Recent Results on Balanced Symmetric Boolean Functions

Ying-ming Guo* Guang-pu Gao Ya-Qun Zhao

Abstract

In this paper we prove all balanced symmetric Boolean functions of fixed degree are trivial when the number of variables grows large enough. We also present the nonexistence of trivial balanced elementary symmetric Boolean functions except for $n = l \cdot 2^{t+1} - 1$ and $d = 2^t$, where t and l are any positive integers, which shows Cusick's conjecture for balanced elementary symmetric Boolean functions is exactly the conjecture that all balanced elementary symmetric Boolean functions are trivial balanced. In additional, we obtain an integer n_0, which depends only on d, that Cusick's conjecture holds for any $n > n_0$.

Keywords: Boolean functions, Balancedness, elementary symmetric functions

1 Introduction

Boolean functions play an important role in the design of symmetric cryptographic systems. They are used for S-Box design in block cipher and utilized as nonlinear filters and combiners in stream ciphers. Symmetric Boolean functions, which have the property that their outputs only depend on the Hamming weight of their inputs, are an interesting subclass of Boolean functions for their advantage in both implementation complexity and storage space. In [1], A. Canteaut and M. Videau studied in detail symmetric boolean functions. They established a link between the periodicity of simplified value vector of a symmetric function and its degree. Cai *et al.* computed a closed formula for the correlation between any two symmetric Boolean functions in terms of their periods[5]. Castro *et al.* improved the formula for computing the exponential sums of symmetric Boolean functions[2](also see, Lemma 1).

Balancedness is a primary requirement to resist the attacks on each cryptosystem. In [8], J. von zur Gathen and J. Rouche found all the balanced

*The authors are with the Department of Applied Mathematics, Zhengzhou Information Science and Technology Institute, P.O. Box 1001-741, Zhengzhou 450002, China (e-mail:guoyingming123@gmail.com).

symmetric boolean functions up to 128 variables. Canteaut *et al.* proved that balanced symmetric functions of degree less than or equal to 7(excluding the trivial cases) only exist for eight variables[1]. Since the number of nontrivial balanced functions seems to be very small, they conjectured that balanced symmetric functions of fixed degree do not exist when the number of variables grows. For elementary symmetric Boolean functions, Cusick *et al.* proposed a conjecture in [3] about the nonexistence of nonlinear balanced elementary symmetric Boolean functions $\sigma_{n,d}$ except for $n = l \cdot 2^{t+1} - 1$ and $d = 2^t$, where t and l are any positive integers. They also obtained many results towards the conjecture in [4]. Later in [6] Gao *et al.* proved that when $n = 3 \bmod 4$, the function is balanced if and only if $d = 2^k, 1 \leq k \leq t$. It was mentioned in [4][2] that Cusick's conjecture holds for sufficient large number of variables, but a certain bound had not been obtained.

2 Preliminaries

Let F_2^n be the vector space of n-tuples over the Field $F_2 = \{1, 0\}$ of two elements. We denote by $\oplus$ the sum over F_2. A Boolean function of n variables is a function from F_2^n into F_2. A Boolean function is said to be symmetric if its output is invariant under any permutation of its input bits. We denote by B_n (resp. SB_n) the set of all Boolean functions (resp. symmetric Boolean functions) of n variables. If $f : F_2^n \to F_2$, then f can be uniquely represented as a multivariate polynomial over F_2, called *algebraic normal form* (ANF):

$$f(x_1, \cdots, x_n) = \bigoplus_{\mu \in F_2^n} \lambda_\mu \left(\prod_{i=1}^{n} x_i^{\mu_i} \right), \quad \text{with} \quad \lambda_\mu = \bigoplus_{x \preceq \mu} f(x)$$

Where $(x_1, \cdots, x_n) \preceq (\mu_1, \cdots, \mu_n)$ if and only if $\forall i,\ x_i \leq \mu_i$. The addition and multiplication operations are in F_2. The number of variables in the highest order product term with nonzero coefficient is called its algebraic degree (denoted by $deg(f)$).

