ASYMPTOTIC BEHAVIOR OF THE EXPONENTIAL SUM OF PERTURBATIONS OF SYMMETRIC POLYNOMIALS

FRANCIS N. CASTRO AND LUIS A. MEDINA

Abstract. In this paper we consider perturbations of symmetric boolean functions $\sigma_{n,k_1} + \cdots + \sigma_{n,k_s}$ in n-variable and degree k_s. We compute the asymptotic behavior of boolean functions of the type

$$\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + F(X_1, \ldots, X_j)$$

for j fixed. In particular, we characterize all the boolean functions of the type

$$\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + F(X_1, \ldots, X_j)$$

that are asymptotic balanced. We also present an algorithm that computes the asymptotic behavior of a family of Boolean functions from one member of the family. Finally, as a byproduct of our results, we provide a relation between the parity of families of sums of binomial coefficients.

1. Introduction

Boolean functions are very important in the theory of error-correcting codes as well as in cryptography. These functions are beautiful combinatorial objects with rich combinatorial properties. In particular, symmetric booleans have received a lot attention for their advantage since they can be identified by an $(n+1)$ bit vector (for example, see [31, 7, 9, 10, 19, 26]).

One can find many papers and books discussing the properties of boolean functions (see, for example, [5, 13, 2, 6]). 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 asymptotic behavior of exponential sums of perturbed symmetric boolean functions.

The correlation between two Boolean functions of n inputs is defined as the number of times the functions agree minus the number of times they disagree all divided by 2^n, i.e.,

$$C(F_1, F_2) = \frac{1}{2^n} \sum_{x_1,\ldots,x_n \in \{0,1\}} (-1)^{F_1(x_1,\ldots,x_n)+F_2(x_1,\ldots,x_n)}. \tag{1.1}$$

In this paper we are interested in the case when $F_1 + F_2$ can be written as $\sigma_{n,k_1} + \sigma_{n,k_2} + \cdots + \sigma_{n,k_s} + F(X_1, \ldots, X_j)$, where $\sigma_{n,k}$ is the elementary symmetric boolean polynomial of degree k in the n variables $X_1, \ldots, X_n$ and F is a boolean function in the first j-variables (j fixed). We write $C(\sigma_{n,k_1} + \sigma_{n,k_2} + \cdots + \sigma_{n,k_s} + F)$ instead of $C(F_1, F_2)$. In [4], A. Canteaut and M. Videau studied in detail symmetric boolean functions. They established a link between the periodicity of the simplified value vector of a symmetric Boolean function and its degree. Recently, a new

Date: January 28, 2013.

2010 *Mathematics Subject Classification.* 05E05, 11T23.

Key words and phrases. Symmetric boolean functions, exponential sums, recurrences.

cryptographic property have been introduced. This property is called algebraic immunity of boolean functions ([20]). All the symmetric boolean functions with maximal algebraic immunity have been found ([16, 29, 22, 17]).

In [7, 21], Carlet and Olejár-Stanek studied the asymptotic nonlinearity of boolean functions. Later, in [23], Rodier improved their results by showing that the nonlinearity of almost all boolean functions is equal to $\sqrt{2^{m+1}\log 2^m}$.

In [14, 15], the authors considered rotation symmetric Boolean functions of degree 3 in n variables. In [14], Bileschi-Cusick-Padgett provided an algorithm for finding a recursion for the truth table of any cubic rotation symmetric Boolean function generated by a monomial (their work reduced the computational complexity). In [15], Cusick improved the computational complexity found in [14] to something linear in the number of variables n assuming the mild condition that the roots of the characteristic polynomial are distinct.

In[3], J. Cai et al. computed a closed formula for the correlation between any two symmetric Boolean functions. This formula implies that $C(\sigma_{n,k_1}+\sigma_{n,k_2}+\cdots+\sigma_{n,k_s})$ satisfies a homogeneous linear recurrence with integer coefficients and provides an upper bound for the degree of the minimal recurrence of this type that $C(\sigma_{n,k_1}+\sigma_{n,k_2}+\cdots+\sigma_{n,k_s})$ satisfies. We obtain a homogeneous linear recurrence with integer coefficients satisfied by $C(\sigma_{n,k_1}+\sigma_{n,k_2}+\cdots+\sigma_{n,k_s}+F)$. This generalize the result of J. Cai et al.

In this paper, we prove that

$$\lim_{n\to\infty} C(\sigma_{n,k_1}+\sigma_{n,k_2}+\cdots+\sigma_{n,k_s}+F(X_1,\ldots,X_j))=0, \tag{1.2}$$

if and only if $C(F(X_1,\ldots,X_j))$ is balanced or $\sigma_{n,k_1}+\cdots\sigma_{n,k_s}$ is asymptotic balanced. In [12], Cusick et al. conjectured that there no nonlinear balanced elementary symmetric polynomials except for the elementary symmetric boolean function of degree $k=2^r$ in $2^r\cdot l-1$ variables, where r and l are any positive integers. This conjecture has been the central topic for several papers. Recent results about the Cusick et al.'s conjecture can be found in [27]. In [8], we characterize the asymptotic behavior of the elementary symmetric boolean functions, i.e., $\lim_{n\to\infty} C(\sigma_{n,k})=\dfrac{2^{w_2(k)-1}-1}{2^{w_2(k)-1}}$, where $w_2(k)$ is the Hamming weight of k. In particular, this implies that Cusick et al.'s conjecture is true for large n. Combining the last two results, we have that when k is not a power of two, $\sigma_{n,k}+F(X_1,\ldots,X_j)$ is asymptotic balanced if and only if $C(F)$ is balanced.

In general, we compute the asymptotic value

$$\lim_{n\to\infty} C(\sigma_{n,k_1}+\sigma_{n,k_2}+\cdots+\sigma_{n,k_s}+F(X_1,\ldots,X_j))=c_0(k_1,\ldots,k_r)\cdot\frac{S(F)}{2^j}, \tag{1.3}$$

where $S(F)$ and $c_0(k_1,\cdots,k_s)$ are defined in section 2. We present an algorithm to compute the asymptotic behavior of a family of symmetric boolean function given the asymptotic behavior of one of its members. Finally, we use these asymptotic coefficients to prove some results about the parity of some sums of binomial coefficients.

2. Preliminaries

Let $\mathbb{F}$ be the binary field, $\mathbb{F}^n = \{(x_1, \ldots, x_n) \,|\, x_i \in \mathbb{F}, i = 1, \ldots, n\}$, 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:

$$S(F) = \sum_{\mathbf{x} \in \mathbb{F}^n} (-1)^{F(\mathbf{x})}. \tag{2.1}$$

A boolean function $F(\mathbf{X})$ is called balanced if $S(F) = 0$. This property is important for some applications in cryptography.

In [8], F. Castro and L. Medina studied exponential sums of elementary symmetric polynomials. Let $\sigma_{n,k}$ be the elementary symmetric polynomial in n variables of degree k. Suppose that $1 \leq k_1 < \cdots < k_s$ are integers. Castro and Medina were able to show that the sequence $\{S(\sigma_{n,k_1} + \cdots + \sigma_{n,k_s})\}_{n \in \mathbb{N}}$ satisfies a homogeneous linear recurrence with integer coefficients. They used this recurrence to study the asymptotic behavior of such sequences. In particular, they exploited the fact that

$$\lim_{n \to \infty} \frac{1}{2^n} S(\sigma_{n,k_1} + \cdots + \sigma_{n,k_s}) = c_0(k_1, \cdots, k_s), \tag{2.2}$$

where

$$c_0(k_1, \cdots, k_s) = \frac{1}{2^r} \sum_{i=0}^{2^r - 1} (-1)^{\binom{i}{k_1} + \cdots + \binom{i}{k_s}}, \tag{2.3}$$

and $r = \lfloor \log_2(k_s) \rfloor + 1$.

