdots v_n \rangle$ is the first $n + 1$ number of $\left\{ \frac{1 - (-1)^{C(j,12)}}{2} \right\}_{j=0}^{\infty} = \overline{0000000000001111}$.

When $n = 16q + r$, $0 \leq r \leq 11$, the value vectors $\langle v_0 \cdots v_n \rangle$ are

$$\overbrace{\langle \overbrace{0000000000001111}^{16} \cdots \overbrace{0000000000001111}^{16} \overbrace{0 \cdots 0}^{r+1} \rangle}^q.$$

We have $k_{\min} = 11$ and $k_{\max} = 16q - 1$, so

$$s(X(12, n)) = \max\{16q + r - 11, 16q\} = 16q = 16 \left\lfloor \frac{n}{16} \right\rfloor.$$

When $n = 16q + r$, $12 \leq r \leq 15$, the value vectors $\langle v_0 \cdots v_n \rangle$ are

$$\overbrace{\langle \overbrace{0000000000001111}^{16} \cdots \overbrace{0000000000001111}^{16} \overbrace{0 \cdots 01 \cdots 1}^{12 \quad r-11} \rangle}^q.$$

Since $k_{\min} = 11$ and $k_{\max} = 16q + 11$, we have

$$s(X(12, n)) = \max\{16q + 12, n - 11\} = \max\{16q + 12, 16q + r - 11\} = 16q + 12 = 16 \left\lfloor \frac{n}{16} \right\rfloor + 12. \quad \square$$

It is clear that one can continue to compute the explicit formulas of $X(d, n)$ for fixed d . In the following, we will consider the situation that d is very close to n . We already know $s(X(n, n)) = n$.

Lemma 3.25. *Let $n \geq 3$, then $s(X(n - 1, n)) = 2 \left\lfloor \frac{n}{2} \right\rfloor$.*

Proof. Since

$$X(n - 1, n) = x_2 \cdots x_n \oplus x_1 x_3 \cdots x_n \oplus \cdots \oplus x_1 \cdots x_{n-1},$$

obviously, $X(n - 1, n)(j) = 0$ for $j = 0, 1, \dots, n - 2$, $X(n - 1, n)(n - 1) = 1$, and $X(n - 1, n)(n) = \frac{1 - (-1)^n}{2}$. The value vector $\langle v_0, \dots, v_n \rangle$ is $\left\langle 0, \dots, 0, 1, \frac{1 - (-1)^n}{2} \right\rangle$. The result follows from Lemmas 3.9 and 3.18. $\square$

Lemma 3.26. *For $n \geq 5$, the sensitivity of $X(n - 2, n)$ is*

$$s(X(n - 2, n)) = \begin{cases} n, & n = 4q, 4q + 1, 4q + 3 \\ n - 2, & n = 4q + 2. \end{cases}$$

Proof. By Lemma 3.11, the value vector is

$$\langle v_0, \dots, v_n \rangle = \left\langle 0, \dots, 0, 1, \frac{1 - (-1)^{n-1}}{2}, \frac{1 - (-1)^{\frac{n(n-1)}{2}}}{2} \right\rangle.$$

Case 1: $n = 4q + 0$, $\langle v_0, \dots, v_n \rangle = \langle 0, \dots, 0, 1, 1, 0 \rangle$.

Case 2: $n = 4q + 1$, $\langle v_0, \dots, v_n \rangle = \langle 0, \dots, 0, 1, 0, 0 \rangle$.

Case 3: $n = 4q + 2$, $\langle v_0, \dots, v_n \rangle = \langle 0, \dots, 0, 1, 1, 1 \rangle$.

Case 4: $n = 4q + 3$, $\langle v_0, \dots, v_n \rangle = \langle 0, \dots, 0, 1, 0, 1 \rangle$.

By Lemmas 3.9, 3.10, and 3.18, the formula of the sensitivity is obtained. $\square$

It is clear that one can continue to calculate the explicit sensitivity formulas of $X(n - d, n)$ for $d = 3, 4, \dots$

Now we will discuss more properties of the sequence $\left\{ \frac{1 - (-1)^{C(j, d)}}{2} \right\}_{j=0}^{\infty}$ and generalize the above results.

Proposition 3.27. *If $\left\{ \frac{1 - (-1)^{C(j, d)}}{2} \right\}_{j=0}^{\infty} = \overline{a_0 a_1 \cdots a_{m-1}}$, then*

$$\left\{ \frac{1 - (-1)^{C(j, 2d)}}{2} \right\}_{j=0}^{\infty} = \overline{a_0 a_0 a_1 a_1 \cdots a_{m-1} a_{m-1}}.$$

Proof. By Lemma 3.14, if the least period of $\left\{ \frac{1 - (-1)^{C(j, d)}}{2} \right\}_{j=0}^{\infty} = \overline{a_0 a_1 \cdots a_{m-1}}$ is $m = 2^{\lfloor \log_2 d \rfloor + 1}$, then the least period of $\left\{ \frac{1 - (-1)^{C(j, 2d)}}{2} \right\}_{j=0}^{\infty}$ is $2m$. Hence, we may assume

$$\left\{ \frac{1 - (-1)^{C(j, 2d)}}{2} \right\}_{j=0}^{\infty} = \overline{b_0 b_1 \cdots b_{2m-1}}.$$

We only need to show $b_{2j} = b_{2j+1} = a_j$ for $j = 0, \dots, m - 1$.

For all $j = 0, 1, 2, \dots$, since $a_j \equiv C(j, d) \pmod{2}$ and $b_{2j} \equiv C(2j, 2d) \pmod{2}$, it is clear that $C(j, d) \equiv C(2j, 2d) \pmod{2}$ by Lemma 3.13. So $a_j = b_{2j}$. On the other hand, from

$$C(2j + 1, 2d) = C(2j, 2d) + C(2j, 2d - 1)$$

and

$$(2d - 1)C(2j, 2d - 1) = 2jC(2j - 1, 2d - 2),$$

we have $2|C(2j, 2d - 1)$. Therefore,

$$b_{2j+1} \equiv C(2j + 1, 2d) = C(2j, 2d) + C(2j, 2d - 1) \equiv C(2j, 2d) \equiv b_{2j} \pmod{2},$$

and $b_{2j+1} = b_{2j}$. □

By a direct calculation and Lemma 3.14, we have

Lemma 3.28. For $d = 2^k - 1$, $\left\{ \frac{1 - (-1)^{C(j,d)}}{2} \right\}_{j=0}^{\infty} = \overbrace{0 \cdots 01}^{2^k}$.

