EXACT DIVISIBILITY OF EXPONENTIAL SUMS ASSOCIATED TO ELEMENTARY SYMMETRIC BOOLEAN FUNCTIONS

FRANCIS N. CASTRO, OSCAR E. GONZÁLEZ, LUIS A. MEDINA, RAÚL E. NEGRÓN, AND IVELISSE M. RUBIO

Abstract. In this paper, we present an elementary method to compute or estimate the exact 2-divisibility of exponential sums associated to symmetric Boolean functions. As a direct consequence of these results, we prove some of the open cases of Cusick-Li-Stănică's conjecture about balanced symmetric Boolean functions.

1. Introduction

An n-variable Boolean function F is a function defined over $\mathbb{F}^n$ with values in $\mathbb{F}$, the finite field with two elements. Symmetric Boolean functions in n variables are Boolean functions whose value does not depend on the permutation of its input. These functions are simpler to study because instead of having to consider all of the 2^n possible inputs, we only need to consider $n+1$ inputs; this also makes them more efficient to use if their values need to be stored in a computer (memory constraints).

Elementary symmetric Boolean functions are the building blocks for all symmetric Boolean functions. This is why understanding their behavior is very important. There is a unique elementary symmetric Boolean function in n variables of degree k and it is denoted by

$$\sigma_{n,k} = \sigma_k(X_1, \ldots, X_n) = \sum_{1 \leq j_1 < j_2 < \ldots < j_k \leq n} X_{j_1} \cdots X_{j_k}. \tag{1}$$

Surprisingly, these functions are still not completely understood. In general, the problem of computing the exact divisibility of Boolean functions is hard. Usually, the known results just provide an estimate for the divisibility. The main goal of this paper is to present an elementary method to calculate the divisibility of exponential sums associated to symmetric Boolean functions. As an application of our method, we compute the exact divisibility of several infinite families of symmetric Boolean functions. In some cases we obtain estimates that improve previously known lower bounds in divisibility. To calculate the divisibility of the exponential sums studied, one can follow a general method which will be described in the next section.

In 2008, Cusick-Li and Stănică proposed a conjecture about the non-balancedness of elementary symmetric Boolean functions, which states ([CLS08]):

Conjecture 1.1 (Cusick-Li-Stănică)**.** *There are no nonlinear balanced elementary symmetric Boolean functions except for degree $k = 2^l$ and $2^{l+1}D - 1$-variables, where l, D are positive integers.*

Date: January 9, 2017.

In [CLS08, CLS09, GLZ11, STP13, CM11, GGZ12], several cases of Cusick-Li and Stănică's conjecture are tackled. The state of the art of results on the conjecture up to 2013 can be found in [STP13]. In 2015, many of the boundary cases of Cusick-Li and Stănică's conjecture were shown to be true [CGM15]. Our results give affirmative answer to some open cases of this conjecture.

Finally, we want to point out that our method could be applied to other families of symmetric Boolean functions not included in this paper, but we feel that the families presented here show its efficiency.

2. Preliminaries and Description of Our Method

Let $\mathbb{F}$ be the binary field, $\mathbb{F}^n = \{(x_1, \ldots, x_n) : x_i \in \mathbb{F}, i = 1, ..., n\}$, and $F(\mathbf{X}) = F(X_1, \ldots, X_n)$ be a polynomial in n variables over $\mathbb{F}$. The exponential sum associated to F over $\mathbb{F}$ is

$$S(F) = \sum_{x_1,\ldots,x_n \in \mathbb{F}} (-1)^{F(x_1,\ldots,x_n)}. \tag{2}$$

A Boolean function F is called balanced iff $S(F) = 0$, i.e. the number of zeros and the number of ones are equal in the truth table of F. Equivalently, F is called balanced iff $|\{x \in \mathbb{F}^n : F(x) = 1\}| = 2^{n-1}$. The property of being balanced is a very useful one for cryptographic applications, for it means that the function has no bias towards a specific value (in a certain way this guarantees that the function is "random"). Determining whether or not a function is balanced can be difficult in general. However, as a direct application of some of our results, we can determine whether certain families of Boolean functions are balanced.