As part of their study, they introduced the concept of an asymptotically balanced function. We say that $\sigma_{n,k_1} + \cdots + \sigma_{n,k_s}$ is asymptotically balanced if

$$\lim_{n \to \infty} \frac{1}{2^n} S(\sigma_{n,k_1} + \cdots + \sigma_{n,k_s}) = 0. \tag{2.4}$$

Note that if a function $\sigma_{n,k_1} + \cdots + \sigma_{n,k_s}$ is *not* asymptotically balanced, then we know that it is not balanced for all sufficiently large n. The authors provided families of symmetric polynomials that were asymptotically balanced and families that were not. For example, they show that if $1 \leq k_1 < \cdots < k_s$ are integers with k_s a power of 2, then the polynomial $\sigma_{n,k_1} + \cdots + \sigma_{n,k_s}$ is asymptotically balanced.

In this article, we study some perturbations of symmetric functions and extend some of the results of [8] to them. Recall that $\sigma_{n,k}$ is the elementary symmetric polynomial of degree k in the variables $X_1, \cdots, X_n$. Suppose that $j < n$ and let $F(\mathbf{X})$ be a binary polynomial in the variables $X_1, \cdots, X_j$ (the first j variables in $X_1, \cdots, X_n$). We are interested in the exponential sum of polynomials of the form

$$\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + F(\mathbf{X}), \tag{2.5}$$

where $k_1 < \cdots < k_s$. In particular, we study the sequence

$$\{S(\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + F(\mathbf{X}))\}_{n \in \mathbb{N}}$$

where $k_1, \cdots, k_s$ and $F(\mathbf{X})$ are fixed and n varies.

Of special interest is the asymptotic behavior of the exponential sum of (2.5). We want to know the value (if exists) of

$$\lim_{n \to \infty} \frac{1}{2^n} S(\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + F(\mathbf{X})).$$

Example 2.1. Consider the sequence

$$\{S(\sigma_{n,5} + X_1X_2 + X_1)\}_{n\in\mathbb{N}}. \tag{2.6}$$

Using *Mathematica* 8.0 with its built-in function `FindLinearRecurrence`, we guess that the sequence (2.6) satisfies the recurrence

$$x_n = 6x_{n-1} - 14x_{n-2} + 16x_{n-3} - 10x_{n-4} + 4x_{n-5}. \tag{2.7}$$

Moreover, it can be proved, using some of the machinery presented in this paper, that

$$\lim_{n\to\infty} \frac{1}{2^n} S(\sigma_{n,5} + X_1X_2 + X_1) \quad = \quad \frac{1}{4}.$$

In Figure 1 you can see a graphical representation of this limit. The blue dots represents $S(\sigma_{n,5} + X_1X_2 + X_1)/2^n$. The line $y = 1/4$ is in red.

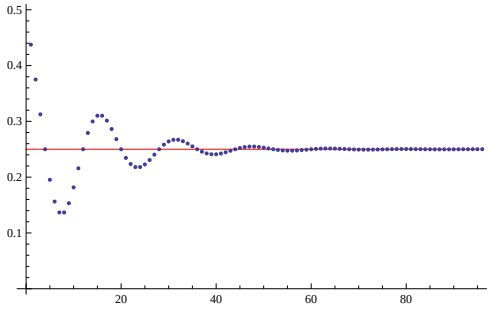

FIGURE 1. Graphical representation of $S(\sigma_{n,5} + X_1X_2 + X_2)/2^n$.

In the next section we show that Example 2.1 is not a coincidence, but the rule. In other words, we show that the exponential sum of these perturbations satisfies the same recurrence as the exponential sum of symmetric polynomials. In Section 4, we study the asymptotic behavior of them.

3. The linear recurrence

Let $1 \leq k_1 < \cdots < k_s$ be integers and $F(\mathbf{X})$ be a binary polynomial in the variables $X_1, \cdots, X_j$ (j fixed). In this section we show that

$$\{S(\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + F(\mathbf{X}))\}_{n\in\mathbb{N}}$$

satisfies the recurrence

$$x_n = \sum_{m=1}^{2^r-1} (-1)^{m-1} \binom{2^r}{m} x_{n-m}, \tag{3.1}$$

where $r = \lfloor \log_2(k_s) \rfloor + 1$.

We start with the following preliminary results.

Definition 3.1. For $\mathbf{x} \in \mathbb{F}_2^n$, let $w_2(\mathbf{x})$ be the Hamming weight of $\mathbf{x}$, in other words, $w_2(\mathbf{x})$ is the number of entries of $\mathbf{x}$ that are one. For example, $w_2((0,1,1,0,1)) = 3$.

Theorem 3.2. *Suppose $1 \leq k_1 < \cdots < k_s$ are integers. Let $F(\mathbf{X})$ be a binary polynomial in the variables $X_1, \cdots, X_j$. Define*

$$C_m(F) = \sum_{\mathbf{x} \in \mathbb{F}_2^j \text{ with } w_2(\mathbf{x})=m} (-1)^{F(\mathbf{x})} \tag{3.2}$$

for $m = 0, 1, \cdots, j$. Then,

$$S(\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}+F(\mathbf{X})) = \sum_{m=0}^{j} C_m(F) S\left(\sum_{i=0}^{m} \binom{m}{i} [\sigma_{n-j,k_1-i} + \cdots + \sigma_{n-j,k_s-i}]\right). \tag{3.3}$$

Proof. We provide the proof of the case of one elementary symmetric polynomial, i.e. we show that

$$S(\sigma_{n,k} + F(\mathbf{X})) = \sum_{m=0}^{j} C_m(F) S\left(\sum_{i=0}^{m} \binom{m}{i} \sigma_{n-j,k-i}\right)$$

is true. The purpose of doing this is to simplify the notation and the writing of the proof. The general case follows in a similar manner.

Recall that

$$S(\sigma_{n,k} + F(\mathbf{X})) \quad = \quad \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{\sigma_{n,k}(\mathbf{x})+F(\mathbf{x})}.$$

This can be re-written as

$$\begin{aligned} S(\sigma_{n,k} + F(\mathbf{X})) \quad &= \quad \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{F(\mathbf{x})} (-1)^{\sigma_{n,k}(\mathbf{x})} \\ &= \quad \sum_{\mathbf{x}_{(0)}^j \in \mathbb{F}_2^n} (-1)^{F(\mathbf{x})} (-1)^{\sigma_{n,k}(\mathbf{x})} + \sum_{\mathbf{x}_{(1)}^j \in \mathbb{F}_2^n} (-1)^{F(\mathbf{x})} (-1)^{\sigma_{n,k}(\mathbf{x})} + \\ &\quad \cdots + \sum_{\mathbf{x}_{(j)}^j \in \mathbb{F}_2^n} (-1)^{F(\mathbf{x})} (-1)^{\sigma_{n,k}(\mathbf{x})}, \end{aligned} \tag{3.4}$$

where $\mathbf{x}_{(m)}^j$ represents a tuple in $\mathbb{F}_2^n$ that has exactly m ones in the first j entries. Let us assign values to the first j entries of the variable $\mathbf{X}$ and let the rest of it vary. Fix this assignment. Suppose it has m ones in the first j entries, i.e. the assignment has the form

$$(\delta_1, \cdots, \delta_j, X_{j+1}, \cdots, X_n),$$

where the $\delta_i \in \{0, 1\}$ are fixed, $\delta_1 + \cdots + \delta_j = m$, and $X_{j+1}, \cdots, X_n$ are binary variables. It is not hard to see that in this case the elementary symmetric polynomial $\sigma_{n,k}$ gets transform to $\sum_{i=0}^{m} \binom{m}{i} \sigma_{n-j,k-i}$, where the variables of $\sigma_{n-j,k-i}$ are $X_{j+1}, \cdots, X_n$. Thus, for this particular assignment, we have

$$\sum_{(\delta_1, \cdots, \delta_j, x_{j+1}, \cdots, x_n)} (-1)^{F(\mathbf{x})} (-1)^{\sigma_{n,k}(\mathbf{x})} = (-1)^{F(\delta_1, \cdots, \delta_j)} S\left(\sum_{i=0}^{m} \binom{m}{i} \sigma_{n-j,k-i}\right).$$