From Proposition 3.27 and Lemma 3.28, we have

Lemma 3.29. For $k \geq 2$, $d = 2^{k+1} - 2$, $2^{k+2} - 4, \dots, 2^{k+t} - 2^t$, and $t \geq 1$, we have

$$\begin{aligned} \left\{ \frac{1 - (-1)^{C(j, 2^{k+1}-2)}}{2} \right\}_{j=0}^{\infty} &= \overbrace{0 \cdots 011}^{2^{k+1}}, \\ \left\{ \frac{1 - (-1)^{C(j, 2^{k+2}-4)}}{2} \right\}_{j=0}^{\infty} &= \overbrace{0 \cdots 01111}^{2^{k+2}}, \\ &\dots, \\ \left\{ \frac{1 - (-1)^{C(j, 2^{k+t}-2^t)}}{2} \right\}_{j=0}^{\infty} &= \overbrace{0 \cdots 01 \cdots 1}^{2^{k+t}}. \end{aligned}$$

Theorem 3.30. For $k \geq 2$, $t \geq 1$, $d = 2^{k+t} - 2^t$, and $n \geq d$, the sensitivity of $X(d, n)$ is

$$s(X(2^{k+t} - 2^t, n)) = \begin{cases} 2^{k+t} \left\lfloor \frac{n}{2^{k+t}} \right\rfloor, & n = 2^{k+t}q + r, \quad 0 \leq r \leq 2^{k+t} - 2^t - 1 \\ 2^{k+t} \left\lfloor \frac{n}{2^{k+t}} \right\rfloor + 2^{k+t} - 2^t, & n = 2^{k+t}q + r, \quad 2^{k+t} - 2^t \leq r \leq 2^{k+t} - 1. \end{cases}$$

Proof. By Lemma 3.29, the value vector $\langle v_0 \cdots v_n \rangle$ is the first $n + 1$ number of $\left\{ \frac{1 - (-1)^{C(j, 2^{k+t}-2^t)}}{2} \right\}_{j=0}^{\infty} = \overbrace{0 \cdots 01 \cdots 1}^{2^{k+t}}$.

When $n = 2^{k+t}q + r$, $0 \leq r \leq 2^{k+t} - 2^t - 1$, the value vector is

$$\overbrace{\overbrace{0 \cdots 01 \cdots 1}^{2^t} \cdots \overbrace{0 \cdots 01 \cdots 1}^{2^t} 0 \cdots 0}^q.$$

Since $k_{\min} = 2^{k+t} - 2^t - 1$ and $k_{\max} = 2^{k+t}q - 1$, we have

$$\begin{aligned} s(X(2^{k+t} - 2^t, n)) &= \max\{2^{k+t}q - 1 + 1, n - 2^{k+t} + 2^t + 1\} \\ &= \max\{2^{k+t}q, 2^{k+t}(q - 1) + r + 2^t + 1\} \\ &= 2^{k+t}q = 2^{k+t} \left\lfloor \frac{n}{2^{k+t}} \right\rfloor. \end{aligned}$$

When $n = 2^{k+t}q + r$, $2^{k+t} - 2^t \leq r \leq 2^{k+t} - 1$, the value vector $\langle v_0 \cdots v_n \rangle$ is

$$\overbrace{\overbrace{0 \cdots 01 \cdots 1}^{2^t} \cdots \overbrace{0 \cdots 01 \cdots 1}^{2^t} 0 \cdots 01 \cdots 1}^q.$$

From $k_{\min} = 2^{k+t} - 2^t - 1$ and $k_{\max} = 2^{k+t}q + 2^{k+t} - 2^t - 1$, we have

$$\begin{aligned} s(X(2^{k+t} - 2^t, n)) &= \max\{2^{k+t}q + 2^{k+t} - 2^t, n - 2^{k+t} + 2^t + 1\} \\ &= 2^{k+t}q + 2^{k+t} - 2^t = 2^{k+t} \left\lfloor \frac{n}{2^{k+t}} \right\rfloor + 2^{k+t} - 2^t. \end{aligned}$$

□

Lemma 3.31. If $d = 2^k + 1$, $k \in \mathbb{N}$, then

$$\left\{ \frac{1 - (-1)^{C(j,d)}}{2} \right\}_{j=0}^{\infty} = \left\{ \frac{1 - (-1)^{C(j,2^k+1)}}{2} \right\}_{j=0}^{\infty} = \overbrace{0 \cdots 0}^{2^k} \overbrace{0101 \cdots 01}^{2^k}.$$

Proof. First, it is clear that $C(j, 2^k + 1) = 0$ for $j = 0, 1, \dots, 2^k - 1$. It is straight-forward to check $C(2^k + 2j, 2^k + 1)$ is even for $j = 0, 1, \dots, 2^{k-1} - 1$ (generally, $C(R, S)$ is even for even R and odd S). We only need to show that $C(2^k + 2j + 1, 2^k + 1)$ is odd for $j = 0, 1, \dots, 2^{k-1} - 1$.

Let $2j = c_r 2^r + \cdots + c_1 2$. Then $2^k + 2j + 1 = 2^k + c_r 2^r + \cdots + c_1 2 + 1$. By the Lucas theorem,

$$C(2^k + 2j + 1, 2^k + 1) \equiv C(1, 1)C(c_r, 0) \cdots C(c_1, 0)C(1, 1) \equiv 1 \pmod{2}.$$

We are done since the least period of $\left\{ \frac{1 - (-1)^{C(j,2^k+1)}}{2} \right\}_{j=0}^{\infty}$ is $2^{\lfloor \log_2(2^k+1) \rfloor + 1} = 2^{k+1}$ by Lemma 3.14. □

From Proposition 3.27 and Lemma 3.31, we have

Lemma 3.32. For $k \geq 1$, $d = 2^{k+1} + 2, 2^{k+2} + 4, \dots, 2^{k+t} + 2^t$, and $t \geq 1$, we have

$$\begin{aligned} \left\{ \frac{1 - (-1)^{C(j,2^{k+1}+2)}}{2} \right\}_{j=0}^{\infty} &= \overbrace{0 \cdots 0}^{2^{k+1}} \overbrace{0011 \cdots 0011}^{2^{k+1}}, \\ \left\{ \frac{1 - (-1)^{C(j,2^{k+2}+4)}}{2} \right\}_{j=0}^{\infty} &= \overbrace{0 \cdots 0}^{2^{k+2}} \overbrace{00001111 \cdots 00001111}^{2^{k+2}}, \\ &\dots, \\ \left\{ \frac{1 - (-1)^{C(j,2^{k+t}+2^t)}}{2} \right\}_{j=0}^{\infty} &= \overbrace{0 \cdots 0}^{2^{k+t}} \underbrace{\overbrace{0 \cdots 0}^{2^t} \overbrace{1 \cdots 1}^{2^t} \cdots \overbrace{0 \cdots 0}^{2^t} \overbrace{1 \cdots 1}^{2^t}}_{2^k}. \end{aligned}$$

Theorem 3.33. Let $k, t \in \mathbb{N}$, $d = 2^{k+t} + 2^t$, and $n \geq d$.

If $n = 2^{k+t+1}q + r$, $0 \leq r \leq 2^{k+t} + 2^t - 1$, then

$$s(X(2^{k+t} + 2^t, n)) = 2^{k+t+1} \left\lfloor \frac{n}{2^{k+t+1}} \right\rfloor.$$

If $n = 2^{k+t+1}q + 2^{k+t} + (j+1)2^t + i$, $0 \leq j \leq 2^k - 2$, $0 \leq i \leq 2^t - 1$, then

$$s(X(2^{k+t} + 2^t, n)) = 2^{k+t+1} \left\lfloor \frac{n}{2^{k+t+1}} \right\rfloor + 2^{k+t} + (j+1)2^t.$$

Proof. By Lemma 3.32, the value vector $\langle v_0 \cdots v_n \rangle$ is the first $n+1$ number of

$$\left\{ \frac{1 - (-1)^{C(j,2^{k+t}+2^t)}}{2} \right\}_{j=0}^{\infty} = \overbrace{0 \cdots 0}^{2^{k+t}} \underbrace{\overbrace{0 \cdots 0}^{2^t} \overbrace{1 \cdots 1}^{2^t} \cdots \overbrace{0 \cdots 0}^{2^t} \overbrace{1 \cdots 1}^{2^t}}_{2^k} = \overline{B}.$$

Let $n = 2^{k+t+1}q + r$, $0 \leq r \leq 2^{k+t+1} - 1$.

