P-RECURSIVITY OF SOME FAMILIES OF BOOLEAN FUNCTIONS UNDER BIASED WALSH TRANSFORMS

AXEL O. GÓMEZ-FLORES, LUIS A. MEDINA, AND PANTELIMON STĂNICĂ

ABSTRACT. We showed that, under certain conditions, restricted and biased exponential sums and Walsh transforms of symmetric and rotation symmetric Boolean functions are, as in the case of non-biased domain, C-finite sequences. We also showed that under other conditions, these sequences are P-recursive, which is a somewhat different behavior than their non-biased counterparts. We also show that exponential sums and Walsh transforms of a family of rotation symmetric monomials over the restricted domain $E_{n,j} = \{\mathbf{x} \in \mathbb{F}_2^n : wt(\mathbf{x}) = j\}$ ($wt(\mathbf{x})$ is the weight of the vector $\mathbf{x}$) are given by polynomials of degree at most j, and so, they are also C-finite sequences. Finally, we also present a study of the behavior of symmetric Boolean functions under these biased transforms.

1. INTRODUCTION

An n-variable Boolean function is a function from $\mathbb{F}_2^n \to \mathbb{F}_2$ where $\mathbb{F}_2$ represents the field of two elements and $\mathbb{F}_2^n$ is the vector space of dimension n over $\mathbb{F}_2$. These functions have application to different scientific fields like coding theory, cryptography and information theory. The set of all n-variables Boolean functions is usually denoted by $\mathcal{B}_n$.

A Boolean function $f \in \mathcal{B}_n$ can be regarded as a multi-variable polynomial called the *algebraic normal form* (or ANF for short) of f. To be specific, f can be viewed as

$$f(X_1, \ldots, X_n) = a_0 \oplus \sum_{1 \le i \le n} a_i X_i \oplus \sum_{1 \le i < j \le n} a_{ij} X_i X j \oplus \cdots \oplus a_{12\cdots n} X_1 X_2 \cdots X_n,$$

where $a_0, a_i, a_{ij}, \ldots, a_{12\cdots n} \in \mathbb{F}_2$ and $\oplus$ represents addition modulo 2. The *algebraic degree* of a Boolean function f is the degree of its ANF representation. The *Hamming weight* of a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, which is usually denoted by $wt(\mathbf{x})$, is the number of 1's in $\mathbf{x}$.

The (unnormalized) *Walsh transform* at $\boldsymbol{a} \in \mathbb{F}_2^n$ of $f \in B_n$ is defined as the real valued function

$$W_f(\boldsymbol{a}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \boldsymbol{a} \cdot \mathbf{x}},$$

where $\boldsymbol{a} \cdot \mathbf{x}$ represents the usual scalar product. We sometimes encounter in literature this transform normalized by the factor $2^{-n/2}$. The *nonlinearity* of a Boolean function $f \in \mathcal{B}_n$ is the distance from f to the set of affine functions in n variables,

$$\mathrm{nl}(f) = \min_{g \text{ affine}} \mathrm{dist}(f, g),$$

where $\mathrm{dist}(f, g)$ is the Hamming distance (number of bits where they differ) between f and g. The *spectral amplitude* of a Boolean function f, denoted by $\mathrm{Spec}(f)$, is defined by

$$\mathrm{Spec}(f) = \max_{\mathbf{a} \in \mathbb{F}_2^n} |W_f(\boldsymbol{a})|.$$

Date: June 5, 2020.

2010 *Mathematics Subject Classification.* 05E05, 11T23, 11B37.

Key words and phrases. biased Walsh transform, restricted Walsh transform, restricted domains, symmetric Boolean functions, rotation symmetric Boolean functions, linear recurrences.

