Unbalanced Elementary Symmetric Boolean Functions With The Degree $\mathbf{d}$ And $\mathbf{wt}(\mathbf{d}) \geq \mathbf{3}$ *

Zhi-Hui Ou †and Ya-Qun Zhao

Abstract

In the paper, for $d = 2^t k$, $n = 2^t(2k+q)+m$ and special $k = 2^w(2^0 + 2^1 + \cdots + 2^s)$, we present that a majority of $X(d,n)$ are not balanced. The results include many cases $wt(d) \geq 3$ and $n \equiv 0,1,2,3 mod 4$. The results are also parts of the conjecture that $X(2^t, 2^{t+1}l-1)$ is only nonlinear balanced elementary symmetric Boolean function. Where $t \geq 2$, $q \geq 1$, $s \geq 0$, $w \geq 0$ and $m \geq -1$ are integers, and $X(d,n) = \bigoplus\limits_{1 \leq i_1 < \cdots < i_d \leq n} x_{i_1} \cdots x_{i_d}$.

Keywords: Cryptograph, Boolean functions, balancedness, elementary symmetric.

1 Introduction

Symmetric Boolean function is a subclass of Boolean functions and their outputs only depend on the Hamming weifht of their inputs, namely, for Boolean function $f(x)$, inputs x and y, then $f(x) = f(y)$ when $wt(x) = wt(y)$. They allow reducing memory spaces and gates of hardware implementation and are of great interest to cryptography. Recent years, many significant properties of symmetric Boolean functions have been studied in [1–7], including balancedness, algebraic immunity, resiliency, nonlinearity and so on. In [1–3], some symmetric Boolean functions with maximum algebraic immunity were constructed. The [3] gave the enumeration of symmetric Boolean functions with maximum algebraic immunity. In [4] and [5], it was proved that the maximum nonlinearity of n-variable symmetric functions is respectively $2^{n-1} - 2^{n/2-1}$ and $2^{n-1} - 2^{(n-1)/2}$ when n is respectively even and odd. The [6] gave all balanced symmetric Boolean functions whose degrees are smaller than 7. The [6] and [7] investigated the relationships among the significant properties of symmetric Boolean functions.

*This work is supported by National Nature Science Foundation of China under Grant number 61072046.

†The authors are with the Department of Applied Mathematics, Zhengzhou Information Science and Technology Institute, P.O. Box 1001-745, Zhengzhou 450002, China (e-mail:good_0501_oudi@163.com).

It is well known that balancedness is a primary requirement for Boolean functions in cryptosystem. The balancedness of symmetric Boolean functions should be firstly studied. For fixed algebraic degree, the [6] proved the conjecture that there is not balanced symmetric Boolean function when n grows. As a subclass of symmetric Boolean functions, elementary symmetric Boolean function is basic unit composing of symmetric Boolean functions. The balancedness of Elementary symmetric Boolean functions have been studied in [8–10]. The [8] prosed a conjecture that $X(2^t, 2^{t+1}l-1)$ is only nonlinear balanced elementary symmetric Boolean function. The [9] proved the conjecture holds when $wt(d) < 3$ and gave some cases that $X(d,n)$ are not balanced when $wt(d) = 3$. However, the [9] didn't study further when $wt(d) > 3$. In [10], for $n = 2^{t+1}l-1$ with odd l and $2^{t+1} \nmid d$, it showed that $X(d,n)$ is balanced if and only if $d = 2^k$, $1 \leq k \leq t$. Hence, for $n = 2^{t+1}l-1$ with odd l, the only case left is $2^{t+1} \mid d$. A majority of conjecture have been proved when $n \equiv 3mod4$, however, there are not many results when $n \equiv 0, 1, 2mod4$.