Case 1. $n = 2^{k+t+1}q + r$, $0 \leq r \leq 2^{k+t} + 2^t - 1$.

The value vector of $X(2^{k+t} + 2^t, n)$ is

$$\langle \overbrace{B \cdots B}^q \overbrace{0 \cdots 0}^{r+1} \rangle.$$

Since $k_{\min} = 2^{k+t} + 2^t - 1$ and $k_{\max} = 2^{k+t+1}q - 1$, we have

$$\begin{aligned} s(X(2^{k+t} + 2^t, n)) &= \max\{n - k_{\min}, k_{\max} + 1\} \\ &= \max\{2^{k+t+1}q + r - 2^{k+t} - 2^t + 1, 2^{k+t+1}q\} \\ &= 2^{k+t+1}q = 2^{k+t+1} \left\lfloor \frac{n}{2^{k+t+1}} \right\rfloor. \end{aligned}$$

Case 2. $n = 2^{k+t+1}q + r$, $2^{k+t} + 2^t \leq r \leq 2^{k+t+1} - 1$.

Let $l = r - 2^{k+t} - 2^t$, $0 \leq l \leq 2^{k+t+1} - 2^{k+t} - 2^t - 1$, $l = 2^t j + i$, $0 \leq j \leq 2^k - 2$, $0 \leq i \leq 2^t - 1$.

When $n = 2^{k+t+1}q + 2^{k+t} + 2^t + 2^t j + i$, j is even, the value vector is

$$\langle \overbrace{B \cdots B}^q \overbrace{0 \cdots 0}^{2^{k+t}} \overbrace{0 \cdots 0}^{2^t} \overbrace{1 \cdots 1}^{2^t} \overbrace{0 \cdots 0}^{2^t} \cdots \overbrace{1 \cdots 1}^{2^t} \overbrace{0 \cdots 0}^{2^t} \overbrace{1 \cdots 1}^{i+1} \rangle.$$

From $k_{\min} = 2^{k+t} + 2^t - 1$ and $k_{\max} = 2^{k+t+1}q + 2^{k+t} + 2^t + 2^t j - 1$, we have

$$\begin{aligned} s(X(2^{k+t} + 2^t, n)) &= \max\{n - k_{\min}, k_{\max} + 1\} \\ &= \max\{2^{k+t+1}q + 2^t j + i + 1, 2^{k+t+1}q + 2^{k+t} + 2^t + 2^t j\} \\ &= 2^{k+t+1}q + 2^{k+t} + 2^t(j + 1) \\ &= 2^{k+t+1} \left\lfloor \frac{n}{2^{k+t+1}} \right\rfloor + 2^{k+t} + (j + 1)2^t. \end{aligned}$$

When $n = 2^{k+t+1}q + 2^{k+t} + 2^t + 2^t j + i$, j is odd, the value vector is

$$\langle \overbrace{B \cdots B}^q \overbrace{0 \cdots 0}^{2^{k+t}} \overbrace{0 \cdots 0}^{2^t} \overbrace{1 \cdots 1}^{2^t} \overbrace{0 \cdots 0}^{2^t} \cdots \overbrace{1 \cdots 1}^{2^t} \overbrace{0 \cdots 0}^{2^t} \overbrace{0 \cdots 0}^{i+1} \rangle.$$

The calculation is identical to the case of even j . The theorem is proved. $\square$

Example 3.34. In Theorem 3.30, if $k = 2$, $t = 1$, then $d = 6$. If $k = 2$, $t = 2$, then $d = 12$.

In Theorem 3.33, if $k = 1$, $t = 1$, then $d = 6$. If $k = 2$, $t = 1$, then $d = 10$. If $k = 1$, $t = 2$, then $d = 12$. One can check that these results are consistent with the previous lemmas.

If $\left\{ \frac{1 - (-1)^{C(j,d)}}{2} \right\}_{j=0}^{\infty}$ for an odd d can be calculated, then one can find the sequence

$$\left\{ \frac{1 - (-1)^{C(j,2^k d)}}{2} \right\}_{j=0}^{\infty}$$

by Proposition 3.27. Hence, the explicit formula of $s(X(2^k d, n))$ can be obtained.

Let $A = \{2^{k+t} - 2^t | k \geq 2, t \geq 1\}$, $B = \{2^{k+t} + 2^t | k \geq 1, t \geq 1\}$, and $C = \{2^k | k \geq 1\}$. For A, B, C , any set is not contained in the other set. It is easy to check that

$$A \cap B = \{2^{i+2} - 2^i = 2^{i+1} + 2^i | i \geq 1\} = \{3 \times 2^i | i \geq 1\}$$

and

$$A \cup B \cup C$$

$$= \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 24, 28, 30, 32, 34, 36, 40, 48, 56, 60, 62, 64, 66, 68, 72, 80, 96, 124, \dots\}.$$

4 The block sensitivities of symmetric Boolean functions

In this section, we will obtain a formula for the block sensitivity of symmetric Boolean function based on its value vector.

Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}^n$, $[n] = \{1, \dots, n\}$. For any subset S of $[n]$, we form $\mathbf{x}^S$ by complementing those bits in $\mathbf{x}$ indexed by elements of S .

Definition 4.1. [24] The block sensitivity $bs(f; \mathbf{x})$ of f at $\mathbf{x}$ is the maximum number of disjoint subsets $B_1, \dots, B_r$ of $[n]$ such that for all j , $f(\mathbf{x}) \neq f(\mathbf{x}^{B_j})$. We refer to such a set B_j as a block. The block sensitivity of f , denoted $bs(f)$, is $\max_{\mathbf{x}} bs(f; \mathbf{x})$.

Obviously, we have $0 \leq s(f; \mathbf{x}) \leq bs(f; \mathbf{x}) \leq n$ and $0 \leq s(f) \leq bs(f) \leq n$.

Example 4.2. Let $n = 6$ and $\langle v_0 v_1 v_2 v_3 v_4 v_5 v_6 \rangle = \langle 1100011 \rangle$ be the value vector of a symmetric Boolean function $f(\mathbf{x})$. We calculate the block sensitivities of f over the words $\mathbf{x}_0 = (0, 0, 0, 0, 0, 0)$, $\mathbf{x}_3 = (1, 1, 1, 0, 0, 0)$, and $\mathbf{x}_5 = (1, 1, 1, 1, 1, 0)$.

For $\mathbf{x}_0 = (0, 0, 0, 0, 0, 0)$, $f(\mathbf{x}_0) = v_0 = 1$. In order to change the value to 0, we have to change at least two 0s in $\mathbf{x}_0 = (0, 0, 0, 0, 0, 0)$ since $v_1 = 1$. We are looking for the maximal number of blocks such that the value of f will be changed when the bits in each of these blocks are changed. So, we just change exactly two zeros in $\mathbf{x}_0 = (0, 0, 0, 0, 0, 0)$. Hence, the maximal number of blocks is $\left\lfloor \frac{6}{2} \right\rfloor = 3$. Therefore, $bs(f, (0, 0, 0, 0, 0, 0)) = 3$.

