A DIVISIBILITY APPROACH TO THE OPEN BOUNDARY CASES OF CUSICK-LI-STĂNICĂ'S CONJECTURE

FRANCIS N. CASTRO, OSCAR E. GONZÁLEZ, AND LUIS A. MEDINA

Abstract. In this paper we compute the exact 2-divisibility of exponential sums associated to elementary symmetric Boolean functions. Our computation gives an affirmative answer to most of the open boundary cases of Cusick-Li-Stănică's conjecture. As a byproduct, we prove that the 2-divisibility of these families satisfies a linear recurrence. In particular, we provide a new elementary method to compute 2-divisibility of symmetric Boolean functions.

1. Introduction

The theory of Boolean functions is one of the most active areas in combinatorics because of its applications and its beauty. In general, understanding the behavior of Boolean functions presents a challenge to mathematicians. The subject can be studied from the point of view of complexity theory or from the algebraic point of view as we do in this paper, where we compute the 2-divisibility of some families of symmetric Boolean functions.

Divisibility of Boolean functions is an active area of research and it has been used to classify some families, see [3, 4, 15, 19]. This part of the subject can be studied using the theory of exponential sums; a theory that is rich in literature, for example, see [1, 2, 7, 8, 9, 18, 20, 21, 22, 23, 24]. In this work, we study the 2-divisibility of some families of elementary symmetric Boolean functions. The number of variables and the degree of these Boolean functions come from the open cases of the Cusick-Li-Stănică conjecture ([10, 25]).

In [10], Cusick, Li and Stănică stated the following conjecture:

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.

In [11], the same authors proved the conjecture for elementary symmetric functions of odd degree (they also proved other cases). In [17], Gao, Liu, and Zhang proved most of the cases of the conjecture when the number of variables of the elementary symmetric function is congruent to 3 mod 4. Recently in [25], Su, Tang and Pott presented the known results about the conjecture. They also gave an affirmative answer to the conjecture for many open cases by proving that the Hamming weight of the considered elementary symmetric functions was less than 2^{n-1}. In [5], Castro and Medina proved an asymptotic version of the conjecture. Moreover, in [13], Guo, Gao and Zhao refined the result of [5] and provided a bound $N(k)$ such that the conjecture is true for $n > N(k)$. The bound $N(k)$ depends on the degree k of the elementary Boolean function. In [6], Castro and Medina proved an asymptotic

Date: August 14, 2014.

2010 *Mathematics Subject Classification.* Primary 33E20, 33B15.

generalization of Cusick-Li-Stănică's conjecture. The only remaining open cases of Cusick-Li-Stănică's conjecture are stated in Conjecture 1.1 ([25]). To properly state them, we need the following definition:

Definition 1.1. For $x \in \mathbb{F}_2^n$, let $w_2(x)$ be the Hamming weight of x, in other words, $w_2(x)$ is the number of entries of x that are one. For example, $w_2((0,1,1,0,1)) = 3$. If d is any non-negative integer, then we define the Hamming weight of d, denoted by $w_2(d)$, as the number of 1's in the binary representation of d.

Conjecture 1.1 (Cusick-Li-Stănică)**.** *Let $D \geq 3$ be odd, $a \geq 1$, $n = 2^{a+1}D + r$, $r = -1, 0, 1, 2$. The elementary symmetric Boolean function $\sigma_k(X_1, \ldots, X_n)$ is not balanced in the following cases:*

(1) $k = 2^{a+1}d'$, $w_2(d') \geq 2$, and $2 \leq d' \preceq \dfrac{D-1}{2}$ for $r = -1, 0, 1, 2$.

(2) $k = 2^{a+1}d' + 2^a$, $w_2(d') \geq 2$, and $2 \leq d' \preceq \dfrac{D-1}{2}$ for $r = 0, 1, 2$.

In this paper we introduce a new approach to compute the exact 2-divisibility of elementary symmetric functions. In general, computing the exact 2-divisibility of Boolean functions is a hard problem due to their "randomness". We prove that the 2-divisibility of the families considered here satisfies a linear recurrence relation. As a byproduct, we prove that Cusick-Li-Stănică's conjecture holds for most of the open boundary cases. Our method to compute divisibility is elementary and can be applied to perturbations of elementary symmetric Boolean functions. However, we omit these results because they are not directly linked to the open cases of Conjecture 1.1.

The divisibility of the entries of the rows in Pascal's triangle has been studied in [12, 14, 16]. In this work, to obtain our results we need to estimate the divisibility of subsequences of the entries of the rows in Pascal's triangle. Those results are of independent interest.

2. Preliminaries

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

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

A Boolean function F is called balanced if $S(F) = 0$, i.e. the number of zeros and the number of ones are equal in the truth table of F. This property is important for some applications in cryptography. Our aim is to compute the highest power of 2 dividing $S(F)$ for the case when $F(\mathbf{X})$ is an elementary 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 $\sigma_{n,k} = \sigma_k(X_1, \ldots, X_n)$ be the elementary symmetric polynomial in n variables of degree k. For example,

$$\sigma_{5,3} = \sigma_3(X_1, \ldots, X_5) = \sum_{1 \leq i_1 < i_2 < i_3 \leq 5} X_{i_1} X_{i_2} X_{i_3}. \tag{2}$$

It is not hard to see that, in the case of an elementary symmetric polynomial, the exponential sum can be written as

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

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

$$S(\sigma_{n,k}) \;=\; 2^n - 2 \sum_{j \in N(n,k)} \binom{n}{j}. \tag{4}$$

Thus, if $S(\sigma_{n,k}) \neq 0$, then

$$\nu_2(S(\sigma_{n,k})) = \nu_2 \left(2 \sum_{j \in N(n,k)} \binom{n}{j} \right). \tag{5}$$

In other words, computing the exact divisibility of $\displaystyle\sum_{j \in N(n,k)} \binom{n}{j}$ yields the exact divisibility of $S(\sigma_{n,k})$.

We point out that the classical theorem of Ax ([2]) implies

$$\nu_2(\sigma_{n,k}) \geq \left\lceil \frac{n}{k} \right\rceil. \tag{6}$$

For our families, Ax's result implies that 2^ν divides $S(\sigma_{n,k})$ where $\nu = 2$ or 3. Our results greatly improve Ax's theorem for these families.

3. Boundary case for $r = 0$

In this section we consider the boundary case of Cusick-Li-Stănică's conjecture for $r = 0$. In other words, we explore whether or not the exponential sum of $\sigma_{n,k}$ is different from 0 for $n = 2^a D$ and

$$k = 2^a \left(\frac{D-1}{2} \right) \text{ or } k = 2^a \left(\frac{D-1}{2} \right) + 2^{a-1} = 2^{a-1} D,$$

where $D \geq 3$ is odd and $a \geq 2$. Notice that we replaced the power 2^{a+1} in Conjecture 1.1 with 2^a. Therefore, Cusick-Li-Stănică's conjecture is now re-stated as:

Conjecture 3.1 (Cusick-Li-Stănică)**.** *Let $D \geq 3$ be odd, $a \geq 2$, $n = 2^a D + r$, $r = -1, 0, 1, 2$. The elementary symmetric Boolean function $\sigma_k(X_1, \ldots, X_n)$ is not balanced in the following cases:*

(1) $k = 2^a d'$, $w_2(d') \geq 2$, and $2 \leq d' \preceq \frac{D-1}{2}$ for $r = -1, 0, 1, 2$.