But this yields

$$\begin{aligned}\sum_{\mathbf{x}_{(m)}^{j}\in\mathbb{F}_2^n}(-1)^{F(\mathbf{x})}(-1)^{\sigma_{n,k}(\mathbf{x})} &= \left(\sum_{\mathbf{x}\in\mathbb{F}_2^j \text{ with } w_2(\mathbf{x})=m}(-1)^{F(\mathbf{x})}\right) S\left(\sum_{i=0}^{m}\binom{m}{i}\sigma_{n-j,k-i}\right)\\ &= C_m(F)S\left(\sum_{i=0}^{m}\binom{m}{i}\sigma_{n-j,k-i}\right). \qquad (3.5)\end{aligned}$$

Note that (3.4) and (3.5) imply the theorem. □

Remark. There are three things about equation (3.3). First, note that the values of $\binom{m}{i}$ that are inside the exponential sum can be taken modulo two, since only the parity matters. Second, if $k_l - i < 0$, then the term σ_{n-j,k_l-i} does not exist. Finally, in the case that $k_l - i = 0$, then $\sigma_{n-j,0}$ should be interpreted as 1.

Corollary 3.3. *Let $1 \le k_1 < \cdots < k_s$ be integers and $F(\mathbf{X})$ a binary polynomial in the variables $X_1, \cdots, X_j$ (j fixed). Consider the sequence*

$$\{S(\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + F(\mathbf{X}))\}_{n\in\mathbb{N}} \qquad (3.6)$$

and let $r = \lfloor \log_2(k_s) \rfloor + 1$. Then, (3.6) satisfies recurrence (3.1). In particular,

$$\lim_{n\to\infty}\frac{1}{2^n}S(\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + F(\mathbf{X})) \qquad (3.7)$$

exists.

Proof. Theorem 3.2 implies

$$S(\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}+F(\mathbf{X})) = \sum_{m=0}^{j} C_m(F)S\left(\sum_{i=0}^{m}\binom{m}{i}[\sigma_{n-j,k_1-i} + \cdots + \sigma_{n-j,k_s-i}]\right).$$

However, we know that each $S\left(\sum_{i=0}^{m}\binom{m}{i}[\sigma_{n-j,k_1-i} + \cdots + \sigma_{n-j,k_s-i}]\right)$ satisfies recurrence (3.1), see [8] for details. Thus, $S(\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + F(\mathbf{X}))$ satisfies the same recurrence. Finally, since the biggest modulo of the roots of the characteristic polynomials associated to (3.1) is 2 (see [8]), then

$$\lim_{n\to\infty}\frac{1}{2^n}S(\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + F(\mathbf{X})) \qquad (3.8)$$

exists. □

Example 3.4. Consider the perturbation

$$\sigma_{n,5} + \sigma_{n,3} + X_1X_2X_3X_4X_5X_6.$$

Apply Theorem 3.2 to get the coefficients

$$\begin{aligned}C_0(F) &= 1\\ C_1(F) &= 6\\ C_2(F) &= 15\\ C_3(F) &= 20\\ C_4(F) &= 15\\ C_5(F) &= 6\\ C_6(F) &= -1.\end{aligned}$$

Take each binomial coefficient inside the exponential sums modulo 2 to obtain

$$\begin{aligned} S(\sigma_{n,5}+\sigma_{n,3}+X_1X_2X_3X_4X_5X_6) &= S(\sigma_{n-6,5}+\sigma_{n-6,5}) \\ &\quad +6S(\sigma_{n-6,5}+\sigma_{n-6,4}+\sigma_{n-6,3}+\sigma_{n-6,2}) \\ &\quad +15S(\sigma_{n-6,5}+\sigma_{n-6,1}) \\ &\quad -20S(\sigma_{n-6,5}+\sigma_{n-6,4}+\sigma_{n-6,1}) \\ &\quad +15S(\sigma_{n-6,5}+\sigma_{n-6,3}+\sigma_{n-6,1}) \\ &\quad -6S(\sigma_{n-6,5}+\sigma_{n-6,4}+\sigma_{n-6,3}+\sigma_{n-6,2}+\sigma_{n-6,1}) \\ &\quad -S(\sigma_{n-6,5}). \end{aligned}$$

Note that the third and fifth coefficients appear as negative instead of positive. The reason for this is that the term $\sigma_{n-6,0}=1$ appears inside the corresponding exponential sum and

$$S(G(\mathbf{X})+1) = -S(G(\mathbf{X}))$$

for any binary polynomial G.

Now, Corollary 3.3 tells us that

$$\lim_{n\to\infty}\frac{1}{2^n}S(\sigma_{n,5}+\sigma_{n,3}+X_1X_2X_3X_4X_5X_6)$$

exists. If fact, in the next section we show that this limit is $31/64$. Below you can see a graphical representation of this fact. The blue dots correspond to $S(\sigma_{n,5}+\sigma_{n,3}+X_1X_2X_3X_4X_5X_6)/2^n$. The red line correspond to $y=31/64$.

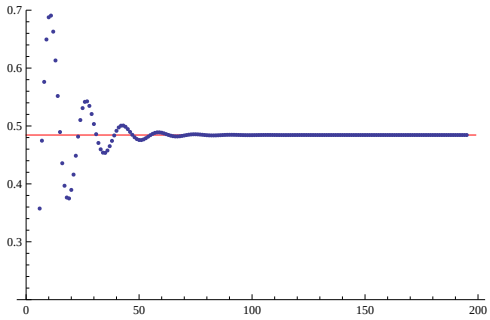

FIGURE 2. Graphical representation of $S(\sigma_{n,5}+\sigma_{n,3}+X_1X_2X_3X_4X_5X_6)/2^n$.

Example 3.5. Let us go back to the sequence in Example 2.1, i.e.

$$\{S(\sigma_{n,5}+X_1X_2+X_1)\}_{n\in\mathbb{N}}.$$

Following Theorem 3.2 with $F(\mathbf{X})=X_1X_2+X_1$, we get

$$\begin{aligned} C_0(F) &= 1 \\ C_1(F) &= 0 \\ C_2(F) &= 1. \end{aligned}$$

This implies that

$$S(\sigma_{n,5}+X_1X_2+X_1) = S(\sigma_{n-2,5})+S(\sigma_{n-2,5}+\sigma_{n-2,3}).$$

Now, using the theory presented in [8], it can be showed that both, $S(\sigma_{n-2,5})$ and $S(\sigma_{n-2,5}+\sigma_{n-2,3})$, satisfy recurrence (2.7). Since $S(\sigma_{n,5}+X_1X_2+X_1)$ is a linear combination of them, then $S(\sigma_{n,5}+X_1X_2+X_1)$ satisfies the same recurrence. Also,

$$\begin{aligned}\lim_{n\to\infty}\frac{1}{2^n}S(\sigma_{n,5}+X_1X_2+X_1) &= \lim_{n\to\infty}\frac{1}{2^n}\left(S(\sigma_{n-2,5})+S(\sigma_{n-2,5}+\sigma_{n-2,3})\right)\\ &= \lim_{n\to\infty}\frac{1}{4}\left(\frac{S(\sigma_{n-2,5})}{2^{n-2}}+\frac{S(\sigma_{n-2,5}+\sigma_{n-2,3})}{2^{n-2}}\right)\\ &= \frac{1}{4}(c_0(5)+c_0(5,3))\\ &= \frac{1}{4}\left(\frac{1}{2}+\frac{1}{2}\right)=\frac{1}{4},\end{aligned}$$

where the values of $c_0(5)$ and $c_0(5,3)$ can be obtained from (2.3).