For $\mathbf{x}_3 = (1, 1, 1, 0, 0, 0)$, $f(\mathbf{x}_3) = v_3 = 0$. In order to change its value to 1, we either change two 1s to 0s or change two 0s to 1s. There are $\left\lfloor \frac{3}{2} \right\rfloor + \left\lfloor \frac{3}{2} \right\rfloor = 2$ blocks. Hence, $bs(f, (1, 1, 1, 0, 0, 0)) = 2$.

For $\mathbf{x}_5 = (1, 1, 1, 1, 1, 0)$, $f(\mathbf{x}_5) = v_5 = 1$. In order to change its value to 0, we change one 1 to 0 in $\mathbf{x}_5 = (1, 1, 1, 1, 1, 0)$, so, $bs(f, (1, 1, 1, 1, 1, 0)) = 5$.

Similarly, one can find $bs(f, (1, 0, 0, 0, 0, 0)) = 5$, $bs(f, (1, 1, 0, 0, 0, 0)) = bs(f, (1, 1, 1, 1, 0, 0)) = bs(f, (1, 1, 1, 1, 1, 1)) = 3$. Hence, the block sensitivity of the function f is $bs(f) = 5$.

We have

Proposition 4.3. Let $\langle v_0 v_1 \dots v_n \rangle = \langle \overbrace{u_1 \dots u_1}^{k_1} \overbrace{u_2 \dots u_2}^{k_2} \dots \overbrace{u_t \dots u_t}^{k_t} \rangle$ be the value vector of symmetric Boolean function $f(\mathbf{x})$, where $u_1 \neq u_2 \neq \dots \neq u_t$, $k_i \geq 1$, $i \geq 1$. If $k_i = 1$ for some i , then $s(f) = bs(f) = n$.

Proof. This follows from Lemmas 3.9 and 3.10. □

Generally, we have

Theorem 4.4. Let $\langle v_0 v_1 \dots v_n \rangle = \langle \overbrace{u_1 \dots u_1}^{k_1} \overbrace{u_2 \dots u_2}^{k_2} \dots \overbrace{u_t \dots u_t}^{k_t} \rangle$ be the value vector of symmetric Boolean function $f(\mathbf{x})$, where $u_1 \neq u_2 \neq \dots \neq u_t$, $k_i \geq 1$, $i \geq 1$, $k_1 + k_2 + \dots + k_t = n + 1$. $v_0 = v_1 = \dots = v_{k_1-1} = u_1$, $v_{k_1} = v_{k_1+1} = \dots = v_{k_1+k_2-1} = u_2, \dots, v_{k_1+\dots+k_{t-1}} = \dots = v_n = u_t$. Then the block sensitivity of $f(\mathbf{x})$ is

$$bs(f) = \max \left\{ \sum_{i=1}^j k_i + \left\lfloor \frac{n - \sum_{i=1}^j k_i}{k_{j+1}} \right\rfloor, n + 1 - \sum_{i=1}^j k_i + \left\lfloor \frac{\sum_{i=1}^j k_i - 1}{k_j} \right\rfloor \mid j = 1, \dots, t-1 \right\}. \quad (4.1)$$

Proof. If there exists j , $1 \leq j \leq t$ such that $k_j = 1$, by Proposition 4.3, $bs(f) = n$. It is clear the formula of equation (4.1) is also equal to n .

In the following, we assume $k_i \geq 2$ for $i = 1, \dots, t$. Since f is symmetric, we only need to calculate the sensitivities of f over the $n + 1$ words $\mathbf{x}_i = (\overbrace{1 \dots 1}^i 0 \dots 0)$, $i = 0, 1, \dots, n$ and the greatest sensitivity will be

$bs(f)$. We divide this $n + 1$ words into t groups. For each group, we do straightforward calculation as we did in Example 4.2. We list the results below. For easy notation, we write word $(x_1, \dots, x_n)$ as $(x_1 \cdots x_n)$.

Group 1: $\mathbf{x}_i = (\overbrace{1 \cdots 1}^i 0 \cdots 0)$, $0 \leq i \leq k_1 - 1$, $f(\mathbf{x}_i) = u_1$.

For $\mathbf{x}_0 = (0 \cdots 0)$, $bs(f, \mathbf{x}_0) = \left\lfloor \frac{n}{k_1} \right\rfloor$.

For $\mathbf{x}_1 = (10 \cdots 0)$, $bs(f, \mathbf{x}_1) = \left\lfloor \frac{n-1}{k_1-1} \right\rfloor$.

...

For $\mathbf{x}_{k_1-1} = (\overbrace{1 \cdots 1}^{k_1-1} 0 \cdots 0)$, $bs(f, \mathbf{x}_{k_1-1}) = \left\lfloor \frac{n-k_1+1}{1} \right\rfloor$.

Group 2: $\mathbf{x}_i = (\overbrace{1 \cdots 1}^i 0 \cdots 0)$, $k_1 \leq i \leq k_1 + k_2 - 1$, $f(\mathbf{x}_i) = u_2$.

For $\mathbf{x}_{k_1} = (\overbrace{1 \cdots 1}^{k_1} 0 \cdots 0)$, $bs(f, \mathbf{x}_{k_1}) = \left\lfloor \frac{k_1}{1} \right\rfloor + \left\lfloor \frac{n-k_1}{k_2} \right\rfloor$.

For $\mathbf{x}_{k_1+1} = (\overbrace{1 \cdots 1}^{k_1+1} 0 \cdots 0)$, $bs(f, \mathbf{x}_{k_1+1}) = \left\lfloor \frac{k_1+1}{2} \right\rfloor + \left\lfloor \frac{n-k_1-1}{k_2-1} \right\rfloor$.

...

For $\mathbf{x}_{k_1+k_2-1} = (\overbrace{1 \cdots 1}^{k_1+k_2-1} 0 \cdots 0)$, $bs(f, \mathbf{x}_{k_1+k_2-1}) = \left\lfloor \frac{k_1+k_2-1}{k_2} \right\rfloor + \left\lfloor \frac{n-k_1-k_2+1}{1} \right\rfloor$.

...

Group j : $2 \leq j \leq t-1$, $\mathbf{x}_i = (\overbrace{1 \cdots 1}^i 0 \cdots 0)$, $k_1 + \cdots + k_{j-1} \leq i \leq k_1 + \cdots + k_j - 1$, $f(\mathbf{x}_i) = u_j$.

For $\mathbf{x}_{k_1+\cdots+k_{j-1}} = (\overbrace{1 \cdots 1}^{k_1+\cdots+k_{j-1}} 0 \cdots 0)$, $bs(f, \mathbf{x}_{k_1+\cdots+k_{j-1}}) = \left\lfloor \frac{k_1+\cdots+k_{j-1}}{1} \right\rfloor + \left\lfloor \frac{n-k_1-\cdots-k_{j-1}}{k_j} \right\rfloor$.