(2) $k = 2^a d' + 2^a$, $w_2(d') \geq 2$, and $2 \leq d' \preceq \frac{D-1}{2}$ for $r = 0, 1, 2$.

Since D is an odd natural number, then it has the form $D = 2^i m - 1$, where $i \geq 1$ and m is an odd natural number. We re-write $n = 2^a(2^i m - 1) + r$ and

$$k = 2^a(2^{i-1} m - 1) \text{ or } k = 2^a(2^{i-1} m - 1) + 2^{a-1}.$$

We show the veracity of Cusick-Li-Stănică's conjecture for a large part of this boundary case. We achieve this by computing the exact 2-divisibility of the exponential sum for families of polynomials that are included in this case. We study first the case $n = 2^a(2^i m - 1)$ and $k = 2^a(2^{i-1}m - 1) + 2^{a-1}$. It turns out that this case is simpler than the case $k = 2^a(2^{i-1}m - 1)$. We start with an example.

Example 3.1. Suppose that $a = 2$ and $i = 3$. In this case, $n = 32m - 4$ and $k = 16m - 2$. The first few values of $\nu_2(S(\sigma_{n,k}))$, when m runs through the odd positive integers, are given by

$$4, 5, 5, 6, 5, 6, 6, 7, 5, 6, 6, 7, 6, 7, 7, 8, 5, 6, 6, 7, \cdots .$$

In Figure 1 you can see a graphical representation of these numbers. Note that this information suggests that $S(\sigma_{32m-4,16m-2})$ is not balanced, since its valuation is always finite. Moreover, it seems by observing the data that there is a pattern in it. We will try to describe it. We write $m = 2j - 1$ and let

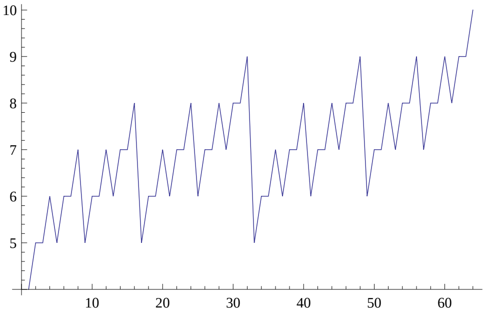

Figure 1. Graphical representation of $\nu_2(S(\sigma_{32m-4,16m-2}))$.

$$t_j = \nu_2(S(\sigma_{32((2j-1)-4),16((2j-1)-1)-2})). \tag{7}$$

We are now interested in the values of the sequence $t_1, t_2, \cdots, t_s, \cdots$, which are plotted in Figure 1. To decipher the pattern, we plot the differences of the values $t_{j+1} - t_j$, as in Figure 2. The alert reader may observe a pattern in this graph. We now multiply the graph of Figure 2 by -1 and add 1 to the result to obtain the graph in Figure 3. The reader can identify this picture with the 2-adic valuation of

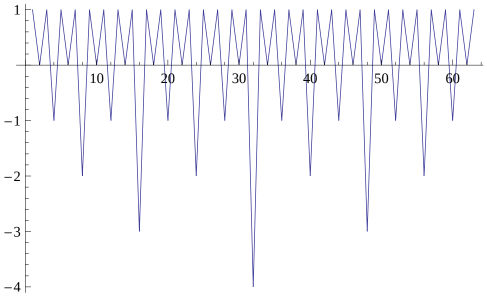

Figure 2. The graph of the values of $t_{j+1} - t_j$.

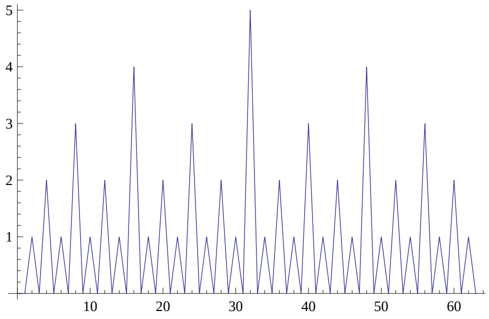

FIGURE 3. The graph of the values of $t_j - t_{j+1} + 1$.

the integers, i.e. $\nu_2(j)$ for $j = 1, 2, 3, \cdots$. In other words, it looks like the sequence $\{t_j\}_{j\in\mathbb{N}}$ satisfies the recurrence

$$t_j - t_{j+1} + 1 = \nu_2(j). \tag{8}$$

The general solution to (8) is $w_2(2j-1) + c$, where c is some constant. Thus, if all of this is true, then

$$\nu_2(S(\sigma_{32m-4,16m-2})) = w_2(m) + c. \tag{9}$$

In Figure 4 you can see a graphical representation of $\nu_2(S(\sigma_{32m-4,16m-2}))$ versus $w_2(m)$ for m odd. The blue graph represents $\nu_2(S(\sigma_{32m-4,16m-2}))$ while the red graph represents $w_2(m)$. Observe that it appears that $c = 3$, i.e.

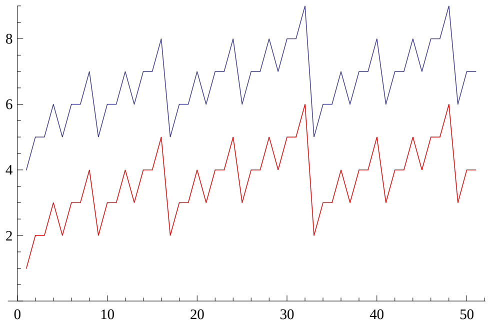

FIGURE 4. Graphical representation of $\nu_2(S(\sigma_{32m-4,16m-2}))$ vs $w_2(m)$ for m odd.

$$\nu_2(S(\sigma_{32m-4,16m-2})) = w_2(m) + 3. \tag{10}$$

Example 3.2. Suppose now that $a = 2$ and $i = 4$. In this case, $n = 64m - 4$ and $k = 32m - 2$. The first few values of $\nu_2(S(\sigma_{n,k}))$, when m runs through the odd positive integers, are given by

$$5, 6, 6, 7, 6, 7, 7, 8, 6, 7, 7, 8, 7, 8, 8, 9, 6, 7, 7, 8, \cdots.$$

Again, note that these values are simply the weight of the odd numbers shifted by a constant, which in this case is 4.

In general, computer experiments suggest that the 2-adic valuation of $S(\sigma_{n,k})$, for $n = 2^a(2^i m - 1)$ and $k = 2^a(2^i m - 1) + 2^{a-1}$, depends on i and on the weight of m, but not on a. This dependence is stated in the next theorem.

Definition 3.3. Let $m = 2^{i_0} + \cdots + 2^{i_r}$ be the 2-expansion of m. We define the support of m by

$$\operatorname{supp}(m) = \{i_0, \ldots, i_r\}. \tag{11}$$

Theorem 3.2. *Suppose that a, i, and m are positive integers with m odd. Let $n = 2^a(2^i m - 1)$, $k = 2^a(2^{i-1} m - 1) + 2^{a-1}$. Then*

$$\nu_2(S(\sigma_{n,k})) = w_2(m) + i, \tag{12}$$

and so $\sigma_{n,k}$ is not balanced. In particular, if we write $m = 2j - 1$ and let

$$t_j = \nu_2(S(\sigma_{2^a(2^i(2j-1)-1),2^a(2^{i-1}(2j-1)-1)+2^{a-1}})), \tag{13}$$

then $\{t_j\}_{j\in\mathbb{N}}$ satisfies the recurrence,

$$\begin{aligned} t_1 &= i + 1, \\ t_{j+1} &= t_j - \nu_2(j) + 1. \end{aligned} \tag{14}$$

Thus, Cusick-Li-Stănică's conjecture is true for $n = 2^{a+1}D$ and $k = 2^a D$.