The spectral amplitude of a Boolean function is related to its nonlinearity via the equation

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2}\mathrm{Spec}(f).$$

Highly nonlinear Boolean functions are desirable in some cryptographic applications. Boolean functions with the highest nonlinearity, i.e. $2^{n-1} - 2^{n/2-1}$ (n even) are known as *bent functions*. These functions were introduced in the mid 1960's in [27]. Observe that an n-variable Boolean function f is bent if

$$\frac{1}{2^{n/2}}|W_f(\boldsymbol{a})| = 1, \text{ for all } \boldsymbol{a} \in \mathbb{F}_2^n.$$

Another desirable property in cryptographic applications is balancedness. Order the elements of $\mathbb{F}_2^n$ lexicographically and denote $\mathbf{x}_0 = (0, 0, \ldots, 0, 0)$, $\mathbf{x}_1 = (0, 0, \ldots, 0, 1)$, $\ldots$, $\mathbf{x}_{2^n-1} = (1, 1, \ldots, 1, 1)$. The *truth table* of a Boolean function $f \in \mathcal{B}_n$ is the vector $[f(\mathbf{x}_0), f(\mathbf{x}_1), \ldots, f(\mathbf{x}_{2^n-1})]$. A Boolean function f is said to be *balanced* if the number of 0's and the number of 1's in its true table are the same, that is, $wt(f) = 2^{n-1}$ ($wt(f)$ is the Hamming weight of f's truth table).

Balancedness of Boolean functions is often studied from the point of view of exponential sums. The *exponential sum* of a Boolean function $f \in \mathcal{B}_n$ is defined as

$$S(f) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x})}.$$

Observe that the exponential sum of a Boolean function coincides with its Walsh transform at $\boldsymbol{a} = \mathbf{0}$, that is, $S(f) = W_f(\mathbf{0})$. Also, a Boolean function f is balanced if and only if $S(f) = 0$. For a comprehensive study of Boolean functions, please refer to [2, 5, 18].

Balancedness of some special classes of Boolean functions, like symmetric and rotation symmetric Boolean functions, have been extensively studied and are an active area of research [1, 4, 7, 8, 9, 14, 15, 16, 17, 19, 21, 24, 28, 29]. A Boolean function $f \in \mathcal{B}_n$ is *symmetric* if it is fixed under the action of the symmetric group S_n of n symbols, that is, if

$$f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n), \text{ for every } \sigma \in S_n.$$

It is a well-established result that every symmetric Boolean function $f \in \mathcal{B}_n$ can be identified with an expression of the form

$$f = \boldsymbol{e}_{n,k_1} \oplus \cdots \oplus \boldsymbol{e}_{n,k_s}, \tag{1.1}$$

where $0 \leq k_1 < k_2 < \cdots < k_s$ are integers and $\boldsymbol{e}_{n,k}$ represents the n-variable *elementary symmetric polynomial* of degree k. For simplicity, we denote the linear combination on the right-hand side of (1.1) as $\boldsymbol{e}_{n,[k_1,\ldots,k_s]}$. Symmetric Boolean functions are useful in efficient implementations (thanks to their symmetry), however, they may be vulnerable to attacks.

A Boolean function $f \in \mathcal{B}_n$ is *rotation symmetric* if it is fixed under the action of the cyclic group C_n of n elements, that is, if

$$f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n), \text{ for every } \sigma \in C_n.$$

Rotation symmetric Boolean functions where introduced by Pieprzyk and Qu [26] (although, they did appear before in the work of Filiol and Fontaine [20] as idempotents). As in the case of symmetric Boolean functions, these functions have efficient implementations. However, Pieprzyk and Qu showed that these functions are useful, among other things, in the design of fast hashing algorithms with strong cryptographic properties. Let $1 < j_1 < \cdots < j_s$ be integers. A rotation symmetric Boolean function of the form

$$R_{n,[j_1,\ldots,j_s]} = X_1X_{j_1} \cdots X_{j_s} \oplus X_2X_{j_1+1} \cdots X_{j_s+1} \oplus \cdots \oplus X_nX_{j_1-1} \cdots X_{j_s-1},$$

where the indices are taken modulo n and the complete system of residues mod n is $\{1, 2, \ldots, n\}$, is called a *monomial rotation symmetric* Boolean function on n variables. We say that $R_{n,[j_1,\ldots,j_s]}$ is a *long cycle* if the period is n and a *short cycle*, if the period is a nontrivial divisor of n (we then