Our aim is to compute the highest power of 2 dividing $S(F)$ for the case when $F(\mathbf{X})$ is a symmetric Boolean function. In general, if m is a non-zero integer, we denote the highest power of 2 that divides m by $\nu_2(m)$, where $m = 2^{\nu_2(m)}a$ and a is not divisible by 2. We refer to $\nu_2(m)$ as the 2-*adic valuation* of m or as the *exact* 2-*divisibility* of m.

Let $A_j = \{(x_1, \cdots, x_n) \in \mathbb{F}^n : w_2((x_1, \cdots, x_n)) = j\}$. Clearly, $|A_j| = \binom{n}{j}$ and $\sigma_{n,k}(\mathbf{x}) = \binom{j}{k}$ for $\mathbf{x} \in A_j$. Thus, in the case of an elementary symmetric polynomial, the exponential sum can be written as

$$S(\sigma_{n,k}) = \sum_{j=0}^{n} \binom{n}{j} (-1)^{\binom{j}{k}}. \tag{3}$$

In general, we have that

$$S(\sigma_{n,k_1}+\cdots+\sigma_{n,k_r}) = \sum_{x_1,\ldots,x_n \in \mathbb{F}} (-1)^{\sigma_{n,k_1}(x_1,\ldots,x_n)+\cdots+\sigma_{n,k_r}(x_1,\ldots,x_n)} = \sum_{j=0}^{n} \binom{n}{j} (-1)^{\binom{j}{k_1}+\cdots+\binom{k}{k_r}}. \tag{4}$$

Define $N(n,k) = \left\{0 \le j \le n \,|\, \binom{j}{k} \equiv 1 \bmod 2\right\}$. Note that

$$S(\sigma_{n,k}) = 2^n - 2 \sum_{j \in N(n,k)} \binom{n}{j}. \tag{5}$$

Thus,

$$\nu_2(S(\sigma_{n,k})) = \nu_2\left(2^n - 2\sum_{j\in N(n,k)}\binom{n}{j}\right). \tag{6}$$

In other words, whenever $\nu_2\Big(\sum_{j\in N(n,k)}\binom{n}{j}\Big) < n-1$ we have that computing the exact 2-divisibility of $\sum_{j\in N(n,k)}\binom{n}{j}$ yields the exact 2-divisibility of $S(\sigma_{n,k})$.

To study $\nu_2(S(\sigma_{n,k}))$, we will do the following:

1. Use Lucas' theorem to determine which binomial coefficients will be elements of $N(n,k) = \{0 \le j \le n \,|\, \binom{j}{k} \equiv 1 \bmod 2\}$.
2. Conjecture the value of $\nu_2(S(\sigma_{n,k})) = l$ via computer experiments.
3. Study the binomial coefficients in the sum $\sum_{j\in N(n,k)}\binom{n}{j}$ and show that some of these have valuation greater than or equal to l.
4. Consider the binomials in the sum which have 2-adic valuation smaller than l, and show that the 2-adic valuation of the sum of these binomials is equal to $l-1$.

Recall that $\nu_2(m+n) \ge \min\{\nu_2(m),\nu_2(n)\}$ and $\nu_2(m+n) = \min\{\nu_2(m),\nu_2(n)\}$ for $\nu_2(m) \ne \nu_2(n)$. Since we have $\sum_{j\in N(n,k)}\binom{n}{j} = \sum_{\substack{j\in N(n,k)\\ \nu_2(\binom{n}{j})\ge l}}\binom{n}{j} + \sum_{\substack{j\in N(n,k)\\ \nu_2(\binom{n}{j})< l}}\binom{n}{j}$, then, if we are able to show that $\nu_2\Big(\sum_{\substack{j\in N(n,k)\\ \nu_2(\binom{n}{j})< l}}\binom{n}{j}\Big) = l-1$ we would have that

$$\nu_2\Big(\sum_{\substack{j\in N(n,k)\\ \nu_2(\binom{n}{j})\ge l}}\binom{n}{j} + \sum_{\substack{j\in N(n,k)\\ \nu_2(\binom{n}{j})< l}}\binom{n}{j}\Big) = \nu_2\Big(\sum_{\substack{j\in N(n,k)\\ \nu_2(\binom{n}{j})< l}}\binom{n}{j}\Big) = l-1. \tag{7}$$

Hence, if we complete the steps described above, we will obtain $\nu_2(S(\sigma_{n,k})) = l$.