Proof. Recall that

$$\nu_2(S(\sigma_{n,k})) = \nu_2\left(\sum_{j\in N(n,k)} \binom{n}{j}\right) + 1. \tag{15}$$

Therefore, we must show that

$$\nu_2\left(\sum_{j\in N(n,k)} \binom{n}{j}\right) = w_2(m) + i - 1. \tag{16}$$

We start by noticing that $n = 2k$, and so

$$\nu_2\left(\binom{n}{k}\right) = w_2(n). \tag{17}$$

Suppose that $m = b_s \cdot 2^s + b_{s-1} \cdot 2^{s-1} + \cdots + b_1 \cdot 2 + 1$ with $s \geq 1$. Lucas' Theorem implies that $N(n,k) = \{k + m' \,|\, \operatorname{supp}(k) \cap \operatorname{supp}(m') = \emptyset, k + m' \leq n\}$. Since $n = 2^{a+i+1} + b_1 \cdot 2^{a+i+2} + \cdots + b_s \cdot 2^{a+i+s+1} - 2^a$, then

$$\nu_2\left(\binom{n}{k}\right) = w_2(n) = w_2(m) + i - 1. \tag{18}$$

Therefore, if we prove that

$$\nu\left(\binom{n}{k+m'}\right) \geq w_2(m) + i \tag{19}$$

for $m' \neq 0$, then we are done.

A direct calculation shows that

$$\begin{align}
\nu_2\left(\binom{n}{k+m'}\right) &= w_2(k+m') + w_2(n-k-m') - w_2(n) \notag\\
&= w_2(m) + i - 1 + w_2(m') + w_2(2^{a+i}m - 2^a - m') - w_2(m) - i + 1 \notag\\
&= w_2(m') + w_2(2^{a+i}m - 2^a - m') \tag{20}\\
&= w_2(m') + w_2(k-m') \notag\\
&\geq 1 + w_2(k) \notag\\
&= w_2(m) + i \notag
\end{align}$$

Observe that $w_2(k-m') \geq w_2(k)$ because $\mathrm{supp}(k) \cap \mathrm{supp}(m') = \emptyset$. We conclude that

$$\nu_2(S(\sigma_{n,k})) = w_2(m) + i. \tag{21}$$

Note that (14) follows from (21). This completes the proof. □

We now consider the case $n = 2^a(2^i m - 1)$ and $k = 2^a(2^{i-1}m - 1)$. As before, we start the study with an example.

Example 3.4. Let $a = 2$ and $i = 2$. Then $n = 16m - 4$ and $k = 8m - 4$. The first few values of $\nu_2(S(\sigma_{n,k}))$, when m runs through the odd positive integers, are given by

$$3, 4, 4, 5, 4, 5, 5, 6, 4, 5, 5, 6, 5, 6, 6, 7, 4, 5, 5, 6, \cdots$$

As before, it appears that the valuation depends on the weight of m, in this case $\nu_2(\sigma_{16m-4,8m-4}) = w_2(m) + 2$. In fact, the reader can check via computer experiments that as long as $i \geq 2$, the 2-adic valuation of $S(\sigma_{n,k})$ is always $w_2(m) + 2$. In other words, as for the previous k, the 2-adic valuation does not depend on a. However, a major difference is that now the 2-adic valuation does not depend on i either.

We now present the proof this fact. Our proof of the theorem depends on the following elementary result.

Lemma 3.3. *Let a, i, m be natural numbers with $i \geq 3$ and m odd. Write $m = b_s \cdot 2^s + b_{s-1} \cdot 2^{s-1} + \cdots + b_1 \cdot 2 + 1$ with $s \geq 1$. Let $b_{s-l_1}, b_{s-l_2}, \ldots, b_{s-l_r}$ be all the b_t in the expansion of m such that $b_t = 0$. Define*

$$b_{a,i} = \delta_1 \cdot 2^{a+i-1+(s-l_1)} + \cdots + \delta_r \cdot 2^{a+i-1+(s-l_r)}$$

Then,

$$\frac{(2^{a+i-1} \cdot m - 2^a + b_{a,i} + 2^{a+i-1}) \cdots (2^{a+i-1} \cdot m - 2^a + b_{a,i} + 1)}{(2^{a+i-1} \cdot m - b_{a,i}) \cdots (2^{a+i-1} \cdot m - b_{a,i} - 2^{a+i-1} + 1)} \equiv 3 \bmod 4. \tag{22}$$

Remark. Our proof of Lemma 3.3 is elementary, but rather tedious (it depends on a double induction!). As a result, we decided not to present the proof of the lemma in this manuscript. However, the interested reader can find our proof on the following website:

`http://emmy.uprrp.edu/lmedina/papers/cusick/`

Theorem 3.4. *Let a, i, m be natural numbers with $i \geq 2$ and m odd. Suppose that $n = 2^a(2^i m - 1)$ and $k = 2^a(2^{i-1}m - 1)$. Then,*

$$\nu_2(S(\sigma_{n,k})) = w_2(m) + 2,$$

and so $\sigma_{n,k}$ is not balanced. In particular, if we write $m = 2j-1$ and let

$$t_j = \nu_2(S(\sigma_{2^a(2^i(2j-1)-1),2^a(2^{i-1}(2j-1)-1)})), \tag{23}$$

then $\{t_j\}_{j\in\mathbb{N}}$ satisfies the recurrence,

$$\begin{aligned} t_1 &= 3, \\ t_{j+1} &= t_j - \nu_2(j) + 1. \end{aligned} \tag{24}$$

Thus, Cusick-Li-Stănică's conjecture is true for $n = 2^{a+1}D$ and $k = 2^a(D-1)$ for $D \equiv 3 \bmod 4$.

Proof. We only present the proof for $i \geq 3$. The case $i = 2$ can be treated in a similar manner.

Suppose that m is odd. Then m can be written as $m = b_s \cdot 2^s + b_{s-1} \cdot 2^{s-1} + \cdots + b_1 \cdot 2 + 1$ with $s \geq 1$. Let $b_{s-l_1}, b_{s-l_2}, \ldots, b_{s-l_r}$ be all the b_t in the expansion of m such that $b_t = 0$. By Lucas' Theorem $j \in N(n,k)$ if and only if

$$j = k + \delta_1 \cdot 2^{a+i-1+s-l_1} + \delta_2 \cdot 2^{a+i-1+s-l_2} + \cdots + \delta_r \cdot 2^{a+i-1+s-l_r} + t_{r+1} \cdot 2^{a+i-1} + \delta,$$

where $\delta_i \in \{0,1\}$ and $0 \leq \delta \leq 2^a - 1$. We divide the proof in two cases: $m = 1$ and $m > 1$.

Case $m > 1$: We consider first the case $m > 1$. Let

$$\begin{aligned} b_{a,i} &= \delta_1 \cdot 2^{a+i-1+(s-l_1)} + \cdots + \delta_r \cdot 2^{a+i-1+(s-l_r)}, \\ l_{a,i} &= k + b_{a,i}, \\ l'_{a,i} &= k + b_{a,i} + 2^{a+i-1}, \end{aligned}$$

where $\delta_t \in \{0,1\}$, $(s - l_t)$ is such that 2^{s-l_t} does not appear in the expansion of m, and at least one of the $\delta_t \neq 0$. We will show that

(a) $\nu_2\left(\binom{n}{l_{a,i}} + \binom{n}{l'_{a,i}}\right) \geq w_2(m) + 2$,

(b) $\nu_2\left(\binom{n}{k} + \binom{n}{k+2^{a+i-1}}\right) = w_2(m) + 1$, and

(c) $\nu_2\left(\binom{n}{j}\right) \geq w_2(m) + 2$ for all remaining $j \in N(n,k)$.