Since $X(d,n)$ is not balanced when $d > \lceil n/2 \rceil$ [8], we consider special elementary symmetric Boolean functions with forms $d \leq \lceil n/2 \rceil$. Combining with [9] and [10], in the paper, we consider special forms $2^t \mid d$, $n = 2^tl+m$ and $d \leq \lceil n/2 \rceil$. We assume that $d = k2^t$ and $n = 2^t(2k+q)+m$. As the cases $wt(d) < 3$ were discussed in [9] and the general cases $wt(d) \geq 3$ are difficult to be discussed, we consider special d whose '1s' are consecutive in the 2-adic description. Namely, $d = 2^{t+w}(1+2^1+\cdots+2^s)$ and $n = 2^{t+w+1}(1+2^1+\cdots+2^s)+2^tq+m$. For the several kinds of elementary symmetric Boolean functions, we give most cases that $X(d,n)$ are not balanced. The results include many cases $wt(d) \geq 3$ and $n \equiv 0, 1, 2, 3mod4$.

2 Preliminaries

There are some general definitions about Boolean functions. Denote by $GF(2)$ the finite field with two elements 0 and 1, and denote by $\bigoplus$ the addition over $GF(2)$. We consider function $f(x)$ called n-variable Boolean function from $GF^n(2)$ to $GF(2)$, where $GF^n(2)$ is the n-dimensional vector space over $GF(2)$ and $x = (x_1, x_2, \ldots, x_n) \in GF^n(2)$. $f(x)$ can be represented as a polynomial, called its algebraic normal form (ANF):

$$f(x_1, \ldots, x_n) = \bigoplus_{u \in GF^n(2)} \lambda_u(\prod_{i=1}^{n} x_i^{u_i}), \qquad \lambda_u \in GF(2).$$

The number of variables in the highest order product term with nonzero coefficient is called its algebraic degree. The Hamming weight of a binary vector $x = (x_1, x_2, \ldots, x_n)$ is the number of its nonzero coordinates, denoted by $wt(x)$. Denote by $\mid A \mid$ the size of the group A. $\mid \{x \in GF^n(2) | f(x) = 1\} \mid$ is called the Hamming weight of Boolean function $f(x)$, denoted by $wt(f(x))$.

$f(x)$ is called balanced if $wt(f(x)) = 2^{n-1}$. Hence, $\mid \{x \in GF^n(2) | f(x) = 0\} \mid - wt(f(x)) = 2^n - 2wt(f(x))$ can refer the balancedness of $f(x)$, namely, $f(x)$ is balanced if and only if $2^n - 2wt(f(x)) = 0$.

An n-variable Boolean function $f(x)$ is called symmetric if its output is invariant under any permutation of its input bits. Equivalently, the output of $f(x)$ only depends on the Hamming weight of its input vector. The form of elementary symmetric Boolean functions is as follows:

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

Let $Z(d,n) = 2^n - 2wt(X(d,n))$, then $X(d,n)$ is balanced if and only if $Z(d,n) = 0$. We write $\binom{n}{i}$ as C_n^i for short, and it is easy to get $X(d,n) = [1 - (-1)^{C_i^d}]/2$ when $x \in GF^n(2)$ and $wt(x) = i$. Hence,

$$\begin{aligned} Z(d,n) &= 2^n - 2 \cdot \sum_{i=0}^{n} [C_n^i \cdot \frac{1 - (-1)^{C_i^d}}{2}] \\ &= \sum_{i=0}^{d-1} C_n^i + \sum_{i=d}^{n} [C_n^i \cdot (-1)^{C_i^d}]. \end{aligned} \tag{1}$$

Definition 1. *[2] Let $a = (a_1, \cdots, a_n) \in GF^n(2)$, $b = (b_1, \cdots, b_n) \in GF^n(2)$, we say $a \preceq b$ if $a_i \le b_i$ for all $1 \le i \le n$; we say $a \npreceq b$ if $a_i > b_i$ for some i.*

Lemma 1. *[11] Let k and t be nonnegative integers, $k \ge t$, their 2-adic descriptions are $a = (k_0, k_1, \cdots, k_l)$ and $t = (t_0, t_1, \cdots, t_l)$, then*

$$C_k^t \equiv C_{k_0}^{t_0} C_{k_1}^{t_1} \cdots C_{k_l}^{t_l} \equiv \begin{cases} 1 mod 2 & , \quad a \preceq b \\ 0 mod 2 & , \quad a \npreceq b \end{cases}$$

We get the following two lemmas from basic knowledge of mathematical.