Also, we point out that of these four "steps", number 4 is definitely the hardest. This is because in general, calculating the valuation of a sum is not easy if some of the summands have the same valuation (which is our case). Estimating the valuation is somewhat easier, and this is what we do in step (3).

Theorem 2.1 is one of the tools we use to show $\nu_2\Big(\sum_{\substack{j\in N(n,k)\\ \nu_2(\binom{n}{j})< l}}\binom{n}{j}\Big) = l-1$.

Theorem 2.1 ([TL04], Corollary)**.** *Define the lacunary binomial sum*

$$G_{l,\,k}(n) = \sum_{t=0}^{\lfloor n/l\rfloor}\binom{n}{k+lt}, \tag{8}$$

with $k : 0 \le k \le l-1$, and consider the situation where $l = p^m$, p prime, $m \ge 1$. For $m \ge 1$, $0 \le k \le 2^m$, $n \ge 2^{m-1}$, we have $\nu_2\big(G_{2^m,\,k}(n)\big) \ge \lfloor \frac{n}{2^{m-1}}\rfloor - 1$, where $G_{l,\,k}(n)$ is as in (8).

Furthermore, if

$$n = \varepsilon_0 + 2\varepsilon_1 + 4\varepsilon_2 + \cdots + 2^{m-1}\varepsilon_{m-1} + 2^m q$$

and

$$k = \gamma_0 + 2\gamma_1 + 4\gamma_2 + \cdots + 2^{m-1}\gamma_{m-1}$$

with $0 \leq \varepsilon_i, \gamma_i \leq 1$, *then*

1. *when* $q = 0$ *equality holds if and only if* $\varepsilon_i \geq \gamma_i, i = 0, 1, \cdots, m-1$,
2. *when* $q > 0$ *equality holds if and only if* $\varepsilon_i \geq \gamma_i, i = 0, 1, \cdots, m-3$ *and* $\gamma_{m-2}+\gamma_{m-1} \geq \varepsilon_{m-1}$ *if* $\varepsilon_{m-2} = 1$ *or* $\gamma_{m-2} = \varepsilon_{m-1}$ *if* $\varepsilon_{m-2} = 0$.

In some of what follows will use the following well known result:

Lemma 2.2. *For* $m \geq 3$,

$$\prod_{l=1}^{2^{m-1}} (2l-1) \equiv 1 \pmod{2^m}.$$

Proof. For $m = 3$ the result is trivial. We proceed by induciton on m. Suppose $\prod_{l=1}^{2^{k-1}}(2l-1) \equiv 1 \pmod{2^k}$ for some $k \geq 3$. Then

$$\prod_{l=1}^{2^k}(2l-1) = \prod_{l=2^{k-1}+1}^{2^k} (2l-1) \prod_{l=1}^{2^{k-1}} (2l-1)$$

$$= (2(2^k)-1)(2(2^k-1)-1)\cdots(2(2^k-2^{k-1}+2)-1)(2(2^k-2^{k-1}+1)-1) \prod_{l=1}^{2^{k-1}} (2l-1)$$

$$\equiv (-1)(-3)\cdots(-(2^k-3))(-(2^k-1)) \prod_{l=1}^{2^{k-1}} (2l-1) \pmod{2^{k+1}}$$

$$= (-1)^{2^{k-2}} \prod_{l=1}^{2^{k-1}} (2l-1) \prod_{l=1}^{2^{k-1}} (2l-1) = \left(\prod_{l=1}^{2^{k-1}} (2l-1) \right)^2.$$

But $\prod_{l=1}^{2^{k-1}}(2l-1) \equiv 1 \pmod{2^k}$ implies $\prod_{l=1}^{2^{k-1}}(2l-1) \equiv 1$ or $1+2^k \pmod{2^{k+1}}$. In both cases $\left(\prod_{l=1}^{2^{k-1}}(2l-1)\right)^2 \equiv 1 \pmod{2^{k+1}}$, for $(1+2^k)^2 = 1 + 2^{2k} + 2^{k+1} \equiv 1 \pmod{2^{k+1}}$.

□

Corollary 2.3. *The product of* 2^{j-1} *consecutive odd integers is congruent to* $1 \pmod{2^j}$.