For $\mathbf{x}_{k_1+\cdots+k_{j-1}+1} = (\overbrace{1 \cdots 1}^{k_1+\cdots+k_{j-1}+1} 0 \cdots 0)$, $bs(f, \mathbf{x}_{k_1+\cdots+k_{j-1}+1}) = \left\lfloor \frac{k_1+\cdots+k_{j-1}+1}{2} \right\rfloor + \left\lfloor \frac{n-k_1-\cdots-k_{j-1}-1}{k_j-1} \right\rfloor$.

...

For $\mathbf{x}_{k_1+\cdots+k_{j-1}} = (\overbrace{1 \cdots 1}^{k_1+\cdots+k_{j-1}} 0 \cdots 0)$, $bs(f, \mathbf{x}_{k_1+\cdots+k_{j-1}}) = \left\lfloor \frac{k_1+\cdots+k_{j-1}}{k_j} \right\rfloor + \left\lfloor \frac{n-k_1-\cdots-k_{j-1}}{1} \right\rfloor$.

...

Group t : $\mathbf{x}_i = (\overbrace{1 \cdots 1}^i 0 \cdots 0)$, $k_1 + \cdots + k_{t-1} \leq i \leq n$, $f(\mathbf{x}_i) = u_t$.

For $\mathbf{x}_{k_1+\cdots+k_{t-1}} = (\overbrace{1 \cdots 1}^{k_1+\cdots+k_{t-1}} 0 \cdots 0)$, $bs(f, \mathbf{x}_{k_1+\cdots+k_{t-1}}) = \left\lfloor \frac{k_1+\cdots+k_{t-1}}{1} \right\rfloor$.

For $\mathbf{x}_{k_1+\cdots+k_{t-1}+1} = (\overbrace{1 \cdots 1}^{k_1+\cdots+k_{t-1}+1} 0 \cdots 0)$, $bs(f, \mathbf{x}_{k_1+\cdots+k_{t-1}+1}) = \left\lfloor \frac{k_1+\cdots+k_{t-1}+1}{2} \right\rfloor$.

...

For $\mathbf{x}_{k_1+\cdots+k_{t-1}} = \mathbf{x}_n = (1 \cdots 1)$, $bs(f, (1 \cdots 1)) = \left\lfloor \frac{k_1+\cdots+k_{t-1}}{k_t} \right\rfloor = \left\lfloor \frac{n}{k_t} \right\rfloor$.

We will first find the maximal sensitivity number in each group.

In Group 1, it is clear that $bs(f, \mathbf{x}_0) \leq bs(f, \mathbf{x}_1) \leq \cdots \leq bs(f, \mathbf{x}_{k_1-1}) = \left\lfloor \frac{n-k_1+1}{1} \right\rfloor$.

In Group j , $2 \leq j \leq t-1$, we will show the maximal number will be the first or the last one.

Namely, $\max \left\{ \left\lfloor \frac{k_1+\cdots+k_{j-1}}{1} \right\rfloor + \left\lfloor \frac{n-k_1-\cdots-k_{j-1}}{k_j} \right\rfloor, \left\lfloor \frac{k_1+\cdots+k_{j-1}}{k_j} \right\rfloor + \left\lfloor \frac{n-k_1-\cdots-k_{j-1}}{1} \right\rfloor \right\}$.

Let $\mathbf{y}_m = \mathbf{x}_{k_1+\cdots+k_{j-1}+m}$, $0 \leq m \leq k_j - 1$ be the k_j words in Group j . We already know

$bs(f, \mathbf{y}_m) = \left\lfloor \frac{k_1+\cdots+k_{j-1}+m}{m+1} \right\rfloor + \left\lfloor \frac{n-k_1-\cdots-k_{j-1}-m}{k_j-m} \right\rfloor$, $0 \leq m \leq k_j - 1$.

Now we consider the real variable function $r(x) = \frac{k_1 + \dots + k_{j-1} + x}{x+1} + \frac{n - k_1 - \dots - k_{j-1} - x}{k_j - x}$ over the closed interval $[0, k_j - 1]$. Let $k_1 + \dots + k_{j-1} - 1 = A > 0$ and $n - k_1 - \dots - k_j = B > 0$, then $r(x) = \frac{A}{x+1} + \frac{B}{k_j - x} + 2$. Since $\frac{d^2 r}{dx^2} = \frac{2A}{(x+1)^3} + \frac{2B}{(k_j - x)^3} > 0$ over closed interval $[0, k_j - 1]$, $r(x)$ is concave up over $[0, k_j - 1]$. Hence, $r(x) \leq \max\{r(0), r(k_j - 1)\}$ for any $x \in [0, k_j - 1]$. For $0 \leq m \leq k_j - 1$, we have

$$\begin{aligned} bs(f, \mathbf{y}_m) &= \left\lfloor \frac{k_1 + \dots + k_{j-1} + m}{m+1} \right\rfloor + \left\lfloor \frac{n - k_1 - \dots - k_{j-1} - m}{k_j - m} \right\rfloor \\ &\leq \left\lfloor \frac{k_1 + \dots + k_{j-1} + m}{m+1} + \frac{n - k_1 - \dots - k_{j-1} - m}{k_j - m} \right\rfloor \\ &= \lfloor r(m) \rfloor \leq \lfloor \max\{r(0), r(k_j - 1)\} \rfloor = \max\{\lfloor r(0) \rfloor, \lfloor r(k_j - 1) \rfloor\} \\ &= \max \left\{ \left\lfloor \frac{k_1 + \dots + k_{j-1}}{1} + \frac{n - k_1 - \dots - k_{j-1}}{k_j} \right\rfloor, \left\lfloor \frac{k_1 + \dots + k_j - 1}{k_j} + \frac{n - k_1 - \dots - k_j + 1}{1} \right\rfloor \right\} \\ &= \max \left\{ k_1 + \dots + k_{j-1} + \left\lfloor \frac{n - k_1 - \dots - k_{j-1}}{k_j} \right\rfloor, \left\lfloor \frac{k_1 + \dots + k_j - 1}{k_j} \right\rfloor + n - k_1 - \dots - k_j + 1 \right\} \\ &= \max\{bs(f, \mathbf{y}_0), bs(f, \mathbf{y}_{k_j-1})\}. \end{aligned}$$

In Group t , it is clear that $\left\lfloor \frac{k_1 + \dots + k_{t-1}}{1} \right\rfloor \geq \left\lfloor \frac{k_1 + \dots + k_{t-1} + 1}{2} \right\rfloor \geq \dots \geq \left\lfloor \frac{n}{k_t} \right\rfloor$.