Lemma 2. *For fixed real number $a > 1$ and b, then $a^x > bx$ when $x > N(a,b)$, where $N(a,b)$ is a real number and is only relative to a and b.*

Lemma 3. *For fixed real number $a > 1$, then $x^a - o(x^a) > 0$ when $x > N(a)$, where $N(a)$ is a real number and is only relative to a. $o(x^a)$ is higher order indefinite small than x^a, namely, $x^a / o(x^a) \to \infty$ when $x \to \infty$.*

3 When $n = 2^{t+w+1}(1 + 2^1 + \cdots + 2^s) + 2^t q - 1$

In the section, we discuss elementary symmetric Boolean functions with form $n = 2^{t+w+1}(1 + 2^1 + \cdots + 2^s) + 2^t q - 1$ and $d = 2^{w+t}(1 + 2^1 + \cdots + 2^s)$. Notice that $n \equiv 3 mod 4$, the section is further work of the [10].

Theorem 1. *Let $q > 0$, $t > 1$, w and s be nonnegative integers, $n = 2^{t+w+1}(1+2^1+\cdots+2^s)+2^tq-1$ and $d = 2^{w+t}(1+2^1+\cdots+2^s)$. For fixed s and q, then $Z(d,n) < 0$ when $w \geq N(s,q)$, where $N(s,q)$ is a nonnegative integer and is only relative to s and q.*

Proof. Let $S = 2^0+2^1+\cdots+2^s$, then $d = 2^{w+t}S$ and $n = 2^{w+t+1}S+2^tq-1 = 2d+2^tq-1$. We have $d \preceq i$ when $d \leq i < d+2^{w+t}$. Assume that $2^w \geq q$, then $d \npreceq i$ when $d+2^{w+t} \leq i \leq n$. Since lemma 1, we have $C_i^d \equiv 1 mod 2$ when $d \leq i < d+2^{w+t}$ and $C_i^d \equiv 0 mod 2$ when $d+2^{w+t} \leq i \leq n$. Note that $C_n^i = C_n^{n-i}$ for all $0 \leq i \leq n$. Hence,

$$\begin{aligned}
Z(d,n) &= \sum_{i=0}^{2^{w+t}S-1} C_n^i - \sum_{i=2^{w+t}S}^{2^{w+t}S+2^{w+t}-1} C_n^i + \sum_{i=2^{w+t}S+2^{w+t}}^{n} C_n^i \\
&= \sum_{i=0}^{2^{w+t}S+2^tq-2^{w+t}-1} C_n^i + \sum_{i=2^{w+t}S+2^tq-2^{w+t}}^{2^{w+t}S-1} C_n^i \\
&\quad - \sum_{i=2^{w+t}S}^{(n-1)/2} C_n^i - \sum_{i=(n+1)/2}^{n-2^{w+t}S} C_n^i \\
&\quad - \sum_{i=n-2^{w+t}S+1}^{n-2^{w+t}S-2^tq+2^{w+t}} C_n^i + \sum_{i=n-2^{w+t}S-2^tq+2^{w+t}+1}^{n} C_n^i \\
&= 2\cdot(\sum_{i=0}^{2^{w+t}S+2^tq-2^{w+t}-1} C_n^i - \sum_{i=2^{w+t}S}^{2^{w+t}S+2^{t-1}q-1} C_n^i). \qquad (2) \\
&\triangleq 2(A-B)
\end{aligned}$$