Definition 1. *For integers n and d, the elementary symmetric Boolean function with n variables $\sigma_{n,d}$ is defined as the sum of all terms of degree d, that is*

$$\sigma_{n,d} = \bigoplus_{1 \leq i_1 \leq \cdots \leq i_d \leq n} x_{i_1} \cdots x_{i_d}.$$

If $f(x) = \sigma_{n,d}$, then$v_f(i) = \binom{i}{d} \bmod 2$.

A Boolean function of n variables is symmetric if and only if its algebraic normal form can be written as follows:

$$f(x_1, \cdots, x_n) = \bigoplus_{i=0}^{n} \lambda_f(i) \left(\bigoplus_{\mu \in F_2^n, w_H(\mu) = i} \prod_{j=1}^{n} x_j^{\mu_j} \right) = \bigoplus_{i=0}^{n} \lambda_\mu \sigma_{n,i},$$

Where $\sigma_{n,i}$ is the elementary symmetric polynomial of degree i in n variables.

A Boolean function is said to be affine if its algebraic degree does not exceed 1. The set of all n-variable affine functions is denoted by $A(n)$. The Hamming weight $w_H(x)$ of a binary vector $x \in F_2^n$ is the number of its nonzero coordinates, and the Hamming weight $w_H(f)$ of a Boolean function f is the size of its support$\{x \in F_2^n \mid f(x) = 1\}$.If $w_H(x) = 2^{n-1}$, we call $f(x)$ balanced. A symmetric function can be represented by a vector $v_f = (v_f(0), \cdots, v_f(n))$, where $v_f(i) = f(x)$ for $x \in F_2^n$ with Hamming weight $w_H(x) = i$. It was proved in [1] that for any $f \in SB_n$, v_f is periodic with period 2^t, $2^t < n$, if and only if $deg(f) \leq 2^t - 1$; $deg(f) = 2^t$ if and only if v_f is periodic with period 2^{t+1} and is a part of $(v_f(0), \cdots, v_f(2^t - 1), v_f(0) \oplus 1, \cdots, v_f(2^t - 1) \oplus 1)^\infty$.

Definition 2. *For any $f \in B_n$, we denote by $\mathcal{F}(f)$ the following value related to the Fourier transform of f*

$$\mathcal{F}(f) = \sum_{x \in F_2^n} (-1)^{f(x)}.$$

Definition 3. *[1] Let n be an odd integer and $f \in SB_n$. We say that f is a trivial balanced function if*

$$v_f(i) = v_f(n-i) \oplus 1, 0 \leq i \leq n.$$

The even case corresponds to affine functions.

Let a, b be positive integers and their 2-*adic* expressions are $a = \sum_{i=0}^{n-1} a_i 2^i, b = \sum_{i=0}^{n-1} b_i 2^i$. We denote $a \preceq b$ if for all $i (0 \leq k \leq n-1)$, $a_i \leq b_i$ and otherwise $a \npreceq b$.The Lucas formula says[7, p. 79], $\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1} \cdots \binom{n_l}{k_l}$. Let $f(x) = \sigma_{n,d}$, by Lucas formula, $v_f(i) = 1$ if and only if $d \preceq i$.

It was proved in [3] that if $\sigma_{n,d}$ is balanced, then $d \leq \lceil \frac{n}{2} \rceil$.

3 Asymptotic Behavior of Symmetric Boolean Functions

In this section, we present the behavior of symmetric Boolean functions with large number of variables. As a consequence of our discussion using the technique for the correlation of symmetric functions in [5], we prove the following conjecture.

Conjecture 1. *[1, VIII] Balanced symmetric functions of fixed degree excluding the trivial cases do not exist when the number of variables grows.*

To prove Conjecture 1, we introduce the following lemma:

Lemma 1. *[2] Let $f(x) = \sigma_{n,k_s} + \cdots + \sigma_{n,k_1}, 1 \le k_1 \le \cdots \le k_s$ and let $r = \lfloor \log_2 k_s \rfloor + 1$. $\mathcal{F}(f)$ is given by*

$$\mathcal{F}(f) = \sum_{i=0}^{n} (-1)^{v_f(i)} \binom{n}{i} = \frac{1}{2^r} \sum_{j=0}^{2^r-1} s_j \lambda_j^n, \tag{1}$$

where $\xi_j = \exp\left(\frac{\pi\sqrt{-1}j}{2^{r-1}}\right), \lambda_j = 1 + \xi_j$, and

$$s_j = \sum_{i=0}^{2^r-1} (-1)^{v_f(i)} \xi_j^{-i}.$$

If f is not affine, then $r \ge 2$. We have the following observation on *Lemma* 1:

$$\begin{aligned} 2^{r-1}\mathcal{F}(f) &= \frac{1}{2} \sum_{j=0}^{2^r-1} s_j \lambda_j^n \\ &= \sum_{j=1}^{2^{r-1}-1} \mathrm{Re}\left(s_j \lambda_j^n\right) + \frac{1}{2}\left(s_0 \lambda_0^n + s_{2^{r-1}} \lambda_{2^{r-1}}^n\right) \end{aligned} \tag{2}$$

where the second equality holds because $\xi_{2^r-j} = \overline{\xi_j}, s_{2^r-j} = \overline{s_j}$ and $\lambda_{2^r-j} = \overline{\lambda_j}$, so that the second half of the j-sum ($2^{r-1} \le j \le 2^r - 1$)is the complex conjugate of the first half. Let us define

$$t_j(n) = \frac{1}{2^{r-1}} \mathrm{Re}\left(s_j \lambda_j^n\right), 0 \le j \le 2^{r-1} - 1.$$

Note that $\lambda_{2^{r-1}} = 0$, thus

$$\mathcal{F}(f) = \frac{1}{2} t_0(n) + \sum_{j=1}^{2^{r-1}-1} t_j(n). \tag{3}$$

If $\mathcal{F}(f) = 0$, there are potentially two reasons for this: either all the $t_j(n)$ are zero or several nonzero $t_j(n)$ ($\frac{1}{2}t_j(n)$ for $j = 0$) can cancel each other. The next lemma states that the latter cannot happen for large enough n. However, we should point out that the following Lemma, although having a different $t_j(n)$, contribute to Cai *et al.*[5].

Lemma 2. *Let $f \in B_n$ and f is not affine. There exists an integer n_0 such that for any $n > n_0$,*

$$\mathcal{F}(f) = 0 \Leftrightarrow t_j(n) = 0, 0 \le j \le 2^{r-1} - 1. \tag{4}$$

Proof. Suppose $\mathcal{F}(f) = 0$. We can express $t_j(n)$ as[1]

$$t_j(n) = |s_j| \left| 2\cos\left(\frac{\pi j}{2^r}\right)\right|^n \cos\left(\arg(s_j) - \frac{\pi n j}{2^r}\right). \tag{5}$$

Clearly, we have $t_j(n) \le |s_j| \left|2\cos\left(\frac{\pi j}{2^r}\right)\right|^n$. On the other hand, if $t_j(n) \neq 0$, since the cosine is periodic in n, for any j there exists a constant $c_j > 0$ (c_j does not depend on n) such that

$$t_j(n) \ge c_j \left|2\cos\left(\frac{\pi j}{2^r}\right)\right|^n.$$

Hence, each $|t_j(n)|$ is either zero or in a constant range of $\left|2\cos\left(\frac{\pi j}{2^r}\right)\right|^n$.

Since $\left|2\cos\left(\frac{\pi j}{2^r}\right)\right|^n$ dominates $\left|2\cos\left(\frac{\pi(j+1)}{2^r}\right)\right|^n$ for large enough n and $j < 2^r - 1$, any $t_j(n) \neq 0$ dominates all the $t_{j'}(n)$ for $j < j' < 2^{r-1}$. Thus if j_0 is the least j such that $t_j(n) \neq 0$, then the subsequent terms cannot cancel $t_{j_0}(n)$ $\quad(\frac{1}{2}t_{j_0}(n)$ for $j = 0)$, and hence, $\mathcal{F}(f) \neq 0$. Therefore, $t_j(n) = 0$, for all $0 \le j \le 2^{r-1} - 1$. □