Note that this implies the result for this case.

Case $m > 1$, part (a):

Expand $\binom{n}{l_{a,i}}$ to obtain,

$$\binom{2^{a+i}\cdot m - 2^a}{2^{a+i-1}\cdot m - 2^a + b_{a,i}} = \frac{(2^{a+i}\cdot m - 2^a)\cdots(2^{a+i-1}\cdot m - 2^a + b_{a,i} + 1)}{(2^{a+i-1}\cdot m - b_{a,i})\cdots 2\cdot 1}. \tag{25}$$

Now expand $\binom{n}{l'_{a,i}}$ to obtain,

$$\binom{2^{a+i}\cdot m - 2^a}{2^{a+i-1}\cdot m - 2^a + b_{a,i} + 2^{a+i-1}} = \frac{(2^{a+i}\cdot m - 2^a)\cdots(2^{a+i-1}\cdot m - 2^a + b_{a,i} + 2^{a+i-1} + 1)}{(2^{a+i-1}\cdot m - b_{a,i} - 2^{a+i-1})\cdots 2\cdot 1}. \tag{26}$$

Consider now the sum of these two binomials and observe that

$$\binom{n}{l_{a,i}}+\binom{n}{l'_{a,i}} = \binom{n}{l'_{a,i}}\left(\frac{(2^{a+i-1}\cdot m-2^a+b_{a,i}+2^{a+i-1})\cdots(2^{a+i-1}\cdot m-2^a+b_{a,i}+1)}{(2^{a+i-1}\cdot m-b_{a,i})\cdots(2^{a+i-1}\cdot m-b_{a,i}-2^{a+i-1}+1)}+1\right).$$

The 2-adic valuation of $\binom{n}{l'_{a,i}}$ satisfies the inequality,

$$\begin{aligned}
&\nu_2\left(\binom{2^{a+i}m-2^a}{2^{a+i-1}m-2^a+b_{a,i}+2^{a+i-1}}\right)\\
&= w_2(2^{a+i-1}m-2^a+b_{a,i}+2^{a+i-1})+w_2(2^{a+i-1}\cdot m-b_{a,i}-2^{a+i-1})-w_2(2^{a+i}\cdot m-2^a)\\
&= w_2(2^{a+i-1}m-2^a+b_{a,i}+2^{a+i-1})+w_2(m-\delta_1\cdot 2^{s-l_1}-\cdots-\delta_r\cdot 2^{s-l_r}-1)-w_2(2^i\cdot m-1)\\
&\geq w_2(2^{i-1}\cdot m+\delta_1\cdot 2^{i-1+(s-l_1)}+\cdots+\delta_r\cdot 2^{i-1+(s-l_r)}+(2^{i-1}-1))\\
&\quad +(w_2(m)-1)-(w_2(m)+i-1)\\
&\geq w_2(m)+i+w_2(m)-1-w_2(m)-i+1=w_2(m).
\end{aligned}$$

Therefore, the problem is reduced to proving that

$$\frac{(2^{a+i-1}\cdot m-2^a+b_{a,i}+2^{a+i-1})\cdots(2^{a+i-1}\cdot m-2^a+b_{a,i}+1)}{(2^{a+i-1}\cdot m-b_{a,i})\cdots(2^{a+i-1}\cdot m-b_{a,i}-2^{a+i-1}+1)}\equiv 3 \bmod 4. \tag{27}$$

This is Lemma 3.3. This concludes the proof of part (a).

Case $m>1$, part (b):

In this part we show that

$$\nu_2\left(\binom{n}{k}+\binom{n}{k+2^{a+i-1}}\right)=w_2(m)+1. \tag{28}$$

Expand the binomial coefficients to obtain

$$\binom{n}{k}=\frac{(2^{a+i}\cdot m-2^a)\cdots(2^{a+i-1}\cdot m-2^a+1)}{(2^{a+i-1}\cdot m)\cdots 2\cdot 1} \tag{29}$$

and

$$\binom{n}{k+2^{a+i-1}}=\frac{(2^{a+i}\cdot m-2^a)\cdots(2^{a+i-1}\cdot m+2^{a+i-1}-2^a+1)}{(2^{a+i-1}\cdot m-2^{a+i-1})\cdots 2\cdot 1}. \tag{30}$$

Now consider the sum $\binom{n}{k}+\binom{n}{k+2^{a+i-1}}$ and factor $\binom{n}{k+2^{a+i-1}}$ to get the expression

$$\binom{n}{k+2^{a+i-1}}\left(\frac{(2^{a+i-1}\cdot m+2^{a+i-1}-2^a)\cdots(2^{a+i-1}\cdot m-2^a+1)}{(2^{a+i-1}\cdot m)\cdots(2^{a+i-1}\cdot m-2^{a+i-1}+1)}+1\right).$$

Observe that

$$\begin{aligned}
&\nu_2\left(\binom{n}{k+2^{a+i-1}}\right)\\
&= w_2(k+2^{a+i-1}) + w_2(n-k-2^{a+i-1}) - w_2(n)\\
&= w_2(2^{a+i-1}\cdot m + 2^{a+i-1} - 2^a) + w_2(2^{a+i-1}\cdot m - 2^{a+i-1}) - w_2(2^{a+i}\cdot m - 2^a)\\
&= w_2(2^{i-1}\cdot m + 2^{i-1} - 1) + w_2(m-1) - w_2(2^i\cdot m - 1)\\
&= w_2(2^{i-1}\cdot m + (1+2+\cdots+2^{i-2})) + w_2(m) - 1 - (w_2(m)+i-1)\\
&= w_2(m) + i - 1 + w_2(m) - 1 - w_2(m) - i + 1 = w_2(m) - 1
\end{aligned}$$

Hence, if

$$\frac{(2^{a+i-1}\cdot m + 2^{a+i-1} - 2^a)\cdots(2^{a+i-1}\cdot m - 2^a + 1)}{(2^{a+i-1}\cdot m)\cdots(2^{a+i-1}\cdot m - 2^{a+i-1} + 1)} \equiv 3 \bmod 8, \tag{31}$$

we are done. However, this can be proved using an argument similar to the double induction of Lemma 3.3. We conclude that

$$\nu_2\left(\binom{n}{k} + \binom{n}{k+2^{a+i-1}}\right) = w_2(m) + 1. \tag{32}$$

This finishes the proof of part (b).

<u>Case $m > 1$, part (c):</u>

In this part we show that both,

$$\nu_2\left(\binom{n}{k+b_{a,i}+\delta}\right) \text{ and } \nu_2\left(\binom{n}{k+b_{a,i}+\delta+2^{a+i-1}}\right), \tag{33}$$

where $0 < \delta \leq 2^a - 1$, are bigger than or equal to $w_2(m)+2$.