For

$$\begin{aligned}
\frac{C_n^{2^{w+t}S+2^{t-1}q-1}}{C_n^{2^{w+t}S+2^tq-2^{w+t}-1}} &= \frac{(2^{w+t}S+2^{w+t})\times\cdots\times(2^{w+t}S+2^{t-1}q+1)}{(2^{w+t}S+2^{t-1}q-1)\times\cdots\times(2^{w+t}S+2^tq-2^{w+t})} \\
&\geq (\frac{2^{w+t}S+2^{w+t}}{2^{w+t}S+2^{t-1}q-1})^{2^{w+t}-2^{t-1}q}. \qquad (3)
\end{aligned}$$

And notice that $2^w \geq q$,

$$\frac{2^{w+t}S+2^{w+t}}{2^{w+t}S+2^{t-1}q-1} = \frac{S+1}{S+\frac{2^{t-1}q-1}{2^{w+t}}} > \frac{S+1}{S+0.5} = \frac{2S+2}{2S+1}. \qquad (4)$$

Then, on the one hand, we have the following inequations from (3) and (4).

$$\begin{aligned}
B &> C_n^{2^{w+t}S+2^{t-1}q-1} \\
&> (\frac{2S+2}{2S+1})^{2^{w+t}-2^{t-1}q} C_n^{2^{w+t}S+2^tq-2^{w+t}-1} \triangleq C. \qquad (5)
\end{aligned}$$

on the other hand, we have the following inequations from $2^w \geq q$.

$$\begin{aligned} A &< (2^{w+t}S + 2^t q - 2^{w+t})C_n^{2^{w+t}S+2^t q-2^{w+t}-1} \\ &\leq 2S(2^{w+t} - 2^{t-1}q)C_n^{2^{w+t}S+2^t q-2^{w+t}-1} \triangleq D. \end{aligned} \tag{6}$$

Since lemma 2, then there exists a positive real number $N_1(S)$ which is only relative to S. When $N_1(S) \geq 2^{w+t} - 2^{t-1}q$, namely, we have the following inequation when $2^w \geq N_1(S)/2^t + q/2$,

$$(\frac{2S+2}{2S+1})^{2^{w+t}-2^{t-1}q} \geq 2S(2^{w+t} - 2^{t-1}q). \tag{7}$$

Therefore, from (2), (5), (6) and(7), if $2^w \geq q$ and $2^w \geq N_1(S)/2^t + q/2$ hold at the same time, then

$$Z(d,n) = 2(A-B) < 2(D-C) < 0. \tag{8}$$

Since $N_1(S)/2^t + q/2 \leq N_1(S)/2 + q/2$, if we let

$$N(s,q) = \lceil max\{\log_2 q, \log_2 (N_1(S)/2 + q/2)\}\rceil \tag{9}$$

then $Z(d,n) < 0$ when $w \geq N(s,q)$. □

Remark 1. *In fact, according to theorem 1 and computer exhausting, $Z(d,n) \neq 0$ when s and q are enough small. Notice that $N(s,q) = \lceil \log_2 q \rceil$ when $q \geq N_1(S)$, $N(s,q) = \lceil \log_2 (N_1(S)/2 + q/2) \rceil < \lceil \log_2 N_1(S) \rceil$ when $q < N_1(S)$. We can let $N(s,q) = \lceil \log_2 N_1(S) \rceil$ when $q < N_1(S)$. The following table 1 presents the relationships clear. From the table 1, we notice that the relationship between s and $N(s,q)$ is almost linearity when $q < N_1(S)$.*

Table 1: The relationships among s, q and $N(s,q)$

s	$q <$	$N(s,q)$	s	$q <$	$N(s,q)$	s	$q <$	$N(s,q)$
0	11	4	7	7772	13	14	1665654	21
1	42	6	8	17068	15	15	3520258	22
2	115	7	9	37156	16	16	7417616	23
3	286	9	10	80318	17	17	15588014	24
4	676	10	11	172590	18	18	32679052	25
5	1554	11	12	368998	19	19	68359552	27
6	3500	12	13	785478	20	20	142713644	28