Remark. Note that Corollary 3.3 tells us that $S(\sigma_{n,5}+X_1X_2+X_1)$ satisfies the recurrence

$$x_n = 8x_{n-1}-28x_{n-2}+56x_{n-3}-70x_{n-4}+56x_{n-5}-28x_{n-6}+8x_{n-7}, \tag{3.9}$$

but we proved that this sequence satisfies recurrence (2.7), which has less order. Therefore, even though Corollary 3.3 provides us with a linear recurrence for these perturbations, this recurrence is not necessary the minimal one. It is interesting to know what is the minimal homogeneous linear recurrence with integer coefficients that these sequences satisfy. However, our main focus in this article is to study the asymptotic behavior of these perturbations and knowing that they satisfy a linear recurrence is enough. Thus, in this paper we do not consider the problem of finding the minimal homogeneous linear recurrence with integer coefficients that they satisfy.

4. Asymptotic behavior

In this section we study the asymptotic behavior of the exponential sum of perturbations of type (2.5). We are interested in the question of when are these perturbations asymptotically balanced. We start with the following example.

Example 4.1. Consider the polynomial

$$\sigma_{n,16}+X_1X_2+X_3X_4X_5.$$

We already know that $\sigma_{n,16}$ is asymptotically balanced. In this case, it turns out that the perturbation is also asymptotically balanced. In Figure 3 you can see a graphical representation of this fact. The blue dots represent $S(\sigma_{n,16})/2^n$ and the red dots represent $S(\sigma_{n,16}+X_1X_2+X_3X_4X_5)/2^n$.

When we started the study of these perturbations, we observed that in the particular case when a symmetric polynomial was disturbed by a linear polynomial, i.e.

$$\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}+X_1+\cdots+X_j, \tag{4.1}$$

the result was an asymptotically balanced function.

Example 4.2. Consider the perturbation

$$\sigma_{n,7}+X_1+X_2+X_3. \tag{4.2}$$

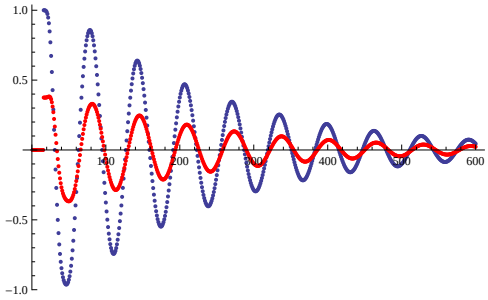

FIGURE 3. Graphical representation of $S(\sigma_{n,16})/2^n$ (blue) vs $S(\sigma_{n,16} + X_1X_2 + X_3X_4X_5)/2^n$ (red).

It turns out that this perturbation is asymptotically balanced, even though $\sigma_{n,7}$ is not. Figure 4 shows a graphical representation of the exponential sums of $\sigma_{n,7}$ and $\sigma_{n,7} + X_1 + X_2 + X_3$. The blue dots represent $S(\sigma_{n,7})/2^n$ and the red dots represent $S(\sigma_{n,7} + X_1 + X_2 + X_3)/2^n$.

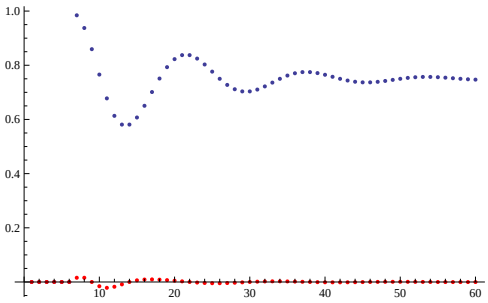

FIGURE 4. Graphical representation of $S(\sigma_{n,7})/2^n$ (blue) vs $S(\sigma_{n,7} + X_1 + X_2 + X_3)/2^n$ (red).

Perturbations of the form $\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + X_1 + \cdots + X_j$ are not the only examples in which you start with a function that is *not* asymptotically balanced, but after you perturb it the result is an asymptotically balanced function.

Example 4.3. Consider the perturbation

$$\sigma_{n,15} + X_1X_2 + X_1X_3 + X_2X_3.$$

The polynomial $\sigma_{n,15}$ is not asymptotically balanced, but this perturbation is. This is a striking example since the asymptotic behavior of $\sigma_{n,15}$ is close to 1, but adding $X_1X_2 + X_1X_3 + X_2X_3$ to $\sigma_{n,15}$ makes the distribution of 0's and 1's close to each other. Figure 5 is graphical representation of the exponential sums of $\sigma_{n,15}$ and $\sigma_{n,15} + X_1X_2 + X_1X_3 + X_2X_3$. The blue dots correspond to $\sigma_{n,15}$ and the red dots to the perturbation.

The two examples above have something in common: the function $F(\mathbf{X})$ is balanced.

As we mentioned before, in Example 4.1 we start with an asymptotically balanced function and after perturbation, we still get an asymptotically balanced function. In Examples 4.2 and 4.3, we start with a polynomial that is not asymptotically

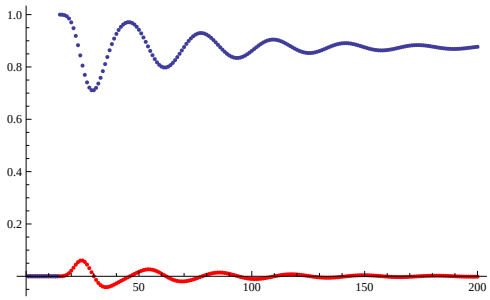

FIGURE 5. Graphical representation of $S(\sigma_{n,15})/2^n$ (blue) vs $S(\sigma_{n,15}+X_1X_2+X_1X_3+X_2X_3)/2^n$ (red).

balanced, however, after we perturb it with a balanced function $F(\mathbf{X})$, the result is asymptotically balanced. In the theorem below we show that these are the only ways to obtain an asymptotically balanced function. In other words, a perturbation of the form

$$\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}+F(\mathbf{X})$$

is asymptotically balanced if and only if $\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}$ is asymptotically balanced or $F(\mathbf{X})$ is balanced.

Theorem 4.4. *Let $1\leq k_1<\cdots<k_s$ be integers and $F(\mathbf{X})$ a binary polynomial in the variables $X_1,\cdots,X_j$ (j fixed). Let $r=\lfloor\log_2(k_s)\rfloor+1$. Then,*

$$S(\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}+F(\mathbf{X}))=c_0(k_1,\cdots,k_s)\cdot\frac{S(F)}{2^j}2^n+O\left(\left(2\cos\left(\frac{\pi}{2^r}\right)\right)^n\right). \tag{4.3}$$

In particular,

$$\lim_{n\to\infty}\frac{1}{2^n}S(\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}+F(\mathbf{X})) \quad=\quad c_0(k_1,\cdots,k_s)\cdot\frac{S(F)}{2^j}. \tag{4.4}$$

Proof. We already know that

$$\left\{\frac{1}{2^n}S(\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}+F(\mathbf{X}))\right\}_{n\in\mathbb{N}} \tag{4.5}$$

is a convergent sequence. The idea in this proof is to construct a subsequence of (4.5) for which we can calculate the limit.