Start with the first term in (33). Note that its valuation satisfies the inequality,

$$\begin{aligned}
&\nu_2\left(\binom{n}{k+b_{a,i}+\delta}\right) = w_2(k+b_{a,i}+\delta) + w_2(n-k-b_{a,i}-\delta) - w_2(n)\\
&= w_2(2^{a+i-1}\cdot m - 2^a + b_{a,i} + \delta) + w_2(2^{a+i-1}\cdot m - b_{a,t} - \delta) - w_2(2^{a+i}\cdot m - 2^a)\\
&\geq w_2(m) + i + w_2(m) + 1 - (w_2(m) + i - 1)\\
&\geq w_2(m) + 2.
\end{aligned}$$

For the second term, observe that

$$\begin{aligned}
&\nu_2\left(\binom{n}{k+b_{a,i}+\delta+2^{a+i-1}}\right) = w_2(k+b_{a,i}+\delta+2^{a+i-1}) + w_2(n-k-b_{a,i}-\delta-2^{a+i-1}) - w_2(n)\\
&= w_2(2^{a+i-1}\cdot m - 2^a + b_{a,i} + t + 2^{a+i-1}) + w_2(2^{a+i-1}\cdot m - b_{a,i} - \delta - 2^{a+i-1}) - w_2(2^{a+i}\cdot m - 2^a)\\
&\geq w_2(m) + i + w_2(m) + 1 - (w_2(m) + i - 1)\\
&\geq w_2(m) + 2.
\end{aligned}$$

This concludes part (c) and, therefore, the case $m > 1$.

<u>Case $m = 1$:</u> This case turns out to be rather simple. The reader can check that

$$\nu_2\left(\binom{n}{k} + 1\right) = w_2(m) + 1 = 2, \tag{34}$$

while

$$\nu_2\left(\binom{n}{j}\right) \geq 3 \tag{35}$$

for all other values of $j \in N(n,k)$. This concludes the proof of the theorem. □

In terms of the parameters a and i, we have proved the veracity of Cusick-Li-Stănică's conjecture for all values of the parameters, except for the case $i = 1$. This case is different from the case $i \geq 2$ in the sense that $\nu_2(\sigma_{2^a(2m-1),2^a(m-1)})$ is not of the form $w_2(m) + c$ for some constant c.

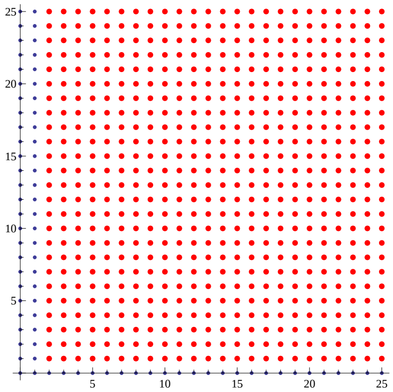

FIGURE 5. Let $n = 2^a(2^i m - 1)$ and $k = 2^a(2^{i-1}m - 1)$. The red dots represent pairs (i, a) for which the conjecture is true.

Example 3.5. Let $a = 2$, $i = 1$, and $m = 25$, then, $n = 196$ and $k = 96$. Note that $w_2(m) = 3$ and $\nu_2(S(\sigma_{196,96})) = 10 = w_2(m) + 7$. However, if $a = 2$, $i = 1$ and $m = 41$, then $n = 324$ and $k = 160$. In this case, $w_2(41) = 3$ and $\nu_2(S(\sigma_{324,160})) = 8 = w_2(m) + 5$.

We will present a study of this case in section 6.

4. Boundary case for $r = 1$ and $r = 2$

In this section we consider the boundary cases of Cusick-Li-Stănică's conjecture for $r = 1$ and $r = 2$. As in the previous section, we explore the veracity of the conjecture by computing the exact 2-divisibility of $S(\sigma_{n,k})$.

We only present the study of the case $r = 1$. Our results can be easily extended to the case $r = 2$. We start with the case $k = 2^a(2^{i-1}m - 1)$.

Example 4.1. Suppose that $a = 2$ and $i = 2$. Then, $n = 16m - 3$ and $k = 8m - 4$. As m runs through the positive odd numbers, the sequence $\nu_2(S(\sigma_{16m-3,8m-4}))$ obtains the values

$$4, 5, 5, 6, 5, 6, 6, 7, 5, 6, 6, 7, 6, 7, 7, 8, 5, 6, 6, 7, \cdots$$

Compare these values with the ones from $\nu_2(S(\sigma_{16m-4,8m-4}))$ in Example 3.4. Note that each term is one more than the corresponding one in the list of $\nu_2(S(\sigma_{16m-4,8m-4}))$.

In other words, the sequence appears to be $w_2(m)+3$. In particular, this seems to be true for all values of $a \geq 2$ and $i \geq 2$, i.e. for this particular n and k we have

$$\nu_2(S(\sigma_{n,k})) = \nu_2(S(\sigma_{n-1,k})) + 1. \tag{36}$$

We suspect that this can be proved directly using an argument similar to the one in Theorem 3.4. We provide a proof for (36) that reduces the case $r=1$ to the case $r=0$. However, by doing this, we only prove (36) for $a \geq 3$ and $i \geq 3$.

Theorem 4.1. *Suppose that a, i, and m are positive integers with $a \geq 3$, $i \geq 3$, and m odd. Let $n = 2^a(2^i m - 1) + 1$ and $k = 2^a(2^{i-1}m - 1)$. Then,*

$$\nu_2(S(\sigma_{n,k})) = w_2(m) + 3. \tag{37}$$

In particular, Cusick-Li-Stănică's conjecture is true for $n = 2^{a+1}D + 1$ and $k = 2^a(D-1)$ with $D \equiv -1 \bmod 8$ and $a \geq 2$.

Proof. We use the proof of Theorem 3.4 and the identity

$$S(\sigma_{n,k}) = S(\sigma_{n-1,k}) + S(\sigma_{n-1,k} + \sigma_{n-1,k-1}), \tag{38}$$

to prove this theorem. Note that $n-1 = 2^a(2^i m - 1)$, which is the case $r=0$. We analyze the terms $S(\sigma_{n-1,k})$ and $S(\sigma_{n-1,k} + \sigma_{n-1,k-1})$ individually.

We start with $S(\sigma_{n-1,k})$. We know that

$$\nu_2(S(\sigma_{n-1,k})) = w_2(m) + 2, \tag{39}$$

because

$$2 \sum_{j \in N(n-1,k)} \binom{n-1}{j} = 2^{w_2(m)+2}(m_1 + 2m_2), \tag{40}$$

with m_1 odd. To be specific,

$$2\left(\binom{n-1}{k} + \binom{n-1}{k+2^{a+i-1}}\right) = 2^{w_2(m)+2} m_1, \tag{41}$$

and the double of the sum of the remaining terms, i.e. all terms of the form

$$\binom{n-1}{k+b_{a,i}}, \ \binom{n-1}{k+b_{a,i}+2^{a+i-1}}, \text{ or } \binom{n-1}{k+b_{a,i}+l_{a,i}},$$

is $2^{w_2(m)+3} m_2$.