Theorem 2. *The conditions are the same as theorem 1. For fixed w, q and t, if $2^w \geq q$, then $Z(d,n) > 0$ when $s \geq N(w,q,t)$, where $N(w,q,t)$ is a nonnegative integer and is only relative to w, q and t.*

Proof. We still let $S = 2^0 + 2^1 + \cdots + 2^s$, From the proof of the theorem 1, we have

$$\begin{aligned} Z(d,n) &= 2 \cdot \Big(\sum_{i=0}^{2^{w+t}S+2^t q-2^{w+t}-1} C_n^i - \sum_{i=2^{w+t}S}^{2^{w+t}S+2^{t-1}q-1} C_n^i \Big) \\ &> 2 \cdot \Big(\sum_{i=2^{w+t}S+2^{t-1}q-2^{w+t}-1}^{2^{w+t}S+2^t q-2^{w+t}-1} C_n^i - 2^{t-1}q C_n^{2^{w+t}S+2^{t-1}q-1} \Big) \qquad (10) \\ &\triangleq E. \end{aligned}$$

If we assume that $\prod_{j=0}^{i-1}(2^{w+t}S + 2^{w+t} + 2^{t-1}q - j) = 1$ when $i = 0$, for any $0 \le i \le 2^{t-1}q$ and $k = i + 2^{w+t}S + 2^{t-1}q - 2^{w+t} - 1$, then

$$\begin{aligned} &\frac{C_n^k \cdot (2^{w+t}S + 2^{t-1}q - 1)!(2^{w+t}S + 2^{w+t} + 2^{t-1}q)!}{(2^{w+t+1}S + 2^t q - 1)!} \\ &= \prod_{j=0}^{2^{w+t}-i-1} (2^{w+t}S + 2^{t-1}q - 1 - j) \cdot \prod_{j=0}^{i-1}(2^{w+t}S + 2^{w+t} + 2^{t-1}q - j). \qquad (11) \end{aligned}$$

Hence, we have the following equations from (10) and (11).

$$\begin{aligned} &\frac{E \cdot (2^{w+t}S + 2^{t-1}q - 1)!(2^{w+t}S + 2^{w+t} + 2^{t-1}q)!}{2 \cdot (2^{w+t+1}S + 2^t q - 1)!} \\ &= \sum_{i=0}^{2^{t-1}q} \Big[\prod_{j=0}^{2^{w+t}-i-1} (2^{w+t}S + 2^{t-1}q - 1 - j) \cdot \prod_{j=0}^{i-1}(2^{w+t}S + 2^{w+t} + 2^{t-1}q - j) \Big] \\ &\quad -2^{t-1}q \prod_{i=0}^{2^{w+t}-1} (2^{w+t}S + 2^{w+t} + 2^{t-1}q - i) \\ &= (2^{t-1}q + 1) \cdot [S^{2^{w+t}} + o(S^{2^{w+t}})] - 2^{t-1}q[S^{2^{w+t}} + o(S^{2^{w+t}})] \\ &= S^{2^{w+t}} - o(S^{2^{w+t}}). \qquad (12) \end{aligned}$$