If $s_j \neq 0$, then for any j, $0 \le j \le 2^{r-1} - 1$, we have

$$\begin{aligned}
t_j(n) = 0 \quad &\Leftrightarrow \quad \cos\left(\arg(s_j) - \frac{\pi n j}{2^r}\right) = 0 \\
&\Leftrightarrow \quad \exists l \quad \arg(s_j) - \frac{\pi n j}{2^r} = \frac{\pi}{2} + l\pi \\
&\Leftrightarrow \quad \exists l \quad \exp(2i\arg(s_j)) = \exp\left(2i\left(\frac{\pi n j}{2^r} + \frac{\pi}{2} + l\pi\right)\right) \\
&\Leftrightarrow \quad |s_j|\exp(i\arg(s_j)) = -|s_j|\exp(-i\arg(s_j))\exp\left(\frac{\pi i}{2^r} n j\right) \\
&\Leftrightarrow \quad s_j = -\xi_j^n \overline{s_j}
\end{aligned} \tag{6}$$

Note that if $s_j = 0$, we get $t_j(n) = 0, s_j = -\xi_j^n\overline{s_j} = 0$. Thus

$$t_j(n) = 0 \Leftrightarrow s_j = -\xi_j^n \overline{s_j}, \quad 0 \le j \le 2^{r-1} - 1 \tag{7}$$

holds no matter whether s_j is zero.

To prove our result, the following lemma is needed.

Lemma 3. *Let $f \in B_n$ and f is not affine. The following properties are equivalent.*

(i) $s_j = -\xi_j^n \overline{s_j}, \quad 0 \le j \le 2^r - 1,$

[1] Any complex number $z \neq 0$ can uniquely be written as $z = |z|(\cos\varphi + i\sin\varphi) = |z|e^{i\varphi}$. where $0 \le \varphi \le 2\pi$. φ is called the argument of z, $\varphi = \arg z$. Hence $\mathrm{Re}(z) = |z|\cos\arg(z)$

(ii) $v_f(i) = 1 \oplus v_f(n-i)$, $\quad 0 \le i \le 2^r - 1$

Proof. If property (ii) is true, then it is clear that

$$s_j = \sum_{i=0}^{2^r-1} (-1)^{v_f(n-i)+1} \xi_j^i, \tag{8}$$

Since $(-1)^{v_f(i)} \xi_j^i$ has period $2^r, 0 \le j \le 2^r - 1$, thus

$$\begin{aligned} -\xi_j^n \overline{s_j} &= -\xi_j^n \sum_{i=0}^{2^r-1} (-1)^{v_f(i)} \xi_j^{-i} \\ &= -\xi_j^n \sum_{i=n}^{n+2^r-1} (-1)^{v_f(i)} \xi_j^{-i} \\ &= -\sum_{i=n}^{n+2^r-1} (-1)^{v_f(i)} \xi_j^{n-i} \\ &= \sum_{i=0}^{2^r-1} (-1)^{v_f(n-i)+1} \xi_j^i = s_j \end{aligned} \tag{9}$$

If property (i) is true, then, for any $0 \le j \le 2^r - 1$,

$$\sum_{i=0}^{2^r-1} (-1)^{v_f(i)} \xi_j^i = \sum_{i=0}^{2^r-1} (-1)^{v_f(n-i)+1} \xi_j^i \tag{10}$$

Note that these sums are the Fourier transforms of the functions $f(i)$ and $f(n-i)$, respectively. We can perform an inverse Fourier transform by using the relation

$$\sum_{j=0, j \ne 2^{r-1}}^{2^r-1} \xi_j^{i-i'} = \begin{cases} 2^r - 1 & , \quad i = i' \\ (-1)^{i-i'+1} & , \quad i \ne i' \end{cases} \tag{11}$$

Now multiply the left and right hand sides of equation (10) by $\xi_j^{-i'}$ and sum over j from 0 to $2^r - 1$. Then we have

$$2^r(-1)^{v_f(i')} - \sum_{i=0}^{2^r-1} (-1)^{v_f(i)} = 2^r(-1)^{v_f(n-i')+1} - \sum_{i=0}^{2^r-1} (-1)^{v_f(n-i)+1} \tag{12}$$