Now we put all the maximal numbers or maximal candidates of each group together to form a set

$$\begin{aligned} S &= \left\{ n - k_1 + 1, k_1 + \dots + k_{j-1} + \left\lfloor \frac{n - k_1 - \dots - k_{j-1}}{k_j} \right\rfloor, \right. \\ &\quad \left. \left\lfloor \frac{k_1 + \dots + k_j - 1}{k_j} \right\rfloor + n - k_1 - \dots - k_j + 1, k_1 + \dots + k_{t-1} \mid 2 \leq j \leq t-1 \right\} \\ &= \left\{ k_1 + \dots + k_{j-1} + \left\lfloor \frac{n - k_1 - \dots - k_{j-1}}{k_j} \right\rfloor, k_1 + \dots + k_{t-1}, \right. \\ &\quad \left. n - k_1 + 1, \left\lfloor \frac{k_1 + \dots + k_j - 1}{k_j} \right\rfloor + n - k_1 - \dots - k_j + 1 \mid 2 \leq j \leq t-1 \right\} \\ &= \left\{ k_1 + \dots + k_j + \left\lfloor \frac{n - k_1 - \dots - k_j}{k_{j+1}} \right\rfloor, k_1 + \dots + k_{t-1}, 1 \leq j \leq t-2 \right\} \\ &\quad \cup \left\{ n - k_1 + 1, \left\lfloor \frac{k_1 + \dots + k_j - 1}{k_j} \right\rfloor + n - k_1 - \dots - k_j + 1, 2 \leq j \leq t-1 \right\} \\ &= \left\{ k_1 + \dots + k_j + \left\lfloor \frac{n - k_1 - \dots - k_j}{k_{j+1}} \right\rfloor, 1 \leq j \leq t-1 \right\} \\ &\quad \cup \left\{ \left\lfloor \frac{k_1 + \dots + k_j - 1}{k_j} \right\rfloor + n - k_1 - \dots - k_j + 1, 1 \leq j \leq t-1 \right\} \\ &= \left\{ k_1 + \dots + k_j + \left\lfloor \frac{n - k_1 - \dots - k_j}{k_{j+1}} \right\rfloor, \left\lfloor \frac{k_1 + \dots + k_j - 1}{k_j} \right\rfloor + n - k_1 - \dots - k_j + 1, 1 \leq j \leq t-1 \right\} \\ &= \left\{ \sum_{i=1}^j k_i + \left\lfloor \frac{n - \sum_{i=1}^j k_i}{k_{j+1}} \right\rfloor, n + 1 - \sum_{i=1}^j k_i + \left\lfloor \frac{\sum_{i=1}^j k_i - 1}{k_j} \right\rfloor \mid j = 1, \dots, t-1 \right\}. \end{aligned}$$

Take the maximal value of this set, we prove the formula of $bs(f)$. □

Since $s(f) \leq bs(f) \leq n$ for any Boolean function f with n variables, by definition, we have the following.

Theorem 4.5. For odd d and $n \geq d$, the block sensitivity of $X(d, n)$ is n .

Proof. This follows from Theorem 3.17. $\square$

Theorem 4.6. If $d = 2^k$, $k \in \mathbb{N}$ and $n \geq d$, then $bs(X(d, n)) = bs(X(2^k, n)) = 2^k \left\lfloor \frac{n}{2^k} \right\rfloor$.

Proof. Let $\langle v_0 v_1 \dots v_n \rangle = \langle \overbrace{u_1 \dots u_1}^{k_1} \overbrace{u_2 \dots u_2}^{k_2} \dots \overbrace{u_t \dots u_t}^{k_t} \rangle$ be the value vector of $X(2^k, n)$ and $n = 2^k q + r$ with $0 \leq r \leq 2^k - 1$, where $u_1 \neq u_2 \neq \dots \neq u_t$. From the proof of Theorem 3.19, we know

$$\langle v_0 \dots v_n \rangle = \langle \overbrace{0 \dots 0 1 \dots 1}^{2^k} \dots \overbrace{0 \dots 0 1 \dots 1}^{2^k} \overbrace{1 0 \dots 0}^{r+1} \rangle$$

when q is even and

$$\langle v_0 \dots v_n \rangle = \langle \overbrace{0 \dots 0 1 \dots 1}^{2^k} \dots \overbrace{0 \dots 0 1 \dots 1}^{2^k} \overbrace{0 \dots 0 1 \dots 1}^{r+1} \rangle$$

when q is odd.

In either case, we always have $t = q + 1$, $k_1 = \dots = k_{t-1} = 2^k$ and $k_t = r + 1$. After a routine simplification of equation (4.1), it is easy to find that no other number is greater than $\sum_{i=1}^{t-1} k_i + \left\lfloor \frac{n - \sum_{i=1}^{t-1} k_i}{k_t} \right\rfloor = 2^k \left\lfloor \frac{n}{2^k} \right\rfloor$ in the set

S . We obtain $bs(X(2^k, n)) = 2^k \left\lfloor \frac{n}{2^k} \right\rfloor$. $\square$

In the following, we see the sensitivity is strictly less than the block sensitivity for some elementary symmetric Boolean functions.

Proposition 4.7. For $n \geq 10$, we have

$$bs(X(10, n)) = \begin{cases} 16 \left\lfloor \frac{n}{16} \right\rfloor, & n = 16q + r, \ 0 \leq r \leq 3 \\ 16 \left\lfloor \frac{n}{16} \right\rfloor + 1, & n = 16q + 4, \ 16q + 5 \\ 16 \left\lfloor \frac{n}{16} \right\rfloor + 2, & n = 16q + 6, \ 16q + 7 \\ 16 \left\lfloor \frac{n}{16} \right\rfloor + 3, & n = 16q + 8, \ 16q + 9 \\ n, & n = 16q + 10, \ 16q + 12, \ 16q + 14 \\ n - 1, & n = 16q + 11, \ 16q + 13, \ 16q + 15. \end{cases}$$

Proof. When $n = 16q + r$, $0 \leq r \leq 9$, by Lemma 3.23, the value vector

$$\langle v_0 v_1 \dots v_n \rangle = \langle \overbrace{u_1 \dots u_1}^{k_1} \overbrace{u_2 \dots u_2}^{k_2} \dots \overbrace{u_t \dots u_t}^{k_t} \rangle \text{ of } X(10, n) \text{ is}$$

$$\langle \overbrace{0000000000110011}^{16} \dots \overbrace{0000000000110011}^{16} \overbrace{0 \dots 0}^{r+1} \rangle.$$

Therefore, we have $t = 4q + 1$,

$k_i = 10$ when $i \equiv 1 \pmod{4}$ and $1 \leq i \leq 4q$,

$k_i = 2$ when $i \equiv 2, 3, 4 \pmod{4}$ and $1 \leq i \leq 4q$,

$k_t = k_{4q+1} = r + 1$.

If $j \equiv 1$ and $1 \leq j \leq 4q(\bmod 4)$, then $K_j = \sum_{i=1}^j k_i = \frac{j+3}{4}10 + \frac{3j-3}{4}2 = 4j + 6$.

If $j \equiv 2$ and $1 \leq j \leq 4q(\bmod 4)$, then $K_j = \sum_{i=1}^j k_i = \frac{j+2}{4}10 + \frac{3j-2}{4}2 = 4j + 4$.

If $j \equiv 3$ and $1 \leq j \leq 4q(\bmod 4)$, then $K_j = \sum_{i=1}^j k_i = \frac{j+1}{4}10 + \frac{3j-1}{4}2 = 4j + 2$.

If $j \equiv 4$ and $1 \leq j \leq 4q(\bmod 4)$, then $K_j = \sum_{i=1}^j k_i = \frac{j}{4}10 + \frac{3j}{4}2 = 4j$.