Define $B_n\subseteq\mathbb{F}^n$ to be the set of all $\mathbf{x}$ such that $\sigma_{n,k_1}(\mathbf{x})+\cdots+\sigma_{n,k_s}(\mathbf{x})=1$. Note that

$$\begin{aligned} S(\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}+F(\mathbf{X})) &= \sum_{\mathbf{x}\in\mathbb{F}}(-1)^{F(\mathbf{x})}-2\sum_{\mathbf{x}\in B_n}(-1)^{F(\mathbf{x})} \\ &= 2^{n-j}S(F)-2\sum_{\mathbf{x}\in B_n}(-1)^{F(\mathbf{x})}. \end{aligned} \tag{4.6}$$

Suppose that $2^{r-1}\leq k_s<2^r$ and consider the subsequence

$$\{S(\sigma_{2^rm+2^r-1,k_1}+\cdots+\sigma_{2^rm+2^r-1,k_s}+F(\mathbf{X}))\}_{m\in\mathbb{N}}.$$

It is not hard to see that

$$\begin{aligned} S(\sigma_{2^r m+2^r-1,k_1} &+ \cdots + \sigma_{2^r m+2^r-1,k_s}) \\ &= \sum_{i=0}^{n} (-1)^{\binom{i}{k_1}+\cdots+\binom{i}{k_s}} \binom{2^r m+2^r-1}{i}. \end{aligned}$$

Let $i_1, \cdots, i_p$ be all integers between 1 and 2^r-1 such that $\binom{i_l}{k_1}+\cdots+\binom{i_l}{k_s} \equiv 1 \pmod 2$. We know that $\binom{i}{k_1}+\cdots+\binom{i}{k_s} \pmod 2$ is periodic and the period is a divisor of 2^r. Therefore, $\binom{i}{k_1}+\cdots+\binom{i}{k_s} \equiv 1 \pmod 2$ if and only if $i \equiv i_l \pmod{2^r}$ for some $i_l \in \{i_1, \cdots, i_p\}$. This implies that $\mathbf{x} \in \mathbb{F}^{2^r m+2^r-1}$ is in $B_{2^r m+2^r-1}$ precisely when

$$w_2(\mathbf{x}) \equiv i_l \pmod{2^r}.$$

Therefore,

$$\begin{aligned} S(\sigma_{2^r m+2^r-1,k_1} + &\cdots + \sigma_{2^r m+2^r-1,k_s} + F(\mathbf{X})) \\ &= 2^{2^r m+2^r-1-j} S(F) - 2 \sum_{l=1}^{p} \sum_{w_2(\mathbf{x}) \equiv i_l \bmod 2^r} (-1)^{F(\mathbf{x})}. \end{aligned}$$

Consider the sum

$$\sum_{w_2(\mathbf{x}) \equiv i_l \bmod 2^r} (-1)^{F(\mathbf{x})} = \sum_{q=0}^{m} \sum_{w_2(\mathbf{x}) = 2^r q + i_l} (-1)^{F(\mathbf{x})}.$$

Note that there are

$$\binom{j}{s}\binom{2^r m+2^r-1-j}{2^r q+i_l-s}$$

tuples with $w_2(\mathbf{x}) = 2^r q + i_l$ and exactly s 1's in the first j entries. The values of $(-1)^{F(\mathbf{X})}$ on these tuples sum to

$$C_s(F)\binom{2^r m+2^r-1-j}{2^r q+i_l-s}.$$

Hence,

$$\begin{aligned} \sum_{w_2(\mathbf{x}) \equiv i_l \bmod 2^r} (-1)^{F(\mathbf{x})} &= \sum_{q=0}^{m} \sum_{s=0}^{j} C_s(F)\binom{2^r m+2^r-1-j}{2^r q+i_l-s} \\ &= \sum_{s=0}^{j} C_s(F) \sum_{q=0}^{m} \binom{2^r m+2^r-1-j}{2^r q+i_l-s}. \end{aligned}$$

Recall the series multisection for the sum of binomial coefficients [30]

$$\binom{n}{t} + \binom{n}{t+s} + \binom{n}{t+2s} + \cdots = \frac{1}{s} \sum_{j=0}^{s-1} \left(2\cos\left(\frac{\pi j}{s}\right)\right)^n \cos\left(\frac{\pi(n-2t)j}{s}\right).$$

This implies that

$$\sum_{q=0}^{m} \binom{2^r m+2^r-1-j}{2^r q+i_l-s} = \frac{1}{2^r} \sum_{a=0}^{2^r-1} \left(2\cos\left(\frac{\pi a}{2^r}\right)\right)^{2^r m+2^r-1-j} \cos\left(\frac{\pi(2^r m+2^r-1-j-2(i_l-s))a}{2^r}\right). \tag{4.7}$$

Note that the biggest term of the sum above is

$$\frac{1}{2^r}\cdot 2^{2^r m+2^r-1-j},$$

and it occurs when $a=0$. Moreover, all other terms in the sum are exponentially smaller than $2^{2^r m-1-j-r}$. However,

$$\sum_{w_2(\mathbf{x})\equiv i_l \bmod 2^r}(-1)^{F(\mathbf{x})} = \sum_{s=0}^{j} C_s(F)\sum_{q=0}^{m}\binom{2^r m+2^r-1-j}{2^r q+i_l-s} \tag{4.8}$$

and (4.7) implies

$$\begin{aligned}\sum_{s=0}^{j} C_s(F)\sum_{q=0}^{m}\binom{2^r m+2^r-1-j}{2^r q+i_l-s} &= \sum_{s=0}^{j} C_s(F)2^{2^r m-2^r-1-j-r}+o(2^{2^r m+2^r-1})\\ &= 2^{2^r m+2^r-1-j-r}\sum_{s=0}^{j} C_s(F)+o(2^{2^r m+2^r-1}) \qquad (4.9)\\ &= 2^{2^r m+2^r-1-j-r}S(F)+o(2^{2^r m+2^r-1}).\end{aligned}$$

Equations (4.8) and (4.9) imply

$$\lim_{m\to\infty}\frac{1}{2^{2^r m+2^r-1}}\sum_{w_2(\mathbf{x})\equiv i_l \bmod 2^r}(-1)^{F(\mathbf{x})}=2^{-j-r}S(F).$$

We conclude that

$$\begin{aligned}&\lim_{m\to\infty}\frac{1}{2^{2^r m+2^r-1}}S(\sigma_{2^r m+2^r-1,k_1}+\cdots+\sigma_{2^r m+2^r-1,k_s}+F(\mathbf{X})) \qquad (4.10)\\ &=\lim_{m\to\infty}\frac{1}{2^{2^r m+2^r-1}}\left(2^{2^r m+2^r-1-j}S(F)-2\sum_{l=1}^{p}\sum_{w_2(\mathbf{x})\equiv i_l \bmod 2^r}(-1)^{F(\mathbf{x})}\right)\\ &=2^{-j}S(F)-2\sum_{l=1}^{p}2^{-j-r}S(F)\\ &=(2^{-j}-p\cdot 2^{1-j-r})S(F)\\ &=(1-p\cdot 2^{1-r})2^{-j}S(F).\end{aligned}$$

Finally, it is not hard to see,

$$\begin{aligned}c_0(k_1,\cdots,k_s) &= \frac{1}{2^r}\sum_{i=0}^{2^r-1}(-1)^{\binom{i}{k_1}+\cdots+\binom{i}{k_s}}\\ &= \frac{1}{2^r}(2^r-2p)=1-p\cdot 2^{1-r}.\end{aligned}$$

Since

$$\left\{\frac{1}{2^{2^r m+2^r-1}}S(\sigma_{2^r m+2^r-1,k_1}+\cdots+\sigma_{2^r m+2^r-1,k_s}+F(\mathbf{X}))\right\}_{m\in\mathbb{N}}$$

is a subsequence of

$$\{\frac{1}{2^n}S(\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}+F(\mathbf{X}))\}_{n\in\mathbb{N}},$$

then we conclude that

$$\lim_{n\to\infty}\frac{1}{2^n}S(\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}+F(\mathbf{X}))=c_0(k_1,\cdots,k_s)\cdot\frac{S(F)}{2^j}.$$

□

Remark. Theorem 4.4 generalizes the asymptotic version of Cusick's conjecture, i.e. for k not a power of two, $\sigma_{n,k}$ is asymptotically not balanced. Note that when k is not a power of two, then Theorem 4.4 implies that $\sigma_{n,k}+F(\mathbf{X})$ is asymptotically balanced if and only if $F(\mathbf{X})$ is a balanced function.