Note that the last two equations are relative to q, since lemma 3, then there exists a positive real number $N_1(w, q, t)$ which is only relative to t, w and q. $S^{2^{w+t}} - o(S^{2^{w+t}}) > 0$ when $S = 1 + 2^1 + 2^2 + \cdots + 2^s > N_1(w, q, t)$. If we let

$$N(w, q, t) = \lceil \log_2(N_1(w, q, t) + 1) - 1\rceil \qquad (13)$$

then $Z(d, n) > 0$ when $s \ge N(w, q, t)$. □

Remark 2. *Note that w and t are variable in the theorem 1 and s is variable in the theorem 2, although the d and n have the same forms in the two theorems, the two theorems have different meanings. $Z(d, n) < 0$ in the theorem 1 and $Z(d, n) > 0$ in the theorem 2. In fact, $wt(X(d, n))/2^n \to 1$*

when $w \to \infty$ in the theorem 1 and $wt(X(d,n))/2^n \to 0$ when $s \to \infty$ in the theorem 2. The two theorems reveal the relationships among w, t, s, q and $Z(d,n)$. The two theorems gave some unbalanced Elementary Symmetric Boolean Functions from two aspects.

4 When $n = 2^{t+w+1}(1 + 2^1 + \cdots + 2^s) + 2^t q$

In the section, we discuss elementary symmetric Boolean functions with form $n = 2^{t+w+1}(1 + 2^1 + \cdots + 2^s) + 2^t q$ and $d = 2^{w+t}(1 + 2^1 + \cdots + 2^s)$, where $n \equiv 0 mod 4$. The following theorem 3 and theorem 4 are similar to the theorem 1 and theorem 2.

Theorem 3. *Let $q > 0$, $t > 1$, w and s be nonnegative integers, $n = 2^{t+w+1}(1 + 2^1 + \cdots + 2^s) + 2^t q$ and $d = 2^{w+t}(1 + 2^1 + \cdots + 2^s)$. For fixed s and q, then $Z(d,n) < 0$ when $w \geq N(s,q)$, where $N(s,q)$ is a nonnegative integer and is only relative to s and q.*

Proof. Let $S = 2^0 + 2^1 + \cdots + 2^s$, then $d = 2^{t+w}S$ and $n = 2^{t+w+1}S + 2^t q$. Assume that $2^w \geq q + 1$, similarly to the proof of the theorem 1, then

$$\begin{aligned} Z(d,n) &= \sum_{i=0}^{2^{w+t}S-1} C_n^i - \sum_{i=2^{w+t}S}^{2^{w+t}S+2^{w+t}-1} C_n^i + \sum_{i=2^{w+t}S+2^{w+t}}^{n} C_n^i \\ &= 2 \cdot (\sum_{i=0}^{2^{w+t}S+2^t q-2^{w+t}-1} C_n^i - \sum_{i=2^{w+t}S}^{2^{w+t}S+2^{t-1}q-1} C_n^i) - C_n^{2^{w+t}S+2^{t-1}q} \\ &< 2 \cdot (\sum_{i=0}^{2^{w+t}S+2^t q-2^{w+t}-1} C_n^i - \sum_{i=2^{w+t}S}^{2^{w+t}S+2^{t-1}q-1} C_n^i). \end{aligned} \tag{14}$$

And note that the inequation (14) is the same as the equation (2), similarly to the proof of the theorem 1, if $2^w \geq q + 1$ and $2^w \geq N_1(S)/2 + q/2$ hold at the same time, then

$$\begin{aligned} & Z(d,n) \\ & < \ 2 \cdot [2S(2^{w+t} - 2^{t-1}q) - (\frac{2S+2}{2S+1})^{2^{w+t}-2^{t-1}q}] \cdot C_n^{2^{w+t}S+2^t q-2^{w+t}-1} \\ & < \ 0. \end{aligned} \tag{15}$$

$N_1(S)$ is a positive real number and is only relative to S. If we let

$$N(s,q) = \lceil max\{\log_2 (q+1), \log_2 (N_1(S)/2 + q/2)\} \rceil \tag{16}$$

then $Z(d,n) < 0$ when $w \geq N(s,q)$. $\square$

Remark 3. *Similarly to the theorem 1, note that* $N(s,q) = \lceil \log_2(q+1) \rceil$ *when* $q \geq N_1(S) - 2$, $N(s,q) = \lceil \log_2(N_1(S)/2 + q/2) \rceil < \lceil \log_2(N_1(S)) \rceil$ *when* $q < N_1(S) - 2$, *therefore,* $N(s,q)$ *is only relative to* s *or* q. *And note aslo that* t *not be limited in the theorem 1.*

Theorem 4. *The conditions are the same as the theorem 3. For fixed* w, q *and* t, *if* $2^w \geq q+1$, *then* $Z(d,n) > 0$ *when* $s \geq N(w,q,t)$, *where* $N(w,q,t)$ *is a nongetative integer and is only relative to* w, q *and* t.