Since $\sum_{i=0}^{2^r-1} (-1)^{v_f(n-i)+1} = -\sum_{i=0}^{2^r-1} (-1)^{v_f(i)}$, thus

$$(-1)^{v_f(i')} + (-1)^{v_f(n-i')} = \frac{1}{2^{r-1}} \sum_{i=0}^{2^r-1} (-1)^{v_f(i)} \tag{13}$$

The left hand side can be ± 2 or 0. If it is ± 2, then f is constant, which contradicts the hypothesis of the theorem. Hence, the left hand side is 0 and we conclude $-1^{v_f(i')} = (-1)^{1+v_f(n-i')}$. The property (ii) follows. $\square$

Now we prove the conjecture.

Theorem 1. *For large enough n, balanced symmetric functions of fixed degree are trivial.*

Proof. When $f \in B_n$ is affine function. If f is balanced, then f is trivial regardless of the parity of n.

Let f be a non-affine function with period 2^r. Following *Lemma* 1 to *Lemma* 3, there exists an integer n_0 such that for any $n > n_0$,

$$\mathcal{F}(f) = 0 \Leftrightarrow v_f(i) = 1 \oplus v_f(n-i), \quad i = 0, \cdots, 2^r - 1.$$

Note that when n is even, we get $v_f(\frac{n}{2}) = 1 + v_f(\frac{n}{2})$, which is a contradiction. That is, for sufficient large n, non-affine balanced symmetric functions are trivial for odd n and do not exist for even n. Therefore, *Theorem* 1 is proved. □

4 The equivalence of Cusick's conjecture

In this section, we discuss the equivalence of Cusick's conjecture for elementary symmetric functions. We show the conjecture is exactly the conjecture that all balanced elementary symmetric Boolean function is trivial balanced. Associating with the theorem in last section, we present the conjecture is validated with sufficient large number of variables.

Conjecture 2. *[3] There are no nonlinear balanced elementary symmetric Boolean functions except for $\sigma_{l\cdot 2^{t+1}-1, 2^t}$, where t and l are any positive integers.*

Let us consider $f(x) = \sigma_{l\cdot 2^{t+1}-1, 2^t}(x)$. Since $deg(f) = 2^t$, v_f is periodic with period 2^{t+1} and is a part of $(v_f(0), \cdots, v_f(2^{t-1}), v_f(0) \oplus 1, \cdots, v_f(2^t - 1) \oplus 1)^\infty$. Note that $n = l2^t - 1$, it is obvious that $f(x)$ is trivial balanced. Next we prove that all trivial balanced elementary symmetric Boolean functions have the form $\sigma_{l\cdot 2^{t+1}-1, 2^t}$.

Theorem 2. *There are no trivial balanced elementary symmetric Boolean functions except for $\sigma_{l\cdot 2^{t+1}-1, 2^t}$, where t and l are any nonnegative integers.*

Proof. Supposed $f(x) = \sigma_{l\cdot 2^{t+1}-1, 2^t}(x)$ is trivial balanced. If $d = 1$, the conclusion follows regardless of the parity of n. When $d > 1$, n must be odd, and $v_f(i) = v_f(n-i)$, $0 \le i \le n$. Since $v_f(i) = \binom{i}{d} \bmod 2$ and $v_f(i) = 1$ if and only if $d \preceq i$, we get either $d \preceq i$ or $d \preceq (n-i)$.

Let the 2-*adic* expressions of d, n are $\overline{d} = \sum_{i=0}^{t} d_i 2^i$, $\overline{n} = \sum_{i=0}^{l} n_i 2^i$, $l > t$. We assert that d is a power of 2. Otherwise, suppose d_t, d_j is ones(i.e. $\overline{d} = 1_t \cdots 1_j \cdots$). Let $\overline{i} = 0_t \cdots 1_j \underbrace{0_{j-1} \cdots 0_0}_{0}$. Since $d \not\preceq i$, we get $d \preceq (n-i)$, which implies $n_j = 0$. On the other hand, let $\overline{i'} = 1_t \cdots \underbrace{0_j \cdots 0_0}_{0}$. Since $d \npreceq i'$,we get $d \preceq (n-i')$,which implies $n_j = 1$. It is a contradiction.