Remark: Series multisection of binomial coefficients ([Ram34]) is a common technique for this type of problems. We tried to apply it to study the divisibility of the lacunary sums considered here but were unsuccessful.

3. Our Method in Action

In this section, we apply our method to a family of elementary symmetric Boolean functions. We compute its exact divisibility, which allows us to see that this family satisfies Cusick-Li-Stănică's conjecture. For this family we provide all the details in the proof and we label each step.

Theorem 3.1. *Let a, i, s be natural numbers with $i \geq 2^{s+1} + s - 4$. Suppose that $n = 2^a(2^i - 1)$ and $k = 2^a(2^{i-s} - 1)$. Then,*

$$\nu_2(S(\sigma_{n,k})) = 2^{s+1} - 1.$$

Proof. We label the steps as in the process described in the previous section.

1. Here k is of the form $2^a(2^{i-s}-1)$. By Lucas' therorem want to find all the j such that $k \preceq j$ and $j \leq n$. Hence $N(n,k) = \{j = k + l : \text{supp}(k) \cap \text{supp}(l) = \emptyset \text{ and } j \leq n\}$.
2. We conjecture $\nu_2\Big(\sum_{j \in N(n,k)} \binom{n}{j}\Big) = 2^{s+1} - 2$, so $\nu = 2^{s+1} - 1$.
3. We study the binomial coefficients in the sum $\sum_{j \in N(n,k)} \binom{n}{j}$ and show that some of these have valuation greater than or equal to $2^{s+1}-1$. Let $j \in N(n,k) \backslash \{k + t \cdot 2^{a+i-s} : t \in \mathbb{N} \cup \{0\}\}$. We have that

$$\nu_2\binom{n}{j} = w_2(j) + w_2(n-j) - w_2(n). \tag{9}$$

   It is clear that $j = k + l$, where $\text{supp}(k) \cap \text{supp}(l) = \emptyset$. Now,
   - $w_2(n) = i$,
   - $w_2(j) + w_2(n-j) = w_2(k) + w_2(l) + w_2(n-k-l) \geq i - s + 1 + i + 2$.

   Thus, we have that $w_2(j) + w_2(n-j) - w_2(n) = i - s + 1 + i + 2 - i = i - s + 3$. Since $i \geq 2^{s+1} + s - 4$, we have $\nu_2\binom{n}{j} \geq 2^{s+1} + s - 4 - s + 3 = 2^{s+1} - 1$.
4. Now we consider the binomials in the sum which have 2-adic valuation smaller than $2^{s+1} - 1$, and show that the 2-adic valuation of the sum of these binomials is equal to $2^{s+1} - 2$.

   Let $j \in \{k + t \cdot 2^{a+i-s} : t \in \mathbb{N} \cup \{0\}\}$. It is clear that $\nu_2\binom{n}{j} = 0 < 2^{s+1} - 1$. We have that $\sum_{j \in \{k + t \cdot 2^{a+i-s} : t \in \mathbb{N} \cup \{0\}\}} \binom{n}{j} = \sum_{t=0}^{2^s-1} \binom{n}{k + t \cdot 2^{a+i-s}}$. Now, by Corollary 2.1 we have that $\nu_2\Big(\sum_{t=0}^{2^s-1} \binom{n}{k + t \cdot 2^{a+i-s}}\Big) = 2^{s+1} - 2$.

We have showed that $\nu_2\Big(\sum_{\substack{j \in N(n,k) \\ \nu_2(\binom{n}{j})=0}} \binom{n}{j}\Big) = 2^{s+1}-2$ while $\nu_2\Big(\sum_{\substack{j \in N(n,k) \\ \nu_2(\binom{n}{j})\geq 1}} \binom{n}{j}\Big) \geq 2^{s+1}-1$, whuch implies $\nu_2(S(\sigma_{n,k})) = 2^{s+1} - 1$. □

4. Valuation of Elementary Symmetric Boolean Functions

In this section we compute the exact divisibility of two families of elementary Boolean functions. Also we apply our method to estimate the divisibility of families of elementary Boolean functions.