Corollary 4.5. *Suppose that $1\leq k_1<\cdots<k_s$ are integers and $F(\mathbf{X})$ a binary polynomials in the variables $X_1,\cdots,X_j$, with j fixed. Then, the polynomial*

$$\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}+F(\mathbf{X})$$

is asymptotically balanced if and only if $\sigma_{n,k_1}+\cdots+\sigma_{n,k_s}$ is asymptotically balanced or $F(\mathbf{X})$ is a balanced function.

Proof. This is a direct consequence of Theorem 4.4. □

Example 4.6. Consider the following perturbation (a generalization to the perturbation in Example 3.4),

$$\sigma_{n,5}+\sigma_{n,3}+X_1X_2X_3\cdots X_j.$$

The reader can check that

$$S(X_1X_2X_3\cdots X_j)=2^j-2.$$

Also,

$$c_0(5,3)=\frac{1}{2},$$

and so

$$c_0(5,3)\cdot\frac{S(F)}{2^j}=\frac{2^{j-1}-1}{2^j}.$$

Theorem 4.4 tells us that

$$\lim_{n\to\infty}\frac{1}{2^n}S(\sigma_{n,5}+\sigma_{n,3}+X_1X_2X_3\cdots X_j)=\frac{2^{j-1}-1}{2^j}.$$

5. A result about binomial coefficients

In this section we present a relation between the asymptotic coefficients of symmetric polynomials. This relation, in turns, will provide us with a relation about the parity of some sums of binomial coefficients.

Recall that if $1\leq k_1<\cdots<k_s$ and $r=\lfloor\log_2(k_s)\rfloor+1$, then

$$\lim_{n\to\infty}\frac{1}{2^n}S(\sigma_{n,k_1}+\cdots+\sigma_{n,k_s})=c_0(k_1,\cdots,k_s),$$

where

$$c_0(k_1,\cdots,k_s)=\frac{1}{2^r}\sum_{i=0}^{2^r-1}(-1)^{\binom{i}{k_1}+\cdots+\binom{i}{k_s}}. \tag{5.1}$$

We say that the degree of the asymptotic coefficient is k_s, i.e. the degree of an asymptotic coefficient is the biggest argument. We introduce the following notation. Consider the expression

$$c_0\left(k, \binom{m}{1}_2(k-1), \binom{m}{2}_2(k-2), \cdots, \binom{m}{m-1}_2(k-m+1), k-m\right). \tag{5.2}$$

We interpret $\binom{m}{i}_2$ as

$$\binom{m}{i} \mod 2.$$

However, if

$$\binom{m}{i} \equiv 0 \mod 2,$$

then the term $\binom{m}{i}_2(k-i)$ is *not* an argument of c_0. For example,

$$\begin{aligned} c_0\left(k, \binom{3}{1}_2(k-1), \binom{3}{2}_2(k-2), k-3\right) &= c_0(k, k-1, k-2, k-3) \\ c_0\left(k, \binom{4}{1}_2(k-1), \binom{4}{2}_2(k-2), \binom{4}{3}_2(k-3), k-4\right) &= c_0(k, k-4). \end{aligned}$$

We now present one of the main results of this section.

Theorem 5.1. *Suppose that $k \geq 2$ be an integer and let $m < k$. Then,*

$$c_0(k) = c_0\left(k, \binom{m}{1}_2(k-1), \binom{m}{2}_2(k-2), \cdots, \binom{m}{m-1}_2(k-m+1), k-m\right).$$

Proof. Apply Theorem 3.2 with $F(\mathbf{X}) = X_1 + \cdots + X_j$ to get

$$S(\sigma_{n,k} + X_1 + \cdots + X_j) = \sum_{l=0}^{j} (-1)^l \binom{j}{l} S\left(\sum_{i=0}^{l} \binom{l}{i} \sigma_{n-j,k-i}\right).$$

Divide each side of the above equation by 2^n, let $n \to \infty$, use the fact that $F(\mathbf{X}) = X_1 + \cdots + X_j$ is balanced, and apply Theorem 4.4 to get

$$0 = \frac{1}{2^j} \sum_{l=0}^{j} (-1)^l \binom{j}{l} c_0\left(k, \binom{l}{1}_2(k-1), \cdots, \binom{l}{l-1}_2(k-l+1), k-l\right). \tag{5.3}$$

We use (5.3) to prove the theorem by induction.

Suppose that $m = 1$. Note that if $j = 1$, then (5.3) implies $0 = c_0(k) - c_0(k, k-1)$. Therefore, the theorem is true if $m = 1$. Suppose the theorem holds for $j \leq m-1$, that is

$$\begin{aligned} c_0(k) &= c_0(k, k-1) = c_0(k, k-2) = \cdots \\ &= c_0\left(k, \binom{m-1}{1}_2(k-1), \binom{m-1}{2}_2(k-2), \cdots, \binom{m-1}{m-2}_2(k-m+2), k-m+1\right). \end{aligned}$$

Let $j = m$. Then,

$$0 = \frac{1}{2^m} \sum_{l=0}^{m} (-1)^l \binom{m}{l} c_0\left(k, \binom{l}{1}_2(k-1), \cdots, \binom{l}{l-1}_2(k-l+1), k-l\right).$$

This equivalent to

$$\begin{aligned} 0 &= \sum_{l=0}^{m-1}(-1)^l\binom{m}{l}c_0\left(k,\binom{l}{1}_2(k-1),\cdots,\binom{l}{l-1}_2(k-l+1),k-l\right) \\ &\quad +(-1)^m c_0\left(k,\binom{m}{1}_2(k-1),\cdots,\binom{m}{l-1}_2(k-m+1),k-m\right). \end{aligned}$$

Apply the induction hypothesis to get

$$\begin{aligned} 0 &= \sum_{l=0}^{m-1}(-1)^l\binom{m}{l}c_0\left(k\right) \\ &\quad +(-1)^m c_0\left(k,\binom{m}{1}_2(k-1),\cdots,\binom{m}{l-1}_2(k-m+1),k-m\right) \\ &= (-1)^{m-1}c_0(k)+(-1)^m c_0\left(k,\binom{m}{1}_2(k-1),\cdots,\binom{m}{l-1}_2(k-m+1),k-m\right). \end{aligned}$$

We conclude that

$$c_0(k)=c_0\left(k,\binom{m}{1}_2(k-1),\cdots,\binom{m}{l-1}_2(k-m+1),k-m\right)$$

and the theorem holds. □

Therem 5.1 can be generalized. We first extend the definition of $c_0(k_1,\cdots,k_s)$, which is originally defined for $1\leq k_1<\cdots<k_s$. Note that if we allow k_1 to be zero, then, by definition (5.1), we obtain

$$c_0(0,k_2,\cdots,k_s)=-c_0(k_2,\cdots,k_s). \tag{5.4}$$

This is consistent with the interpretation $\sigma_{n,0}=1$ and $S(G(\mathbf{X})+1)=-S(G(\mathbf{X}))$. Moreover, if we allow some (not all) of the k_i to be negative, let say $k_1<k_2<\cdots<k_j<0<k_{j+1}<\cdots k_s$, then (5.1) implies

$$c_0(k_1,\cdots,k_j,k_{j+1},\cdots,k_s)=c_0(k_{j+1},\cdots,k_s). \tag{5.5}$$

This is consistent with the fact that if $k_1<k_2<\cdots<k_j<0<k_{j+1}<\cdots k_s$, then $\sigma_{n,k_1}+\cdots+\sigma_{n,k_j}+\sigma_{n,k_{j+1}}+\cdots+\sigma_{n,k_s}=\sigma_{n,k_{j+1}}+\cdots+\sigma_{n,k_s}$, since the terms $\sigma_{n,k_1},\cdots,\sigma_{n,k_j}$ do not exist.