By Theorem 4.4, we have $bs(X(10, n)) = \max\{A, B, C\}$, where $A = \max\left\{K_j + \left\lfloor \frac{n - K_j}{k_{j+1}} \right\rfloor \middle| j = 1, \dots, t-2\right\}$,

$$B = K_{t-1} + \left\lfloor \frac{n - K_{t-1}}{k_t} \right\rfloor, \text{ and } C = \max\left\{n + 1 - K_j + \left\lfloor \frac{K_j - 1}{k_j} \right\rfloor \middle| j = 1, \dots, t-1\right\}.$$

Let $A_s = \max\left\{K_j + \left\lfloor \frac{n - K_j}{k_{j+1}} \right\rfloor \middle| j = 1, \dots, t-2, j \equiv s(\bmod 4)\right\}$, $s = 1, 2, 3, 4$.

Then

$$\begin{aligned} A_1 &= \max\left\{4j + 6 + \left\lfloor \frac{n - 4j - 6}{2} \right\rfloor \middle| 1 \leq j \leq 4q - 1, j \equiv 1(\bmod 4)\right\} \\ &= \max\left\{2j + 3 + \left\lfloor \frac{n}{2} \right\rfloor \middle| 1 \leq j \leq 4q - 1, j \equiv 1(\bmod 4)\right\} \\ &= 2(4q - 3) + 3 + \frac{n}{2} = 16q - 3 + \left\lfloor \frac{r}{2} \right\rfloor, \end{aligned}$$

$$\begin{aligned} A_2 &= \max\left\{4j + 4 + \left\lfloor \frac{n - 4j - 4}{2} \right\rfloor \middle| 1 \leq j \leq 4q - 1, j \equiv 2(\bmod 4)\right\} \\ &= \max\left\{2j + 2 + \left\lfloor \frac{n}{2} \right\rfloor \middle| 1 \leq j \leq 4q - 1, j \equiv 2(\bmod 4)\right\} \\ &= 2(4q - 2) + 2 + \frac{n}{2} = 16q - 2 + \left\lfloor \frac{r}{2} \right\rfloor, \end{aligned}$$

$$\begin{aligned} A_3 &= \max\left\{4j + 2 + \left\lfloor \frac{n - 4j - 2}{2} \right\rfloor \middle| 1 \leq j \leq 4q - 1, j \equiv 3(\bmod 4)\right\} \\ &= \max\left\{2j + 1 + \left\lfloor \frac{n}{2} \right\rfloor \middle| 1 \leq j \leq 4q - 1, j \equiv 3(\bmod 4)\right\} \\ &= 2(4q - 1) + 1 + \frac{n}{2} = 16q - 1 + \left\lfloor \frac{r}{2} \right\rfloor, \end{aligned}$$

$$\begin{aligned} A_4 &= \max\left\{4j + \left\lfloor \frac{n - 4j}{10} \right\rfloor \middle| 1 \leq j \leq 4q - 1, j \equiv 4(\bmod 4)\right\} \\ &= 4(4q - 4) + \left\lfloor \frac{n - 4(4q - 4)}{10} \right\rfloor \\ &= 16q - 16 + \left\lfloor \frac{r + 16}{10} \right\rfloor, \end{aligned}$$

and $A = \max\{A_1, A_2, A_3, A_4\} = 16q - 1 + \left\lfloor \frac{r}{2} \right\rfloor$. It is clear that $B = K_{t-1} + \left\lfloor \frac{n - K_{t-1}}{k_t} \right\rfloor = K_{4q} + \left\lfloor \frac{n - K_{4q}}{k_{4q+1}} \right\rfloor = 16q + \left\lfloor \frac{r}{r+1} \right\rfloor = 16q$.

Let $C_s = \max\left\{n + 1 - K_j + \left\lfloor \frac{K_j - 1}{k_j} \right\rfloor \middle| 1 \leq j \leq t-1, j \equiv s(\bmod 4)\right\}$, $s = 1, 2, 3, 4$.

Then

$$\begin{aligned} C_1 &= \max \left\{ n + 1 - (4j + 6) + \left\lfloor \frac{4j + 5}{10} \right\rfloor \mid 1 \leq j \leq t - 1, j \equiv 1(\bmod 4) \right\} \\ &= n + 1 - (4 + 6) + \left\lfloor \frac{4 + 5}{10} \right\rfloor = n - 9, \end{aligned}$$

$$\begin{aligned} C_2 &= \max \left\{ n + 1 - (4j + 4) + \left\lfloor \frac{4j + 3}{2} \right\rfloor \mid 1 \leq j \leq t - 1, j \equiv 2(\bmod 4) \right\} \\ &= n + 1 - (4 \times 2 + 4) + \left\lfloor \frac{4 \times 2 + 3}{2} \right\rfloor = n - 6, \end{aligned}$$

$$\begin{aligned} C_3 &= \max \left\{ n + 1 - (4j + 2) + \left\lfloor \frac{4j + 1}{2} \right\rfloor \mid 1 \leq j \leq t - 1, j \equiv 3(\bmod 4) \right\} \\ &= n + 1 - (4 \times 3 + 2) + \left\lfloor \frac{4 \times 3 + 1}{2} \right\rfloor = n - 7, \end{aligned}$$

$$\begin{aligned} C_4 &= \max \left\{ n + 1 - 4j + \left\lfloor \frac{4j - 1}{2} \right\rfloor \mid 1 \leq j \leq t - 1, j \equiv 4(\bmod 4) \right\} \\ &= n + 1 - 16 + 7 = n - 8, \end{aligned}$$

and $C = \max\{C_1, C_2, C_3, C_4\} = n - 6 = 16q + r - 6$.

In summary, for $n = 16q + r$, $0 \leq r \leq 9$, we have

$$\begin{aligned} bs(X(10, n)) &= \max\{A, B, C\} = \max \left\{ 16q - 1 + \left\lfloor \frac{r}{2} \right\rfloor, 16q, 16q + r - 6 \right\} \\ &= \begin{cases} 16 \left\lfloor \frac{n}{16} \right\rfloor, & n = 16q + r, 0 \leq r \leq 3 \\ 16 \left\lfloor \frac{n}{16} \right\rfloor + 1, & n = 16q + 4, 16q + 5 \\ 16 \left\lfloor \frac{n}{16} \right\rfloor + 2, & n = 16q + 6, 16q + 7 \\ 16 \left\lfloor \frac{n}{16} \right\rfloor + 3, & n = 16q + 8, 16q + 9. \end{cases} \end{aligned}$$

When $n = 16q + 10, 16q + 12, 16q + 14$, by Lemma 3.23, we have $bs(X(10, n)) = n$.

When $n = 16q + 11, 16q + 13, 16q + 15$, the formula $bs(X(10, n)) = n - 1$ can be similarly proved. $\square$

From Lemma 3.23 and Proposition 4.7, we know $s(X(10, n)) < bs(X(10, n))$ for $n = 16q + r$, $4 \leq r \leq 9$.

After similar calculations, we can obtain the following.

Proposition 4.8. Let $d = 12, n - 2, n - 1$. Then, $s(X(d, n)) = bs(X(d, n))$.

Proposition 4.9. For $n \geq 6$, the block sensitivity of $X(6, n)$ is

$$bs(X(6, n)) = \begin{cases} 8 \left\lfloor \frac{n}{8} \right\rfloor, & n = 8q + r, 0 \leq r \leq 3 \\ 8 \left\lfloor \frac{n}{8} \right\rfloor + 1, & n = 8q + 4, 8q + 5 \\ n, & n = 8q + 6 \\ n - 1, & n = 8q + 7. \end{cases}$$

It is clear that $s(X(6, n)) < bs(X(6, n))$ for $n = 8q + 4, 8q + 5$.