Theorem 4.1. *Let $n = 2^a(2^i - 1), k = 2^a(2^{i-2} + 2^{i-3} - 1)$ with $i \geq 6$. We have*

$$\nu_2(S(\sigma_{n,k})) = 4.$$

Proof. We have that the minimum is attained in $x = k, k + 2^{a+i-3}, k + 2^{a+i-1}, k + 2^{a+i-3} + 2^{a+i-1}$, ie., $\nu_2(\binom{n}{x}) = 0$. We need to prove

$$\binom{n}{k} \equiv 11 \bmod 16, \binom{n}{k + 2^{a+i-3}} \equiv 3 \bmod 16.$$

We have

$$\binom{n}{k} \equiv (\frac{40}{1}+1)(\frac{40}{2}+1)\cdots(\frac{40}{23}+1) \equiv 11 \bmod 16.$$

$$\binom{n}{k+2^{a+i-3}} \equiv (\frac{8}{1}+1)(\frac{8}{2}+1)\cdots(\frac{8}{7}+1) \equiv 3 \bmod 16.$$

Hence

$$\binom{n}{k} + \binom{n}{k+2^{a+i-3}} \equiv 11+3 \equiv 14 \bmod 16.$$

In similar manner we can prove that

$$\binom{n}{k+2^{a+i-1}} \equiv 9 \bmod 16, \binom{n}{k+2^{a+i-3}+2^{a+i-1}} \equiv 1 \bmod 16.$$

Hence

$$\binom{n}{k+2^{a+i-1}} + \binom{n}{k+2^{a+i-3}+2^{a+i-1}} \equiv 9+1 \equiv 10 \bmod 16.$$

Therefore

$$\binom{n}{k} + \binom{n}{k+2^{a+i-3}} + \binom{n}{k+2^{a+i-1}} + \binom{n}{k+2^{a+i-3}+2^{a+i-1}} \equiv 24 \bmod 16$$

We have proved that $\nu_2(\binom{n}{k} + \binom{n}{k+2^{a+i-3}} + \binom{n}{k+2^{a+i-1}} + \binom{n}{k+2^{a+i-3}+2^{a+i-1}}) = 3$. For $j \in N(n,k)$ and j is not a minimal solution, we have $\nu_2(\binom{n}{j}) \geq 4$. Let $A = \{k, k+2^{a+i-3}, k+2^{a+i-1}, k+2^{a+i-3}+2^{a+i-1}\}$. Then

$$S(\sigma_{n,k}) = 2^n - 2\Big(\sum_{j\in N(n,k)\setminus A}\binom{n}{j} + 8m\Big) = 2^n - 16m_1 + 8m,$$

where m is odd and m_1 is an integer. Now This completes the proof. □

Remark. The case for $i = 5$ can be computed but there two cases $a = 0, i = 5$ and $a > 0, i = 5$. For two cases we obtain the same divisibility $\nu_2(S(\sigma_{n,k})) = 4$.

Now, we consider a generalization of Theorem 4.1.

Theorem 4.2. *Let $n = 2^a(2^i-1), k = 2^a(2^{i-s}+2^{i-s-1}-1)$ with $i \geq 2^s+1$. We have*

$$\nu_2(S(\sigma_{n,k})) \geq 2^s.$$

Proof. We have that the minimum is attained at

$$x_i = k + a_1 2^{a+i-s+1} + a_2 2^{a+i-s+2} + \cdots + a_{s-1}2^{a+i-1}, a_i \in \{0,1\},$$

and

$$y_i = k + 2^{a+i-s-1} + b_1 2^{a+i-s+1} + b_2 2^{a+i-s+2} + \cdots + b_{s-1}2^{a+i-1}, b_i \in \{0,1\}$$

i.e., $\nu_2(\binom{n}{x_i}) = \nu_2(\binom{n}{y_i}) = 0$. Using Theorem 2.1, we have

$$\nu_2\Big(\sum_{j=0}^{2^{s-1}} \binom{n}{k + j2^{a+i-s+1}}\Big) = 2^s - 2$$

$$\nu_2\Big(\sum_{j=0}^{2^{s-1}} \binom{n}{k + 2^{a+i-s-1} + j2^{a+i-s+1}}\Big) = 2^s - 2.$$

Any other solution with $\binom{j}{k} \equiv 1 \bmod 2$ satisfies $\nu_2(\binom{n}{k}) > 2^s - 1$. Hence $\nu_2(S(\sigma_{n,k})) \geq 2^s$.