make the convention in the above displayed equation that we stop "shifting" indices if we encounter one of the previous terms, otherwise a short cycle would always sum to 0). The function

$$R_{5,[2,3]} = X_1X_2X_3 \oplus X_2X_3X_4 \oplus X_3X_4X_5 \oplus X_4X_5X_1 \oplus X_5X_1X_2$$

is an example of a long cycle, while

$$R_{4,[3]} = X_1X_3 \oplus X_2X_4$$

is an example of a short cycle.

It is known that under certain conditions, exponential sums and Walsh transforms of symmetric Boolean functions and rotation symmetric Boolean functions are C-finite sequences [3, 7, 8, 10, 12, 13, 16, 17]. We say that a sequence $\{a(n)\}$ of real numbers satisfies a homogeneous linear recurrence with constant coefficients, or that it is *C-finite*, if there is a positive integer d and some constants $c_0, \ldots, c_d \in \mathbb{R}$, with $c_d \neq 0$, such that

$$\sum_{\ell=0}^{d} c_\ell \, a(n+\ell) = 0. \tag{1.2}$$

Many classical sequences, like Fibonacci and Lucas numbers, are defined by this type of recurrences. C-finite sequences are well-understood: solutions to a recurrence relation of type (1.2) are tied to roots of a polynomial called the *characteristic polynomial* of the relation.

We say that a sequence $\{a(n)\}$ satisfies a homogeneous linear recurrence with polynomial coefficients, or that it is *holonomic* or *P-recursive*, if there is a positive integer d and some polynomials $p_0(n), \ldots, p_d(n)$, with $p_d(n)$ not identically zero, such that

$$\sum_{\ell=0}^{d} p_\ell(n) \, a(n+\ell) = 0.$$

Classical examples of P-recursive sequences include the factorial sequence $\{n!\}$, which satisfies

$$a(n+1) - (n+1)a(n) = 0,$$

the central binomial coefficients $\binom{2n}{n}$, which satisfy

$$(n+1)a(n+1) - (4n+2)a(n) = 0,$$

and the Motzkin numbers

$$M_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{1}{k+1} \binom{n}{2k} \binom{2k}{k},$$

which satisfy

$$(n+4)a(n+2) - (2n+5)a(n+1) - (3n+3)a(n) = 0.$$

It is clear that every C-finite sequence is P-recursive, but not the other way around. P-recursive sequences were introduced (formally) by Stanley [30]. There are various celebrated results in this area of mathematics, and we mention here Zeilberger's Algorithm [32], as a famous example. A great read about P-recursive sequences is [31].

In [3, 7] it was shown that exponential sums of symmetric Boolean functions are C-finite. To be specific, if $1 \leq k_1 < \cdots < k_s$ are integers and $r = \lfloor \log_2(k_s) \rfloor + 1$, then $\{S(\boldsymbol{e}_{n,[k_1,\ldots,k_s]})\}$ satisfies the recurrence

$$a(n) = \sum_{j=1}^{2^r-1} (-1)^{j-1} \binom{2^r}{j} a(n-j),$$

whose characteristic polynomial is given by

$$(X-2)\Phi_4(X-1)\Phi_8(X-1)\cdots\Phi_{2^r}(X-1).$$

This result was later extended to exponential sums of perturbations of them in [8], to their Walsh transforms in [12] and to finite fields beyond $\mathbb{F}_2$ in [10, 11].

In [13], Cusick showed that weights (equivalent to exponential sums) of rotation symmetric Boolean functions are also C-finite. This was later extended to Walsh transforms of these [12] and to other finite fields [10]. In the case of [10], their results were obtained using auxiliary functions which they called *trapezoid function*. These functions are defined as

$$T_{n,[j_1,\ldots,j_s]} = X_1X_{j_1}\cdots X_{j_s} \oplus X_2X_{j_1+1}\cdots X_{j_s+1} \oplus \cdots \oplus X_{n+1-j_s}X_{j_1+n-j_s}\cdots X_{j_{s-1}+n-j_s}X_n.$$

Observe that $T_{n,[j_1,\ldots,j_s]}$ is the expression before the rotation part of $R_{n,[j_1,\ldots,j_s]}$.