Also, repetitions can be allowed. Let say that $k_1=k_2$, then (5.1) implies

$$c_0(k_1,k_1,k_3,\cdots,k_s)=c_0(k_3,\cdots,k_s). \tag{5.6}$$

This is consistent with the fact that

$$S(2\sigma_{n,k_1}+\sigma_{n,k_3}+\cdots+\sigma_{n,k_s})=S(\sigma_{n,k_3}+\cdots+\sigma_{n,k_s}).$$

The same happens if one of the k_i's is repeated an even amount of times (as an argument of c_0). On the other hand, if one of the k_i's is repeated an odd amount of times, say $k_1=k_2=k_3$, then

$$c_0(k_1,k_1,k_1,k_4\cdots,k_s)=c_0(k_1,k_4,\cdots,k_s). \tag{5.7}$$

This is consistent with the fact that

$$S(3\sigma_{n,k_1}+\sigma_{n,k_4}+\cdots+\sigma_{n,k_s})=S(\sigma_{n,k_1}+\sigma_{n,k_4}+\cdots+\sigma_{n,k_s}).$$

In summary, if k_i is repeated an even amount of times, then we drop it from the arguments. On the other hand, if k_i is repeated an odd amount of times, then we leave it as an argument, but we only write it once.

We are now in position of providing a generalization of Theorem 5.1. But, before doing this, we introduce yet another notation. We write $[a_i]_{i=1}^n$ to represent the list $a_1, a_2, \cdots, a_n$. In other words,

$$[a_i]_{i=1}^n = a_1, a_2, \cdots, a_n.$$

For example,

$$[i^2]_{i=1}^4 = 1, 4, 9, 16$$
$$[2i+1]_{i=1}^5 = 3, 5, 7, 9, 11$$
$$[b_i]_{i=1}^3 = b_1, b_2, b_3.$$

Next, is a generalization of Theorem 5.1.

Theorem 5.2. *Suppose that $1 \leq k_1 < \cdots < k_s$ and m be any positive integer. Then,*

$$c_0(k_1, \cdots, k_s) =$$
$$c_0\left([k_i]_{i=1}^s, \left[\binom{m}{1}_2 (k_i - 1)\right]_{i=1}^s, \cdots, \left[\binom{m}{m-1}_2 (k_i - m + 1)\right]_{i=1}^s, [k_i - m]_{i=1}^s\right).$$

Proof. The proof is basically the same induction as in the proof of Theorem 5.1. The only difference is that now we use the interpretations (5.4), (5.5), (5.6), and (5.7). □

Remark. Theorems 5.1 and 5.2 provide a method to compute the asymptotic behavior for all the symmetric boolean functions of degree k_s from only knowing few of them. See next examples.

Example 5.3. Consider the case when the degree is 3. In this case, Theorems 5.1 and 5.2 imply

$$\begin{aligned} c_0(3) &= c_0(3,2) \\ c_0(3) &= c_0\left(3, \binom{2}{1}_2 \cdot 2, 1\right) = c_0(3,1) \\ c_0(3) &= c_0\left(3, \binom{3}{1}_2 \cdot 2, \binom{3}{2}_2 \cdot 1, 0\right) = c_0(3,2,1,0) = -c_0(3,2,1). \end{aligned}$$

This covers all cases. Since $c_0(3) = 1/2$, then we conclude that $c_0(3,2) = c_0(3,1) = 1/2$ and $c_0(3,2,1) = -1/2$.

Example 5.4. Consider now the case when the degree is 5. In this case, there are 16 asymptotic coefficients. We only need to know two of them in order to get the rest. Start with $c_0(5) = 1/2$ and apply Theorems 5.1 and 5.2 to get

$$\begin{aligned} &\text{when } m = 1: && c_0(5) = c_0(5,4) \\ &\text{when } m = 2: && c_0(5) = c_0(5,3) \\ &\text{when } m = 3: && c_0(5) = c_0(5,4,3,2) \\ &\text{when } m = 4: && c_0(5) = c_0(5,1) \\ &\text{when } m = 5: && c_0(5) = c_0(5,4,1,0) = -c_0(5,4,1) \\ &\text{when } m = 6: && c_0(5) = c_0(5,3,1,-1) = c_0(5,3,1) \\ &\text{when } m = 7: && c_0(5) = c_0(5,4,3,2,1,0,-1,-2) = -c_0(5,4,3,2,1). \end{aligned}$$

The reader can check that these are all the asymptotic coefficients that can be obtained from $c_0(5)$, i.e. $m \geq 8$ produces a coefficient that is already listed above. To proceed, now choose a coefficient that is not listed above, let say $c_0(5,4,3) = 0$. Apply Theorem 5.2 to get

$$\begin{aligned}
&\text{when } m = 1: && c_0(5,4,3) = c_0(5,4,4,3,3,2) = c_0(5,2)\\
&\text{when } m = 2: && c_0(5,4,3) = c_0(5,3,4,2,3,1) = c_0(5,4,2,1)\\
&\text{when } m = 3: && c_0(5,4,3) = c_0(5,4,3,2,4,3,2,1,3,2,1,0) = -c_0(5,3,2)\\
&\text{when } m = 4: && c_0(5,4,3) = c_0(5,1,4,0,3,-1) = -c_0(5,4,3,1)\\
&\text{when } m = 5: && c_0(5,4,3) = c_0(5,4,1,0,4,3,0,-1,3,2,-1,-2) = c_0(5,2,1)\\
&\text{when } m = 6: && c_0(5,4,3) = c_0(5,3,1,-1,4,2,0,-2,3,1,-1,-3) = -c_0(5,4,2)\\
&\text{when } m = 7: && c_0(5,4,3) = c_0(5,4,3,2,1,0,-1,-2,4,3,2,1,0,-1,-2,-3,3,2,1,0,-1,-2,-3,-4)\\
& && \quad = -c_0(5,3,2,1).
\end{aligned}$$

This completes the list of all asymptotic coefficients.

Remark. It turns out that, using our method, all the 32 asymptotic coefficients of degree 6 can be obtained from $c_0(6), c_0(6,5,4), c_0(6,5,3)$, and $c_0(6,5,2)$. It appears that the amount of asymptotic coefficients needed for our method to compute all asymptotic coefficients of degree k_s grows exponentially in k_s.

Theorems 5.1 and 5.2 also provide us with a relationship between some sums of binomial coefficients. Suppose that $1 \leq k_1 < \cdots < k_s$ and $r = \lfloor \log_2(k_s) \rfloor + 1$. Recall that

$$c_0(k_1, \cdots, k_s) = \frac{1}{2^r} \sum_{i=0}^{2^r-1} (-1)^{\binom{i}{k_1} + \cdots + \binom{i}{k_s}}.$$

Note that $c_0(k_1, \cdots, k_s)$ counts the number of times $\binom{i}{k_1} + \cdots + \binom{i}{k_s}$ is odd when i runs from 0 to $2^r - 1$. This has the following implication.

Theorem 5.5. *Let $1 \leq k_1 < \cdots < k_s$ and $r = \lfloor \log_2(k_s) \rfloor + 1$. If two asymptotic coefficients of degree k_s are equal, say $c_0(k_{l_1}, k_{l_2}, \cdots, k_s) = c_0(k_{j_1}, k_{j_2}, \cdots, k_s)$, then both lists*

$$\left[\binom{i}{k_{l_1}} + \binom{i}{k_{l_2}} + \cdots + \binom{i}{k_s} \right]_{i=0}^{2^r-1}$$

and

$$\left[\binom{i}{k_{j_1}} + \binom{i}{k_{j_2}} + \cdots + \binom{i}{k_s} \right]_{i=0}^{2^r-1}$$

have the same amount of odd numbers. On the other hand, if $c_0(k_{l_1}, k_{l_2}, \cdots, k_s) = -c_0(k_{j_1}, k_{j_2}, \cdots, k_s)$, then the amount of odd numbers in

$$\left[\binom{i}{k_{l_1}} + \binom{i}{k_{l_2}} + \cdots + \binom{i}{k_s} \right]_{i=0}^{2^r-1}$$

is the same as the amount of even numbers in

$$\left[\binom{i}{k_{j_1}} + \binom{i}{k_{j_2}} + \cdots + \binom{i}{k_s} \right]_{i=0}^{2^r-1}$$

and viceversa.