Proof. We still let $S = 2^0 + 2^1 + \cdots + 2^s$, then $d = 2^{t+w}S$ and $n = 2^{t+w+1}S + 2^t q$. From the the proof of the theorem 3, we have

$$\begin{aligned}
Z(d,n) &= 2 \cdot \Big(\sum_{i=0}^{2^{w+t}S+2^t q-2^{w+t}-1} C_n^i - \sum_{i=2^{w+t}S}^{2^{w+t}S+2^{t-1}q-1} C_n^i \Big) - C_n^{2^{w+t}S+2^{t-1}q} \\
&> 2 \cdot \sum_{i=2^{w+t}S-2^{w+t}+2^{t-1}q-2}^{2^{w+t}S+2^t q-2^{w+t}-1} C_n^i - 2(2^{t-1}q+1) C_n^{2^{w+t}S+2^{t-1}q} \qquad (17) \\
&\triangleq F.
\end{aligned}$$

Similarly to the proof of the theorem 2, let $\prod_{j=0}^{i-1}(2^{w+t}S + 2^{w+t} + 2^{t-1}q + 2 - j) = 1$ when $i = 0$, then

$$\begin{aligned}
&\frac{F \cdot (2^{w+t}S + 2^{t-1}q)!(2^{w+t}S + 2^{w+t} + 2^{t-1}q + 2)!}{2 \cdot (2^{w+t+1}S + 2^t q)!} \\
&= \sum_{i=0}^{2^{t-1}q+1} \Big[\prod_{j=0}^{2^{w+t}+1-i} (2^{w+t}S + 2^{t-1}q - j) \\
&\quad \cdot \prod_{j=0}^{i-1} (2^{w+t}S + 2^{w+t} + 2^{t-1}q + 2 - j) \Big] \\
&\quad -(2^{t-1}q+1) \prod_{i=0}^{2^{w+t}+1} (2^{w+t}S + 2^{w+t} + 2^{t-1}q + 2 - i) \\
&= (2^{t-1}q+2) \cdot [S^{2^{w+t}+2} + o(S^{2^{w+t}+2})] \\
&\quad -(2^{t-1}q+1) \cdot [S^{2^{w+t}+2} + o(S^{2^{w+t}+2})] \\
&= S^{2^{w+t}+2} - o(S^{2^{w+t}+2}). \qquad (18)
\end{aligned}$$

Since lemma 3, then there exists a positive real number $N_1(w,q,t)$ which is only relative to w, q and t. $S^{2^{w+t}+2} - o(S^{2^{w+t}+2}) > 0$ when $S = 1 + 2^1 + 2^2 + \cdots + 2^s > N_1(w,q,t)$. If we let $N(w,q,t) = \lceil \log_2(N_1(w,q,t)+1) - 1 \rceil$, then $Z(d,n) > 0$ when $s \geq N(w,q,t)$. $\square$

Remark 4. *For* $n = 2^{t+w+1}(1 + 2^1 + \cdots + 2^s) + 2^t q + m$, $d = 2^{w+t}(1 + 2^1 + \cdots + 2^s)$, $m \equiv p \mod 4$, *similarly to the proof of the case* $n = 2^{t+w+1}(1+$