In this article, we show that some of these results can be extended to both classes of Boolean functions over restricted and biased domains. Let $f \in \mathcal{B}_n$ and $E \subset \mathbb{F}_2^n$. Define the (scaled) restricted exponential sum of f over E as

$$S(f;E) = \sum_{\mathbf{x}\in E} (-1)^{f(\mathbf{x})}.$$

Similarly, define the (scaled) restricted Walsh transform of f over E at $\boldsymbol{a}$ as

$$W_f(\boldsymbol{a};E) = \sum_{\mathbf{x}\in E} (-1)^{f(\mathbf{x})\oplus \boldsymbol{a}\cdot\mathbf{x}}.$$

Boolean functions over restricted domains have been a subject of study recently [6, 22, 23, 25], especially in the context of the FLIP cipher. In general, when working over restricted domains, the distribution is non-uniform, and the cryptographic properties of the involved Boolean function may change significantly. In [22], the concepts of biased exponential sum and biased Walsh transform of a Boolean function were introduced. Let $p(\mathbf{u})$ be a probability distribution on $\mathbb{F}_2^n$. If $f \in \mathcal{B}_n$ and $\boldsymbol{a} \in \mathbb{F}_2^n$, then the *biased Walsh transform* of f at $\boldsymbol{a}$ is defined as

$$W_f^B(\boldsymbol{a};p) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(-1)^{f(\mathbf{x})\oplus \boldsymbol{a}\cdot x}.$$

We are mostly interested in the *biased exponential sum* of f as defined by

$$S^B(f;p) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(-1)^{f(\mathbf{x})}.$$

(Observe that $S^B(f;p) = W_f^B(\mathbf{0};p)$.)

In this article, we show that, under certain conditions, restricted and biased exponential sums and Walsh transforms of symmetric and rotation symmetric Boolean functions are, as is the case of non-biased domain, C-finite sequences. However, we also show that under some other conditions, these sequences are P-recursive. This is a different behavior than their non-biased counterparts. In Section 3 we show that exponential sums of a family of rotation monomials over the restricted domain $E_{n,k} = \{\mathbf{x} \in \mathbb{F}_2^n : wt(\mathbf{x}) = j\}$ is given by a polynomial of degree $j+1$. That implies that they are also C-finite sequences. Finally, in the last section, we study the behavior of symmetric Boolean functions under these biased transforms.

2. Recurrences over biased domains

As in the case of regular exponential sums and Walsh transforms, under certain conditions, biased exponential sums and biased Walsh transforms are C-finite sequences. That is the case when the probability distribution depends only on the first entry of $\mathbf{x} \in \mathbb{F}_2^n$ and the argument is somewhat simple.

Let $\alpha \in \mathbb{R}$ be algebraic such that

$$\alpha^n, \frac{1}{2^{n-1}} - \alpha^n \in (0,1),$$

for every integer $n \geq 1$. Define, for $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, the probability distribution

$$p_\alpha(\mathbf{x}) = \begin{cases} \alpha^n, & x_1 = 0 \\ \frac{1}{2^{n-1}} - \alpha^n, & x_1 = 1 \end{cases} \tag{2.1}$$

and consider the biased exponential sum

$$S^B(f; p_\alpha) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} p_\alpha(\mathbf{x})(-1)^{f(\mathbf{x})}.$$