Proof: This is a direct consequence of Theorems 5.1 and 5.2.

Remark. Lucas' Theorem can be used to obtain the parity of a binomial coefficient. However, our method avoids the difficulty of the calculation of the parity of each individual binomial coefficient to obtain the result of Theorem 5.5.

Example 5.6. Consider the case of degree 5. The complete list of asymptotic coefficients of degree five appears in Example 5.4. Note that $c_0(5,4,3,2) = c_0(5,1)$. Therefore, the lists $\left[\binom{i}{5}+\binom{i}{4}+\binom{i}{3}+\binom{i}{2}\right]_{i=0}^{7}$ and $\left[\binom{i}{5}+\binom{i}{1}\right]_{i=0}^{7}$ contain the same amount of odd numbers (which in this case is 2):

$$\left[\binom{i}{5}+\binom{i}{4}+\binom{i}{3}+\binom{i}{2}\right]_{i=0}^{7} = 0,0,1,4,11,26,56,112$$

$$\left[\binom{i}{5}+\binom{i}{1}\right]_{i=0}^{7} = 0,1,2,3,4,6,12,28.$$

We also know that $c_0(5,4,3,2) = -c_0(5,4,3,2,1)$. Therefore, the amount of odd numbers in $\left[\binom{i}{5}+\binom{i}{4}+\binom{i}{3}+\binom{i}{2}+\binom{i}{1}\right]_{i=0}^{7}$ is the same as the amount of even numbers in $\left[\binom{i}{5}+\binom{i}{4}+\binom{i}{3}+\binom{i}{2}\right]_{i=0}^{7}$, which in this case is 6:

$$\left[\binom{i}{5}+\binom{i}{4}+\binom{i}{3}+\binom{i}{2}+\binom{i}{1}\right]_{i=0}^{7} = 0,1,3,7,15,31,62,119.$$

Acknowledgments. We would like to thank Professor Thomas W. Cusick for his helpful comments and suggestions in a previous version of this paper.

References

[1] C. Bey and G. M. Kyureghyan, *On Boolean functions with the sum of every two of them being bent*, Des. Codes Cryptogr., **49**, 341–346, 2008.

[2] R. E. Canfield, Z. Gao, C. Greenhill, B. McKay and R. W. Robinson, Asymptotic enumeration of correlation-immune Boolean functions, *Cryptogr. Commun.*, **2**, 111-126, 2010

[3] J. Y. Cai, F. Greeen, and T. Thierauf. On the Correlation of Symmetric Functions. *Theory of Computing Systems*, **29**, 245–258, 1996.

[4] A. Canteaut and M. Videau, *Symmetric Boolean Functions, IEEE Transactions on Information Theory*, **51**, 2791–2807, 2005.

[5] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Eds. Yves Crama and Peter Hammer, Cambridge University Press, 2010.

[6] C. Carlet, X. Zeng, C. Li, and L. Hu, Further properties of several classes of Boolean functions with optimum algebraic immunity, *Des. Codes Cryptogr.*, **52**, 303-338, 2009.

[7] C. Carlet, On the Degree, Nonlinearity, algebraic thinckness and non-normality of Boolean Functions, with Developments on Symmetric Functions, *IEEE Trans. Inform. Theory* **50**, 2178-2185, 2004.

[8] F. Castro and L. A. Medina. Linear recurrences and asymptotic behavior of exponential sums of symmetric boolean functions. *Elec. J. Combinatorics*, 18(2):#P8, 2011.

[9] T. W. Cusick, and Y. Li, kth Order Symmetric SAC Boolean Functions and Bisecting Binomial Coefficients, *Discrete. Appl. Math.* **149**, 73-86, 2005.

[10] Y. Li and T. W. Cusick, Linear Structures of Symmetric Functions over Finite Fields, *Inf. Processing Letters* **97**, 124-127, 2006.

[11] T. Cusick, Y. Li, and P. Stănică, Balanced Symmetric Functions over $GF(p)$. *IEEE Trans. on Information Theory*, **54**, 1304-1307, 2008.

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

[13] T. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications*, Academic Press, 2009.
[14] M. Bileschi, T. Cusick, and D. Padgett, Weights of Boolean Cubic Monomial Rotation Symmetric Functions, *Crytogr. Commun.* **4**, 105-130, 2012.
[15] T. Cusick, Finding Hamming Weights Without Looking at Truth Tables, *Crytogr. Commun.* **5**, 7-18, 2013.
[16] D. K. Dalai, S. Maitra, and Sarkar, Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity, *Des. Codes, Cryptogr.* **40**, 41-58, 2006.
[17] K. Feng, F. Lui, L. J. Qu and L. Wang, Constructing Symmetric Boolean Functions with Maximum Algebraic Immunity, *IEEE Trans. Inform. Theory*, **55**, 2406-2412, 2009.
[18] D.J.H. Garling, *A Course in Galois Theory*, Cambridge University Press, 1986.
[19] S. Maitra and P. Sarkar, Maximum Nonlinearity of Symmetric Boolean Functions on Odd Number of Variables, *IEEE Trans. Inform. Theory* **48**, 2626-2630, 2002.
[20] W. Meier, F. Pasalic and C. Carlet, Algebraic Attack and Decomposition of Boolean Functions, *in Advances Crytology-EUROCRYPT 2004*(Lectures Notes in Computer Science), Berlin, Germany: Springer-Verlag **3027** , 474-491, 2004.
[21] D. Olejár and M. Stanek, On Cryptographic Properties of Random Boolean Functions, *J. UCS* **4**, 705-717, 1998.
[22] L. J. Qu, C. Li and K. Feng, A Note on Symmetric Boolean Functions with Maximum Algebraic Degree, *IEEE Trans. Inform. Theory*, **53**, 2908-2910, 2007.
[23] F. Rodier, Asymptotic Nonlinearity of Boolean Functions, *Des. Codes Cryptogr.*, **40**, 59-70, 2006.
[24] O. S. Rothaus, On Bent functions. *J. Combin. Theory Ser. A*, **20**, 300-305, 1976.
[25] P. Sarkar and S. Maitra, Balancedness and correlation immunity of symmetric Boolean functions. *Discrete Mathematics*, **307**, 3251-2358, 2007.
[26] P. Savicky, On the Bent Boolena Functions that are Symmetric, *European J. Combin.* **15**, 407-410, 1994.
[27] W. Su, X. Tang and A. Pott, A Note on a Conjecture for Balanced Elementary Symmetric Boolean Functions,*IEEE Trans. Inform. Theory*(accepted).
[28] J. von zur Gathen and J. Roche, Polynomial with Two Values, *Combinatorica*, **17**, 345-362, 1997.
[29] H. Wang, J. Peng, Y. Li and H. Kan, $2k$-Variables Symmetric Boolean Functions with Maximum Algebraic Immunity k, arXiv:1111.212v1.
[30] E. W. Weisstein, "Series Multisection", From MathWorld, a Wolfram Research Inc. web resource.
[31] C.-k. Wu, and E. Dawson, Correlation Inmmunity and Resiliency of Symmetric Boolean Functions, *Theoret. Comput. Sci.* **312**, 321-335, 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: luis.medina17@upr.edu