□

Example 4.3. The estimate given by Theorem 4.2 is an improvement to Ax's theorem. For example, if $i = 18$ and $s = 4$, we have that $\nu_2(S(\sigma_{2^a(2^{18}-1),2^a(2^{14}+2^{13}-1)})) \geq 16$. Ax's theorem implies that $\nu_2(S(\sigma_{2^a(2^{18}-1),2^a(2^{14}+2^{13}-1)})) \geq 11$. When the value of s increases, we get a much better estimate, i.e., $s = 15$. Our result is $\nu_2(S(\sigma_{n,k})) \geq 32768$, while Ax's result is $\nu_2(S(\sigma_{n,k})) \geq 21846$.

Our data suggests the following conjecture:

$$\nu_2\Big(\sum_{j=0}^{2^{s-1}} \binom{n}{k + j2^{a+i-s+1}} + \sum_{j=0}^{2^{s-1}} \binom{n}{k + 2^{a+i-s-1} + j2^{a+i-s+1}}\Big) = 2^s - 1.$$

Conjecture 4.4. *Let $n = 2^a(2^i - 1), k = 2^a(2^{i-s} + 2^{i-s-1} - 1)$ with $i \geq 2^s + 1$. We have*

$$\nu_2(S(\sigma_{n,k})) = 2^s.$$

Now we estimate the divisibility of another family.

Theorem 4.5. *Let a, i be natural numbers with $i \geq 2^{s+1} + s - 2$ and $a \geq 2$. Suppose that $n = 2^a(2^i - 1) + 1$ and $k = 2^a(2^{i-s} - 1)$. Then,*

$$\nu_2(S(\sigma_{n,k})) \geq 2^{s+1} - 1.$$

Proof. This result follows from the aplication of Theorem 2.1 twice.

We want to show $\nu_2\Big(\sum_{j\in N(n,k)} \binom{n}{j}\Big) \geq 2^{s+1}-1$. We do this by showing that $\nu_2\Big(\sum_{\substack{j\in N(n,k)\\ \nu_2(\binom{n}{j})=0}} \binom{n}{j}\Big) \geq 2^{s+1} - 1$ while $\nu_2\Big(\sum_{\substack{j\in N(n,k)\\ \nu_2(\binom{n}{j})\geq 1}} \binom{n}{j}\Big) \geq 2^{s+1}$.

Let $j \in \{k + t \cdot 2^{a+i-s} : t \in \mathbb{N} \cup \{0\}\}$. It is clear that $\nu_2\binom{n}{j} = 0$. We have that $\sum_{j\in\{k+t\cdot 2^{a+i-s}:t\in\mathbb{N}\cup\{0\}\}} \binom{n}{j} = \sum_{t=0}^{2^s-1} \binom{n}{k+t\cdot 2^{a+i-s}}$. Now, by Theorem 2.1 we have that $\nu_2\Big(\sum_{t=0}^{2^s-1} \binom{n}{k+t\cdot 2^{a+i-s}}\Big) = 2^{s+1} - 2$.

Let $j \in \{k + 1 + t \cdot 2^{a+i-s} : t \in \mathbb{N} \cup \{0\}\}$. It is clear that $\nu_2\binom{n}{j} = 0$. We have that $\sum_{j\in\{k+1+t\cdot 2^{a+i-s}:t\in\mathbb{N}\cup\{0\}\}} \binom{n}{j} = \sum_{t=0}^{2^s-1} \binom{n}{k+1+t\cdot 2^{a+i-s}}$. Now, by Theorem 2.1 we have that $\nu_2\Big(\sum_{t=0}^{2^s-1} \binom{n}{k+1+t\cdot 2^{a+i-s}}\Big) = 2^{s+1} - 2$.

Therefore, $\nu_2\Big(\sum_{t=0}^{2^s-1}\binom{n}{k+t\cdot 2^{a+i-s}}+\sum_{t=0}^{2^s-1}\binom{n}{k+1+t\cdot 2^{a+i-s}}\Big)\geq 2^{s+1}-1$.