Furthermore, we claim that $n = l \cdot 2^{t+1} - 1$ (i.e. $\overline{n} = n_l \cdots n_{t+1} \underbrace{1_t \cdots 1_0}_{1}$). Otherwise, suppose n_j is the first zero from t-th bit to the last bit(i.e. $\overline{n} = n_l \cdots n_{t+1} \underbrace{1_t \cdots 1_{j+1}}_{1} 0_j n_{j-1} \cdots n_0$). Let $\overline{i} = \underbrace{1_t \cdots 1_j}_{1} \underbrace{0_{j-1} \cdots 0_0}_{0}$, then we get $\overline{n-i} = n_l \cdots n_{t+1} \underbrace{1_t \cdots 1_{j+1} 1_j}_{1} n_{j-1} \cdots n_0$, which implies $d \preceq i$. It is a contradiction to $d \preceq (n-i)$. Hence, we conclude that all trivial balanced elementary symmetric Boolean functions have the form of $\sigma_{l \cdot 2^{t+1}-1, 2^t}$. □

Remark. By *Theorem* 2, *Conjure* 2 shows in essence that all balanced elementary symmetric Boolean functions are trivial balanced. According to *Theorem* 1 and *Theorem* 2, we conclude that there exists an integer n_0 such that *Conjure* 2 holds for any $n > n_0$.

In additional, we give an estimation for n_0. Let $f(x) = \sigma_{l \cdot 2^{t+1}-1, 2^t}(x)$, by the conclusion in [1, VI, equation (2)], we get

$$\begin{aligned} \mathcal{F}(f) &= \sum_{i=0}^{2^r-1} (-1)^{v_f(i)} \left(2^{n-r} + 2^{1-r} \sum_{j=1}^{2^{r-1}-1} (2c_j)^n c'_j \right) \\ &= 2^{n-r} \sum_{i=0}^{2^r-1} (-1)^{v_f(i)} + 2^{n-r+1} \sum_{j=1}^{2^{r-1}-1} \sum_{i=0}^{2^r-1} (-1)^{v_f(i)} c_j^n c'_j \qquad (14) \end{aligned}$$

where $c_j = \cos\left(j\frac{\pi}{2^r}\right), c'_j = \cos\left(j(n-2i)\frac{\pi}{2^r}\right)$. It is exactly the equation (3) where for $0 \le j \le 2^{r-1} - 1$

$$t_j(n) = 2^{n-r+1} \cos^n \left(j \frac{\pi}{2^r} \right) \sum_{i=0}^{2^r-1} (-1)^{\binom{i}{d}} \cos\left(j(n-2i) \frac{\pi}{2^r} \right). \qquad (15)$$

Consider the equation. If $t_0(n) \ge 2^{j+1}|t_j(n)|$, it is obvious that $\mathcal{F}(f) = 0$ if and only if $t_0(n) = t_j(n) = 0, 1 \le j \le 2^{r-1} - 1$. Thus we have the following result.

Theorem 3. *Let $r = \lfloor \log_2 d \rfloor + 1$. For any $n, n > -2\left(log_2 \cos\left(\frac{\pi}{2^r}\right)\right)^{-1}$, all these nonlinear balanced elementary symmetric Boolean functions are of the form $\sigma_{l \cdot 2^{t+1}-1, 2^t}$, where t and l are any positive integers.*

Proof. Consider $t_j(n), 1 \le j \le 2^{r-1} - 1$,

(1) If $\sum_{i=0}^{2^r-1}(-1)^{\binom{i}{d}}\cos\left(\frac{j\pi}{2^r}(n-2i)\right)\geq 0$, then

$$\begin{aligned}
&\sum_{i=0}^{2^r-1}(-1)^{\binom{i}{d}}-\sum_{i=0}^{2^r-1}(-1)^{\binom{i}{d}}\cos\left(\frac{j\pi}{2^r}(n-2i)\right)\\
&= 2\sum_{i=0}^{2^r-1}(-1)^{\binom{i}{d}}\sin^2\left(\frac{j\pi}{2^r}\cdot\frac{n-2i}{2}\right)\\
&\geq 2\sum_{i=0}^{2^{r-1}-1}(-1)^{\binom{i}{d}}\left(\sin^2\left(\frac{j\pi}{2^r}\cdot\frac{n-2i}{2}\right)+\cos^2\left(\frac{j\pi}{2^r}\cdot\frac{n-2i}{2}\right)\right)\\
&= 0 \qquad (16)
\end{aligned}$$