Consider now the term $S(\sigma_{n-1,k} + \sigma_{n-1,k-1})$. Note that

$$\begin{aligned} S(\sigma_{n-1,k} + \sigma_{n-1,k-1}) &= \sum_{j=0}^{n} (-1)^{\binom{j}{k}+\binom{j}{k-1}} \binom{n-1}{j} \\ &= \sum_{j=0}^{n} (-1)^{\binom{j+1}{k}} \binom{n-1}{j} \\ &= 2^{n-1} - 2 \sum_{j \in N(n-1,k)} \binom{n-1}{j-1}. \end{aligned} \tag{42}$$

Observe that as j runs through $N(n-1,k)$, $\binom{n-1}{j-1}$ takes the values

$$\binom{n-1}{k}, \ \binom{n-1}{k+2^{a+i-1}}, \ \binom{n-1}{k+b_{a,i}}, \ \binom{n-1}{k+b_{a,i}+2^{a+i-1}}, \tag{43}$$

values of the form

$$\binom{n-1}{k+b_{a,i}+l_{a,i}} \quad \text{(some of the values, not all)} \tag{44}$$

and the values

$$\binom{n-1}{k-1}, \binom{n-1}{k-1+2^{a+i-1}}, \binom{n-1}{k+b_{a,i}-1}, \binom{n-1}{k+b_{a,i}+2^{a+i-1}-1}. \tag{45}$$

The reader can check that if $a \geq 3$, then all the terms of (45) have valuation bigger than or equal to $w_2(m)+2$. Moreover, all terms of the form (44) have valuation bigger than or equal to $w_2(m)+i-1$. Thus, if $a \geq 3$ and $i \geq 3$, then

$$2 \sum_{j \in N(n-1,k)} \binom{n-1}{j-1} = 2^{w_2(m)+2}(m_1 + 2m_2'), \tag{46}$$

where m_2' has the same parity as m_2. We conclude that

$$\begin{aligned} \nu_2(S(\sigma_{n,k})) &= \nu_2\left(2 \sum_{j \in N(n-1,k)} \binom{n-1}{j} + 2 \sum_{j \in N(n-1,k)} \binom{n-1}{j-1}\right) \\ &= \nu_2((2^{w_2(m)+2}(m_1+2m_2)) + (2^{w_2(m)+2}(m_1+2m_2'))) \\ &= \nu_2(2^{w_2(m)+2}(2m_1+2(m_2+m_2'))) \\ &= w_2(m)+3. \end{aligned} \tag{47}$$

This concludes the proof. □

In terms of the parameters a and i, we have proved the veracity of Cusick-Li-Stănică's conjecture for all values of the parameters in red in Figure 6.

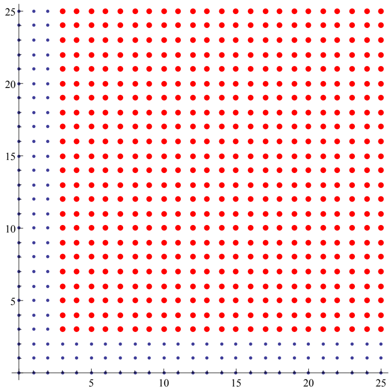

FIGURE 6. Let $n = 2^a(2^i m - 1) + 1$ and $k = 2^a(2^{i-1}m - 1)$. The red dots represent pairs (i, a) for which the conjecture is true.

We now move to the case $k = 2^a(2^{i-1}m - 1) + 2^{a-1}$. This case is similar to the previous one in the sense that

$$\nu_2(S(\sigma_{n+1,k})) = \nu_2(S(\sigma_{n,k})) + 1, \tag{48}$$

for values of $a \geq 2$. For $a = 1$ we have

$$\nu_2(\sigma_{n,k}) = w_2(m) + 2, \tag{49}$$

regardless of the value of i. However, the case $a = 1$ is out of the scope of Cusick-Li-Stănică's conjecture.

Theorem 4.2. *Suppose that a, i, and m are positive integers with $a \geq 2$ and m odd. Let $n = 2^a(2^i m - 1) + 1$ and $k = 2^a(2^{i-1}m - 1) + 2^{a-1}$. Then,*

$$\nu_2(S(\sigma_{n,k})) = w_2(m) + i + 1. \tag{50}$$

If $a = 1$, then

$$\nu_2(\sigma_{n,k}) = w_2(m) + 2. \tag{51}$$

In particular, Cusick-Li-Stănică's conjecture is true for $n = 2^{a+1}D + 1$ and $k = 2^a D$.

Proof. When $a \geq 3$, the proof is very similar to the one Theorem 4.1. The case $a = 2$ follows by a direct calculation, similar to the one presented in Theorem 3.2. The proof of the case $a = 1$ is very similar to the one presented in Theorem 3.4. □

We now consider the case when $r = 2$, i.e. when n has the form $n = 2^a(2^i m - 1) + 2$. It turns out that this case can also be transformed to the case $r = 0$ via the identity

$$\begin{aligned} S(\sigma_{n+2,k}) &= S(\sigma_{n,k}) + 2S(\sigma_{n,k} + \sigma_{n,k-1}) + S(\sigma_{n,k} + 2\sigma_{n,k-1} + \sigma_{n,k-2}) \\ &= S(\sigma_{n,k}) + 2S(\sigma_{n,k} + \sigma_{n,k-1}) + S(\sigma_{n,k} + \sigma_{n,k-2}). \end{aligned} \tag{52}$$

For $k = 2^a(2^{i-1}m - 1)$ we have the following theorem.

Theorem 4.3. *Suppose that a, i, and m are positive integers with $a \geq 4$, $i \geq 4$, and m odd. Let $n = 2^a(2^i m - 1) + 2$ and $k = 2^a(2^{i-1}m - 1)$. Then,*

$$\nu_2(S(\sigma_{n,k})) = w_2(m) + 4. \tag{53}$$

In particular, Cusick-Li-Stănică's conjecture is true for $n = 2^{a+1}D + 1$ and $k = 2^a(D - 1)$ with $D \equiv -1 \bmod 16$ and $a \geq 3$.

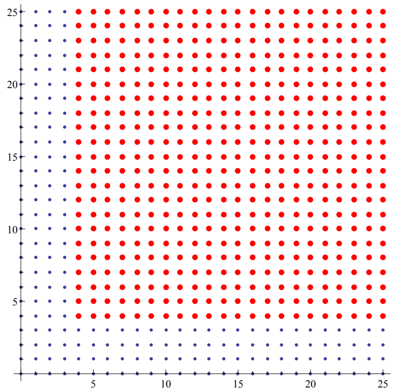

FIGURE 7. Let $n = 2^a(2^i m - 1) + 2$ and $k = 2^a(2^{i-1}m - 1)$. The red dots represent pairs (i, a) for which the conjecture is true.

Recall that for $k = 2^a(2^{i-1}m - 1)$, by transforming the case $r = 1$ to $r = 0$, we obtained Theorem 4.1, which is true for $a \geq 3$ and $i \geq 3$. Now, by transforming the case $r = 2$ to $r = 0$, we obtained Theorem 4.3, which holds for $a \geq 4$ and $i \geq 4$. In other words, we needed to add 1 to each parameter.

Next is the case $r = 2$ for $k = 2^a(2^{i-1}m - 1) + 2^{a-1}$.

Theorem 4.4. *Suppose that a, i, and m are positive integers with $a \geq 3$ and m odd. Let $n = 2^a(2^i m - 1) + 2$ and $k = 2^a(2^{i-1}m - 1) + 2^{a-1}$. Then,*

$$\nu_2(S(\sigma_{n,k})) = w_2(m) + i + 2. \tag{54}$$

If $a = 2$, then

$$\nu_2(S(\sigma_{n,k})) = w_2(m) + 2, \tag{55}$$

regardless of the value of i. In particular, Cusick-Li-Stănică's conjecture is true for $n = 2^{a+1}D + 2$ and $k = 2^a D$.

Proof. For $a \geq 3$, the proof uses the same techniques as in Theorem 4.1. For $a = 2$, the proof is very similar to the one presented in Theorem 3.4. □

Observe that Theorems 3.2, 4.2, and 4.4 prove the boundary cases of Cusick-Li-Stănică's conjecture for $n = 2^{a+1}D + r$ and $k = 2^a D$ where $r = 0, 1, 2$.