5 Conclusion

In this paper, we first improve a proposition of [33] and obtain some properties of the sequence $\left\{ \frac{1 - (-1)^{C(j,d)}}{2} \right\}_{j=0}^{\infty}$ discussed in ref. [8]. For elementary symmetric Boolean functions $X(d, n)$, we obtain explicit formulas for their sensitivities when d is odd and $d = n - 2, n - 1, 2^k, 2^{t+k} \pm 2^t$ for any natural numbers t and k . We also show that for the fixed value of d , the formulas of $s(X(d, n))$ and $s(X(n - d, n))$ can always be obtained. Further more, the explicit formulas of $s(X(d \times 2^k, n))$ can be obtained from the formulas of $\left\{ \frac{1 - (-1)^{C(j,d)}}{2} \right\}_{j=0}^{\infty}$. Based on the value vector of a symmetric Boolean function, we provide a formula for its block sensitivity. We apply this formula to elementary symmetric Boolean functions and obtain some block sensitivity formulas. We provide the tight upper and lower bounds for the sensitivities and block sensitivity for elementary symmetric Boolean functions. It is well known that sensitivity and block sensitivity of monotone Boolean functions are equal [24]. In ref. [18], the authors proved that sensitivity and block sensitivity of nested canalizing functions are also equal. Our results in this paper show that the block sensitivities for some elementary symmetric Boolean functions can be strictly greater than their sensitivities.

Acknowledgments: The authors sincerely thank the anonymous referees for their valuable suggestions and comments to improve the presentation quality of our manuscript.

Conflict of interest: Authors state no conflict of interest.

References

- [1] Arnold RF, Harrison MA. Algebraic properties of symmetric and partially symmetric Boolean functions. *IEEE Trans Electronic Comput.* 1963;EC-12(3):244–51.
- [2] Cai J-Y, Green F, Thierauf T. On the correlation of symmetric functions. *Math Syst Theory.* 1996;29(3):245–58.
- [3] Canteaut A, Videau M. Symmetric Boolean functions. *IEEE Trans Inf Theory.* 2005;51(8):2791–811.
- [4] Castro FN, González OE, Medina LA. A divisibility approach to the open boundary cases of Cusick-Li-Stănică's conjecture. *Cryptogr Commun.* 2015;7(4):379–402.
- [5] Castro FN, González OE, Medina LA. Diophantine equations with binomial coefficients and perturbation of symmetric Boolean functions. *IEEE Trans Inf Theory.* 2018;143 64(2):1347–60.
- [6] Castro FN, Medina LA. Asymptotic behavior of perturbations of symmetric functions. *Ann Combin.* 2014;18:397–417.
- [7] Cook SA, Dwork C, Reischuk R. Upper and lower time bounds for parallel random access machines without simultaneous writes. *SIAM J Comput.* 1986;15:87–9.
- [8] Cusick TW, Li Y, Stănică P. Balanced symmetric functions over $GF(p)$. *IEEE Trans Inf Theory.* 2008;54:1304–7.
- [9] Cusick TW, Li Y, Stănică P. On a conjecture for balanced symmetric Boolean functions. *J Math Crypt.* 2009;3:273–90.
- [10] Das SR, Sheng CL. On detecting total or partial symmetry of switching functions. *IEEE Trans Comput.* 1971;C-20(3):352–5.
- [11] Drucker A. Block sensitivity of minterm-transitive functions. *Theor Comput Sci.* 2011;412:5796–801.
- [12] Fredman M, Khachiyan L. On the complexity of dualization of monotone disjunctive normal forms. *J Algorithms.* 1996;21:618–28.
- [13] Gao G-P, Liu W-F, Zhang X-Y. The degree of balanced elementary symmetric Boolean functions of $4k + 3$ variables. *IEEE Trans Inf Theory.* 2011;57:4822–5.
- [14] Guo Y, Gao G, Zhao Y. Recent results on balanced symmetric Boolean functions. *IEEE Trans Inf Theory.* 2016;62:5199–203.
- [15] Huang H. Induced subgraphs of hypercubes and a proof of the sensitivity conjecture. *Ann Math.* 2019;190(3):945–55.
- [16] Kenyon C, Kutin S. Sensitivity, block sensitivity, and l -block sensitivity of Boolean functions. *Information and Computation.* 2004;189:43–53.
- [17] Li N, Qi W-F. Symmetric Boolean functions depending on an odd Number of variables with maximum algebraic immunity. *IEEE Trans Inf Theory.* 2006;52(5):2271–3.
- [18] Li Y, Adeyeye JO. Maximal sensitivity of Boolean nested canalizing functions. *Theor Comput Sci.* 2019;791:116–22. An early version appeared in Arxiv:1209.1597v1 [cs.DM] 7 Sept 2012.
- [19] Li Y, Adeyeye JO, Murrugarra D, Aguilar B, Laubenbacher R. Boolean nested canalizing functions: a comprehensive analysis. *Theor Comput Sci.* 2013;481:24–36.

- [20] Lidl R, Niederreiter H. Finite fields, New York: Cambridge University Press; 1977.
- [21] Maitra S, Sarker P. Maximum nonlinearity of symmetric Boolean functions on odd number of variables. *IEEE Trans Inf Theory*. 2002;48(9):2626–30.
- [22] Mishchenko A. Fast computation of symmetries in Boolean function. *IEEE Trans Comput-Aided Design Integr Circuits Syst*. 2003;22(11):1588–93.
- [23] Mitchell CJ. Enumerating Boolean functions of cryptographic significance. *J Crypto*. 1990;2(3):155–70.
- [24] Nisan N. CREW PRAMs and decision tree. *SIAM J Comput*. 1991;20(6):999–1007.
- [25] Qian X-N, Dougherty ER. A comparative study on sensitivities of Boolean networks. 2010 IEEE International Workshop on Genomic Signal Processing and Statistics (GENSIPS). NY: Cold Spring Harbor; 2010 p. 1–4.
- [26] Rubinstein D. Sensitivity VS block sensitivity of Boolean functions. *Combinatorica*. 1995;15(2):297–9.
- [27] Savicky P. On the bent Boolean functions that are symmetric. *Europ J Combin*. 1994;15:407–10.
- [28] Shannon CE. A symbolic analysis of relay and switching circuits. *AIEE Trans*. 1938;57:713–23.
- [29] Shmulevich I. Average sensitivity of typical monotone Boolean functions. *arXiv:math/0507030v1 [math.Co]*2005; p. 1.
- [30] Shmulevich I, Kauffman SA. Activities and sensitivities in Boolean network models. *Phys Rev Lett*. 2004;93(4):048701.
- [31] Su W, Tang X-H, Alexander P. A note on a conjecture for balanced elementary symmetric Boolean functions. *IEEE Trans Inf Theory*. 2013;59:665–71.
- [32] Sun X. Block sensitivity of weakly symmetric functions. *Theor Comput Sci*. 2007;384:87–91.
- [33] Wegener I. The critical complexity of all (monotone) Boolean functions and monotone graph properties. *Inf Control*. 1985;67:212–22.