Now let $j\in N(n,k)\setminus(\{k+t\cdot 2^{a+i-s}:t\in\mathbb{N}\cup\{0\}\}\cup\{k+1+t\cdot 2^{a+i-s}:t\in\mathbb{N}\cup\{0\}\})$. We have that

$$\nu_2\binom{n}{j}=w_2(j)+w_2(n-j)-w_2(n). \tag{10}$$

It is clear that $j=k+l$, where $\mathrm{supp}(k)\cap\mathrm{supp}(l)=\emptyset$. Now,

- $w_2(n)=i+1$,
- $w_2(j)+w_2(n-j)=w_2(k)+w_2(l)+w_2(n-k-l)\geq i-s+1+i+3$.

Thus, we have that $w_2(j)+w_2(n-j)-w_2(n)=i-s+1+i+3-i-1=i-s+3$. Hence, if we take $i\geq 2^{s+1}+s-3$, then $\nu_2\binom{n}{j}\geq 2^{s+1}+s-3-s+3=2^{s+1}$.

□

5. Exact Divisibility of a Exponential Sums of the Type Rodier-Moreno-Moreno

In [**?**, **?**], the authors give counterexamples of Cartliz-Uchiyama's conjecture. They considered exponential sums associated polynomials in one variable of degree 2^s-1 over the finite field $\mathbb{F}_{2^{sm}}$. In the authors continued the computation of the divisibility exponential sums with leader monomial $x_1^{2^s-1}\cdots x_n^{2^s-1}$. Motivated by this, we compute the exact divisibility of the symmetric Boolean functions of degree 2^s-1 in $(2^{sm}-1)$-variables. Sometimes the calculation of the exact divisibility of a exponential sum implies the exact value of the exponential sum. Our method can be applied to compute the value of a family of elementary symmetric Boolean functions.

Theorem 5.1. *Let $k=2^s-1$, $n=2^{sm}-1$ and $0<k_1<\cdots<k_r<2^s-1$. Then*

$$\nu_2(S(\sigma))=2^{sm+1-s}-1$$

where $\sigma=\sigma_{n,2^s-1}+\sigma_{n,k_r}+\cdots+\sigma_{k_1}$.

Proof. We have that

$$N(n,2^s-1,k_r\ldots,k_1)=\{j\mid\binom{j}{2^s-1}+\binom{j}{k_r}+\cdots+\binom{j}{k_1}\equiv 1 \bmod 2, 0\leq j\leq n\}$$

$$=\{j+i\cdot 2^s\mid\binom{j}{2^s-1}+\binom{j}{k_r}+\cdots+\binom{j}{k_1}\equiv 1 \bmod 2, 0\leq j\leq 2^s-1, j+i\cdot 2^s\leq n\}.$$

Let $A_i(j)=\{j+i\cdot 2^s\mid\binom{j}{2^s-1}+\binom{j}{k_r}+\cdots+\binom{j}{k_1}\equiv 1 \bmod 2,\}$, where $0\leq j\leq 2^s-1, j+i\cdot 2^s\leq n$. Using Theorem 2.1, we have $\nu_2(A_i(j))=2^{sm+1-s}-2$. The result follows from the fact that then number of j's satisfying $\binom{j}{2^s-1}+\binom{j}{k_r}+\cdots+\binom{j}{k_1}\equiv 1 \bmod 2, 0\leq j\leq 2^s-1$ is odd. □

Now we compute the value of a family of exponential sums associated to elementary symmetric Boolean functions.

Theorem 5.2. *Let $n=m\cdot 2^{s+1}, k=2^s+1$. Then $S(\sigma_{n,k})=2^{n-1}$.*

Proof. We need to find when $\binom{j}{k} \equiv 1 \bmod 2$. This happens when $j = l \cdot 2^r + 1 + 2i$ where l is odd with $1 \leq l \leq 2m$ and $i = 0, \ldots, 2^{r-1}$. There is a one to one correspondence between $\binom{n}{j}$ and $\binom{n}{n-j}$ satisfying

$$(-1)^{\binom{j}{k}+\binom{n-j}{k}} = -1 \text{ for } j \text{ odd.}$$

Let $A = \{j \mid \binom{j}{k} \equiv 1 \bmod 2,\ j \equiv 1 \bmod 2\}$ and $A' = \{j \mid \binom{j}{k} \equiv 0 \bmod 2,\ j \equiv 1 \bmod 2\}$. By the above argument

$$2^{n-1} = \sum_{\substack{j=1,\\ j:odd}}^{n} \binom{n}{j} = \sum_{j \in A} \binom{n}{j} + \sum_{j \in A'} \binom{n}{j} = 2 \sum_{j \in A} \binom{n}{j}.$$

Therefore $\sum_{j \in A} \binom{n}{j} = 2^{n-2}$. We have

$$S(\sigma_{n,k}) = 2^n - 2(\sum_{j \in A} \binom{n}{j}) = 2^n - 2^{n-1} = 2^{n-1}.$$

□

Remark. In [CLS09], the authors proved Theorem 5.2 using other method.