$2^1 + \cdots + 2^s) + 2^t q - 1$ *if* p *is odd, similarly to the proof of the case* $n = 2^{t+w+1}(1 + 2^1 + \cdots + 2^s) + 2^t q$ *if* p *is even, we can get similar results to the foregoing* 4 *theorems.*

5 Conclusion

The paper considers Unbalanced elementary symmetric Boolean functions $X(d, n)$ with special form $d = 2^{t+w}(1+2^1+\cdots+2^s)$, $n = 2^{t+w+1}(1+2^1+\cdots+2^s)+2^t q+m$. For fixed s, q, or fixed w, q, t, we present a majority of $X(d, n)$ are not balanced. Our results include many $X(d, n)$ that $d \equiv 0, 1, 2, 3 mod 4$, which is supplement of only case $d \equiv 3 mod 4$. Our results are also parts of the conjecture that $X(2^t, 2^{t+1}l - 1)$ is only nonlinear balanced elementary symmetric Boolean function. For others special forms $X(d, n)$, we also can give many similar results in the same method.

Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that are going to improve much the technical equality and the editorial quality of this paper.

References

[1] L. Qu, K. Feng, F. Liu and L. Wang, "Constructing symmetric Boolean functions with maximum algebraic immunity," *IEEE Trans. Inf. Theory*, vol.55, no.5, pp.2406–2412, 2009.

[2] Yingdong Chen and Peizhong Lu, "Two classes of symmetric Boolean functions with optimum algebraic immunity:construction and analysis," *IEEE Trans. Inf. Theory*, vol.57, no.4, pp.2522–2538, 2011.

[3] Jie Peng, Quanshui Wu and Haibin Kan, "On symmetric Boolean functions with high algebraic immunity on even number of variables," *IEEE Trans. Inf. Theory*, vol.57, no.10, pp.7205–7220, 2011.

[4] P. Savicky, "On the Bent Boolean functions that are symmetric," *Eur. J.C Combin.*, vol.15, pp. 407–410, 1994.

[5] S. Maitra and P. Sarkar, "Maximum nonlinearity of symmetric Boolean functions on odd number of variables," *IEEE Trans. Inf. Theory*, vol.48, no.9, pp.2626–2630, 2002.

[6] A. Canteaut and M. Videau, "Symmetric Boolean functions," *IEEE Trans. Inf. Theory*, vol.51, no.8, pp.2791–2811, 2005.

[7] C. Carlet, "On the degree, nonlinearity, algebraic thickness and nonormality of Boolean functions, with developments on symmetric Boolean," *IEEE Trans. Inf. Theory*, vol.50, no.9, pp.2178–2185, 2004.

[8] T.W. Cusick, Y. li, and P. Stanica, "Balanced symmetric Boolean functions over GF(p)," *IEEE Trans. Inf. Theory*, vol.3, no.54, pp.1304–1307, 2008.

[9] T.W. Cusick, Y. li, and P. Stanica, "On a conjecture for balanced symmetric Boolean functions," *J. Math. Crypt.*, vol. 3. no. 4, pp. 273–290, 2009.

[10] G. Gao, W. Liu, and X. Zhang, "The degree of balanced elementary symmetric Boolean functions of 4k + 3 Variables," *IEEE Trans. Inf. Theory*, vol.57, no.7, pp. 4822–4825, July, 2011.

[11] R.M. Wilson, "A diagonal form for the incidence matrices of t-subsets vs k-subsets," *Eur. J.C Combin*, vol.11, pp. 609–614, 1990.

Zhi-Hui Ou received the B.S. degree in mathematics from the Zhengzhou Information Science and Technology Institute, China, in 2008. Currently, he is working towards the M.S. degree in mathematics. His research area includes Boolean functions.

Ya-Qun Zhao received the B.S., M.S., and P.h.D. degree in mathematics from the Zhengzhou Information Science and Technology Institute, China, in 1982, 1997 and 2000. She is now a professor at the Zhengzhou Information Science and Technology Institute. Her research area includes cryptography.