5. The case $r = -1$

The only boundary case of Cusick-Li-Stănică's conjecture that we have not considered is the one when

$$n = 2^a(2^i m - 1) - 1 \text{ and } k = 2^a(2^{i-1}m - 1).$$

This case seems to behave similar to the cases when $n = 2^a(2^i m - 1) + r$, for $r = 0, 1, 2$, in the sense that the 2-divisibility of $S(\sigma_{n,k})$ depends on $w_2(m)$. However, we point out this case is also quite different because now $\nu_2(S(\sigma_{n,k}))$ seems to depend on both parameters a and i. To be specific, we conjecture that for $a \geq 4$ and $i \geq 2$ we have

$$\nu_2(S(\sigma_{n,k})) = w_2(m) + i + 3a - 3. \tag{56}$$

Experiments suggest that this exact divisibility is obtained at

$$\nu_2\left(\sum_{j=k}^{k+2^a-1} \binom{n}{j}\right) = w_2(m) + i + 3a - 4, \tag{57}$$

while if $A = N(n, k) \setminus \{k, k+1, \cdots, k + 2^a - 1\}$, then it appears that

$$\nu_2\left(\sum_{j \in A} \binom{n}{j}\right) > w_2(m) + i + 3a - 4. \tag{58}$$

Proving (56) might need an approach different than the ones present in this manuscript. First, the identity

$$S(\sigma_{n,k}) = S(\sigma_{n-1,k}) + S(\sigma_{n-1,k} + \sigma_{n-1,k-1}), \tag{59}$$

which was used in the proof of Theorem 4.1 to reduce the case $r = 1$ to the case $r = 0$, does not work directly because the terms

$$S(\sigma_{n,k}) \quad \text{and} \quad S(\sigma_{n-1,k} + \sigma_{n-1,k-1}) \tag{60}$$

have the same 2-adic valuation. Second, if we try to prove (57) directly, then we encounter the difficulty that each binomial coefficient in the sum has the same 2-adic valuation, i.e.

$$\nu_2\left(\binom{n}{j}\right) = w_2(m) + i - 2. \tag{61}$$

In other words, we need to know the total contribution of them, but we cannot directly use the ultrametric property of the valuation to get such contribution. On the other hand, in (58) we can divide the binomial coefficients in the sum into blocks of length 2^a. All the binomial coefficients in a specific block have the same valuation. However, different blocks might have different valuation. Again, we cannot directly apply the ultrametric property to show (58).

We were able to prove (56) for $a = 4$ and $a = 5$. However, we omit the proof because it follows along the same line of the proofs of our previous results.

Proposition 5.1. *Suppose that a, i, and m are positive integers with $a \in \{4, 5\}$, $i \geq 2$, and m odd. Let $n = 2^a(2^i m - 1) - 1$ and $k = 2^a(2^{i-1}m - 1)$. Then,*

$$\nu_2(S(\sigma_{n,k})) = w_2(m) + i + 3a - 3. \tag{62}$$

In particular, Cusick-Li-Stănică's conjecture is true for $n = 2^{a+1}D - 1$ and $k = 2^a(D - 1)$.

For fixed $a \geq 4$, any m, and any $i \geq 2a$, we have a process that allows us to determine the veracity of (57) and (58). However, this process depends on a computation and therefore, we do not have the proof in general.

6. The case $k = 2^a(m - 1)$

In this section we go back to the boundary case

$$n = 2^a(2^i m - 1) \text{ and } k = 2^a(2^{i-1}m - 1) \tag{63}$$

and explore the behaviour of $\nu_2(S(\sigma_{n,k}))$ when $i = 1$. Observe that this is the only case not covered by Theorem 3.4.

Recall that Theorem 3.4 tells us that

$$\nu_2(S(\sigma_{n,k})) = w_2(m) + 2, \tag{64}$$

as long as $i \geq 2$. On the other hand, Example 3.5 shows that (64) does not hold for $i = 1$. We attempt to find some patterns in the 2-divisibility of the exponential sum of $\sigma_{n,k}$ when $i = 1$. Most of the statements presented in this section have not been proved yet. In other words, this section is completely experimental.

We start the study by reviewing what already have. Remember that the factor $2^i m - 1$ in n represents D in Cusick-Li-Stănică's conjecture. We know that D is odd, thus re-write $D = 2j_0 - 1$ with $j_0 \geq 2$. If we write everything in terms of the new parameter j_0, then we have

$$n = 2^a(2j_0 - 1) \text{ and } k = 2^a(j_0 - 1). \tag{65}$$

Observe that knowing (64) is equivalent to knowing $\nu_2(S(\sigma_{n,k}))$ when j_0 even. Thus, the case when j_0 is odd is open.

Divide the natural numbers into two classes:

$$\begin{aligned} j_0 &= 2j_1 \text{ (even)} \\ j_0 &= 2j_1 + 1 \text{ (odd)} . \end{aligned}$$

We call this the first level (it will become clear what we mean by this). As mentioned in the previous discussion, we know the 2-adic valuation of the even class, i.e. $w_2(2j_1)+2$, but not the one for the odd class. Split the odd class into the two classes:

(1) $4j_2+1$,
(2) $4j_2+3$, for j_2 non-negative integer.

We call this the second level. Consider the class $4j_2+3$. In this case, $n=2^a(20+32j_2)$ and $k=2^a(8+16j_2)$. It appears that as long as $a>1$, then as j_2 runs through the non-negative integers, the sequence $\nu_2(S(\sigma_{n,k}))$ is given by

$$5,6,6,7,6,7,7,8,6,7,7,8,7,8,8,9,6,7,7,8,\cdots$$

This appears to be the sequence $w_2(4j_2+3)+3$. The class $4j_2+1$ does not have this behavior. Thus, as we did before, we split this class, i.e. the class $4j_2+1$, into two classes:

(1) $8j_3+1$,
(2) $8j_3+5$, for j_3 non-negative integer.

We call this the third level. Consider the class $8j_3+5$. Again, it appears that if $a>1$, then the sequence $\nu_2(S(\sigma_{n,k}))$ is given by

$$5,6,6,7,6,7,7,8,6,7,7,8,7,8,8,9,6,7,7,8,\cdots$$

Again, this seems to be the sequence $w_2(8j_2+5)+3$. The node $8j_3+1$ does not have this form. Hence, we split it into two classes:

(1) $16j_4+1$,
(2) $16j_4+9$, for j_4 non-negative integer.

This is the fourth level. As before, consider the class $16j_4+9$. If $a>2$, then the sequence $\nu_2(S(\sigma_{n,k}))$ is given by

$$6,7,7,8,7,8,8,9,7,8,8,9,8,9,9,10,7,8,8,9,\cdots$$

This sequence seems to be $w_2(16j_4+9)+4$. Observe that now we need $a>2$. The class $16j_4+1$ does not behave in this way. Continue branching as before.

It appears that, after the third level, the level l is given by the classes

(1) 2^lj_l+1,
(2) $2^lj_l+2^{l-1}+1$, for j_l non-negative integer.

Moreover, the valuation to be assigned to the class $2^lj_l+2^{l-1}+1$ is $w_2(2^lj_l+2^{l-1}+1)+l$ and this seems to work for $a>\lfloor\log_2(l)\rfloor$. This information is summarized in a tree, see Figure 8.