(2) If $\sum_{i=0}^{2^r-1}(-1)^{\binom{i}{d}}\cos\left(\frac{j\pi}{2^r}(n-2i)\right)< 0$, then

$$\begin{aligned}
&\sum_{i=0}^{2^r-1}(-1)^{\binom{i}{d}}+\sum_{i=0}^{2^r-1}(-1)^{\binom{i}{d}}\cos\left(\frac{j\pi}{2^r}(n-2i)\right)\\
&= 2\sum_{i=0}^{2^r-1}(-1)^{\binom{i}{d}}\cos^2\left(\frac{j\pi}{2^r}\cdot\frac{n-2i}{2}\right)\\
&\geq 2\sum_{i=0}^{2^{r-1}-1}(-1)^{\binom{i}{d}}\left(\cos^2\left(\frac{j\pi}{2^r}\cdot\frac{n-2i}{2}\right)+\sin^2\left(\frac{j\pi}{2^r}\cdot\frac{n-2i}{2}\right)\right)\\
&= 0 \qquad (17)
\end{aligned}$$

These two equalities hold if and only if $d=2^{r-1}$. Therefore $t_0(n)\geq|t_j(n)|$ for $1\leq j\leq 2^{r-1}-1$.

When $n>-2/\left(log_2\cos\left(\frac{\pi}{2^r}\right)\right)$, we have $\cos^n\left(\frac{\pi}{2^r}\right)<\frac{1}{4}$, and hence $t_0(n)>|4t_1(n)|$. In additional, since for any $j, 1\leq j\leq 2^{r-1}-1$,

$$\frac{\cos\left(\frac{j}{2^r}\pi\right)}{\cos\left(\frac{j+1}{2^r}\pi\right)}=\frac{\cos\left(\frac{j}{2^r}\pi\right)}{\cos\left(\frac{\pi}{2^r}\right)\cos\left(\frac{j}{2^r}\pi\right)-\sin\left(\frac{\pi}{2^r}\right)\sin\left(\frac{j}{2^r}\pi\right)}>\frac{1}{\cos\left(\frac{\pi}{2^r}\right)}>4, \qquad (18)$$

$t_0(n)>2^{j+1}|t_j(n)|$ holds for any $j, 1\leq j\leq 2^{r-1}-1$.

So $\mathcal{F}(f)=0$ if and only if $t_0(n)=t_j(n)=0$. From the discussion in *Section* 3, if f is balanced, then f is trivial. Therefore, by *Theorem* 2, *Conjecture* 2 is validated for all $n>-2\left(log_2\cos\left(\frac{\pi}{2^r}\right)\right)^{-1}$, where $2^{r-1}\leq d<2^r$. □

References

[1] A. Canteaut and M. Videau, "Symmetric Boolean functions," *IEEE Trans. Inf. Theory*, vol.51, no.8, pp.2791–2881, 2005.

[2] F.N. Castro, and L.A. Medina, "Linear recurrences and asymptotic behavior of exponential sums of symmetric boolean functions," *The Electronic Journal of Combinatorics*, vol.18, no.2, pp.P8, 2011.

[3] 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.

[4] 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.

[5] J. Y. Cai, F.G. and T. Thierauf., "On the correlation of symmetric functions," *Theory of Computing Systems*, vol.29, pp.245–258, 1996.

[6] 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, 2011

[7] L. Comtet, *Advanced Combinatorics*, Amsterdam. The Netherlands: Reidel, 1974.

[8] J. von zur Gathen and J. Roche, "Polynomials with two values," *Combinatorica*, vol.17, pp.345-362, 1997.