6. Conclusion and conjectures

In this paper we introduced a divisibility method for symmetric Boolean functions. We included several applications of our method to show the simplicity and efficiency. Our method is a good tool to get information about symmetric Boolean functions when the 2-expansion of its degree contains many ones(see the theorems of this paper).

Conjecture 6.1. *Let a, i be natural numbers with $i \geq 2^{s+1} + s$ and $a \geq 2$. Suppose that $n = 2^a(2^i - 1) + r$, $r = 0, 1$ and $k = 2^a(2^{i-s}m - 1)$. Let $m = 2^l + q$ with $q < 2^l$ be an odd number. Then,*

$$\nu_2(S(\sigma_{n,k})) = \begin{cases} 2(2^{s-l} - w_2(m) + l) + r + 1 & \text{if } l = 0, \\ 2^{s-l} - w_2(m) + l + r + 1 & \text{if } l \geq 1. \end{cases}$$

Acknowledgments. This research was supported by a National Science Foundation grant (#DMS1148695) through the Center for Undergraduate Research (CURM), Brigham Young University, and corporate sponsors. Also, partial support was provided to the second and fourth authors by the Claude Shannon Scholarship, NSF-UPR-RP-Scholarship Fund for Excellence in Computer Science and Mathematics (NSF-DUE 1356474), and to the second author by the Mellon-Mays Undergraduate Fellowship. The third author acknowledges the partial support of UPR-FIPI 1890015.00.

References

[CGM15] F. N. Castro, O. E. Gonzalez, and L. A. Medina. A divisibility approach to the open boundary cases of Cusick-Li-Stănică's conjecture. *Cryptography and Communications*, DOI: 10.1007/s12095-015-0124-y, 2015.

[CLS08] T. W. Cusick, Y. Li, and P. Stănică. Balanced symmetric functions over GF(p). *IEEE Trans. on Information Theory*, 5:1304–1307, 2008.

[CLS09] T.W. Cusick, Y. Li, and P. Stănică. On a conjecture for balanced symmetric Boolean functions. *J. Math. Crypt.*, 3:1–18, 2009.

[CM11] F. N. Castro and L. A. Medina. Linear recurrences and asymptotic behavior of exponential sums of symmetric Boolean functions. *Elec. J. Combinatorics*, 18:8, 2011.

[GGZ12] Y. Guo, G. Gao, and Y. Zhao. Recent results on balanced symmetric Boolean functions. *iacr.org (eprint)*, (93), 2012.

[GLZ11] G. Gao, W. Liu, and X. Zhang. The degree of balanced elemetary symmetric boolean functions of 4k + 3 variables. *IEEE Trans. on Information Theory*, 57:4822–4825, 2011.

[Ram34] C. Ramus. Solution générale d'un problème d'analyse combinatoire. *J. Reine Angew. Math*, 11:353–355, 1834.

[STP13] W. Su, X. Tang, and A. Pott. A note on a conjecture for balanced elementary symmetric Boolean functions. *IEEE Trans. on Information Theory*, 59:665–671, 2013.

[TL04] G. Tollisen and T. Lengyel. A congruential identity and the 2-adic order of lacunary sums of binomial coeficients. *INTEGERS*, 4(A04), 2004.

Department of Mathematics, University of Puerto Rico, San Juan, PR 00931

E-mail address: franciscastr@gmail.com

Department of Mathematics, University of Puerto Rico, San Juan, PR 00931

E-mail address: oscar.gonzalez3@upr.edu

Department of Mathematics, University of Puerto Rico, San Juan, PR 00931

E-mail address: luis.medina17@upr.edu

Department of Computer Science, University of Puerto Rico, San Juan, PR 00931

E-mail address: raul.negron3@upr.edu

Department of Computer Science, University of Puerto Rico, San Juan, PR 00931

E-mail address: iverubio@gmail.com