The above discussion leads us to believe that as long as $a>\lfloor\log_2(l)\rfloor$, the information at the l-level is predictable (we are not claiming we can prove it). However, what happens when $a\leq\lfloor\log_2(l)\rfloor$? It appears that if l is not a power of 2 and if $a\leq\lfloor\log_2(l)\rfloor$, then

$$\nu_2(S(\sigma_{n,k}))=w_2(2^lj_l+2^{l-1}+1)+2^a. \tag{66}$$

In the case that l is a power of 2 and $a<\lfloor\log_2(l)\rfloor$, then it seems that

$$\nu_2(S(\sigma_{n,k}))=w_2(2^lj_l+2^{l-1}+1)+2^a. \tag{67}$$

We do not recognize the behavior of the 2-adic valuation for l a power of 2 and $a=\lfloor\log_2(l)\rfloor$.

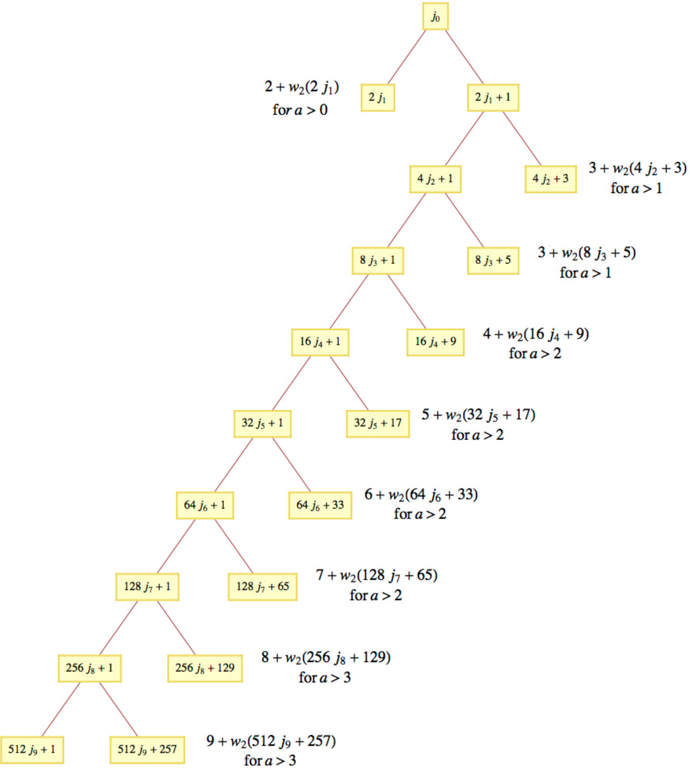

FIGURE 8. The tree for the case $i = 1$.

If we replace n by $n + r$ for $r = 1, 2$ and consider the same k, then it appears that similar behavior occurs for the case when $i = 1$.

REFERENCES

[1] A. Adolphson and S. Sperber, p-adic Estimates for Exponential Sums and the of Chevalley-Warning, *Ann. Sci. Ec. Norm. Super.*, 4^e série, **20**, 545-556, 1987.

[2] J. Ax, Zeros of polynomials over finite fields. *Amer. J. Math.*, **86**, 255-261, 1964.

[3] L. A. Bassalygo and V. A. Zinoviev, On divisibility of exponential sums of polynomials of special type over fields of characteristic 2. *Des. Codes Cryptogr.* **66**, 129-143, 2013.

[4] A. Canteaut, P. Charpin, and H. Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on $GF(2^m)$ and cross correlation of maximum-length sequences. *SIAM Journal on Discrete Mathematics* **13**, 105-138, 2000.

[5] F. Castro and L. Medina, Linear Recurrences and Asymptotic Behavior of Exponential Sums of Symmetric Boolean Functions, *Elec. J. Combinatorics* **18**, 2011, #P8.

[6] F. Castro and L. Medina, Asymptotic Behavior of Perturbations of Symmetric Functions, *Annals of Combinatorics*, **18**, 397-417, 2014.

[7] F. Castro, L. Medina and I. Rubio, Exact Divisibility of Exponential Sums over the Binary Field via the Covering Method, *Contemporary Mathematics* **537**, 129-136, 2009.

[8] F. Castro and I. Rubio, Exact p-Divisibility of Exponential Sums Using the Covering Method, *Proc. AMS* (in press).

[9] F. Castro and I. Rubio, Construction of Systems of Polynomial Equations with Exact p-divisibility via the Covering Method, *J. Algebra and its Applications*, DOI: 10.1142/S0219498814500133.

[10] T. W. Cusick, Yuan Li, and P. Stănică, Balanced Symmetric Functions over $GF(p)$, *IEEE Trans. on Information Theory* **5**, 1304-1307, 2008.

[11] T. W. Cusick, Yuan Li and P. Stănică, On a conjecture for balanced symmetric Boolean functions, J. Math. Crypt. **3**, 1-18, 2009.

[12] K. S. Davis and W. A. Webb, Lucas' Theorem for Prime Powers, *Europ. J. Combinatorics* **11**, pp. 229-233, 1990.

[13] Y. Guo, G. Gao, Y. Zhao, Recent Results on Balanced Symmetric Boolean Functions, *iacr.org*, e-print #93, 2012.

[14] A. Granville, Zaphod Beeblerox's Brain and the Fifty-Ninth Row of Pascal's Triangle, American. Math. Monthly **44**, 318-331, 1992.

[15] C. Güneri and G. McGuire, Supersingular curves over finite fields and weight divisibility of codes, *J. Comput. Appl. Math.* **259**, part B, 474-484, 2014.

[16] J. G. Huard and B. K. Spearman and K. Williams, Pascal Triangle $(\bmod 8)$, *Europ. J. Combinatorics* **19**, 45-61, 1998.

[17] G-P. Gao, W-F Liu and X-Y. Zhang, The degree of balanced elementary symmetric Boolean functions of $4k+3$ variables, *IEEE Trans. Inf. Theory* **57**, 4822-4825, 2011.

[18] M. Kolountzakis, R. J. Lipton, E. Markakis, A. Metha and N. K. Vishnoi, On the Fourier Spectrum of Symmetric Boolean Functions, *Combinatorica*, **29**, 363-387, 2009.

[19] O. Moreno and F. Castro, Divisibility properties for covering radius of certain cyclic codes, *IEEE Trans. Inform. Theory* **49**, no. 12, 3299-3303, 2003.

[20] O. Moreno and C. J. Moreno, Improvement of the Chevalley-Warning and the Ax-Katz theorems, *Amer. J. Math.* **117**, 241-244, 1995.

[21] O. Moreno and C. J. Moreno, The MacWilliams-Sloane Conjecture on the Tightness of the Carlitz-Uchiyama Bound and the Weights of Dual of BCH Codes, *IEEE Trans. Inform. Theory* **40**, 1894-1907, 1994.

[22] O. Moreno, K. Shum, F. N. Castro and P.V. Kumar, Tight Bounds for Chevalley-Warning-Ax Type Estimates, with Improved Applications, *Proc. of the London Mathematical Society*, **88**, 545-564, 2004.

[23] A. Shpilka and A. Tal, On the Minimal Fourier Degree of Symmetric Boolean Functions, *Combinatorica*, **88**, 359-377, 2014.

[24] J. von zur Gathem and J. R. Roche, Polynomial with Two Values, *Combinatorica* **17**, 345-362, 1997.

[25] Wei Su, Xiaohu Tang, Alexander Pott: A Note on a Conjecture for Balanced Elementary Symmetric Boolean Functions, *IEEE Transactions on Information Theory* **59**, 665-671, 2013.

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`