Suppose that $f_n \in \mathcal{B}_n$ is such that the sequences

$$\left\{ \sum_{\mathbf{x} \in \mathbb{F}_2^{n-1}} (-1)^{f_n(0,\mathbf{x})} \right\}_n \text{ and } \left\{ \sum_{\mathbf{x} \in \mathbb{F}_2^{n-1}} (-1)^{f_n(1,\mathbf{x})} \right\}_n$$

satisfy linear recurrences with constant coefficients whose characteristic polynomials are given by $q_0(X)$ and $q_1(X)$, respectively. Suppose that $\beta_1, \ldots, \beta_j$ are the roots of $q_0(X)$ and $\gamma_1, \ldots, \gamma_r$ are the roots of $q_1(X)$. Then,

$$\sum_{\mathbf{x} \in \mathbb{F}_2^{n-1}} (-1)^{f_n(0,\mathbf{x})} = \sum_{\ell=1}^{j} a_\ell(n)\beta_\ell^n \text{ and } \sum_{\mathbf{x} \in \mathbb{F}_2^{n-1}} (-1)^{f_n(1,\mathbf{x})} = \sum_{s=1}^{r} b_s(n)\gamma_s^n,$$

where $a_\ell(n)$ and $b_s(n)$ are some polynomials in n. Observe that

$$\begin{aligned} S^B(f_n; p_\alpha) &= \sum_{\mathbf{x} \in \mathbb{F}_2^n} p_\alpha(\mathbf{x})(-1)^{f(\mathbf{x})} \\ &= \sum_{\mathbf{x} \in \mathbb{F}_2^{n-1}} p_\alpha(0,\mathbf{x})(-1)^{f(0,\mathbf{x})} + \sum_{\mathbf{x} \in \mathbb{F}_2^{n-1}} p_\alpha(1,\mathbf{x})(-1)^{f(1,\mathbf{x})} \\ &= \alpha^n \sum_{\mathbf{x} \in \mathbb{F}_2^{n-1}} (-1)^{f(0,\mathbf{x})} + \left(\frac{1}{2^{n-1}} - \alpha^n \right) \sum_{\mathbf{x} \in \mathbb{F}_2^{n-1}} (-1)^{f(1,\mathbf{x})} \\ &= \alpha^n \sum_{\ell=1}^{j} a_\ell(n)\beta_\ell^n + \left(\frac{1}{2^{n-1}} - \alpha^n \right) \sum_{s=1}^{r} b_\ell(n)\gamma_s^n \\ &= \sum_{\ell=1}^{j} a_\ell(n)(\alpha\beta_\ell)^n + \sum_{s=1}^{r} 2b_\ell(n) \left(\frac{\gamma_s}{2} \right)^n - \sum_{s=1}^{r} b_\ell(n)(\alpha\gamma_s)^n. \end{aligned}$$

That implies that $\{S^B(f_n; p_\alpha)\}$ satisfies linear recurrences with constant coefficients, that is, it is a C-finite sequence. In the particular case when $\deg(a_s) = \deg(b_t) = 0$ for all s, t, i.e., when $q_0(X)$ and $q_1(X)$ do not have repeated roots, $\{S^B(f_n; p_\alpha)\}$ satisfies the recurrence whose characteristic polynomial is given by

$$\operatorname{lcm}\left(\mu_{\alpha\beta_1}(X), \ldots, \mu_{\alpha\beta_j}(X), \mu_{\alpha\gamma_1}(X), \ldots, \mu_{\alpha\gamma_r}(X), \mu_{\frac{\gamma_1}{2}}(X), \ldots, \mu_{\frac{\gamma_r}{2}}(X) \right),$$

where $\mu_\omega(X)$ represents the minimal polynomial of the algebraic number ω.

Several known families of Boolean functions satisfy the above argument. That includes symmetric Boolean functions, trapezoid Boolean functions, rotation symmetric Boolean functions and linear combinations and concatenations of them (degree fixed). Moreover, in the case of those families, the argument can be extended to perturbations without too much effort. Suppose that $f_n \in \mathcal{B}_n$ is either symmetric, trapezoid, rotation symmetric or a linear combination or concatenation of symmetric and rotation symmetric Boolean functions. Let $j < n$ be a fixed positive integer and $F \in \mathcal{B}_j$. The function $f_n(\mathbf{X}) \oplus F(\mathbf{X})$ is called a perturbation of f_n. If $\{S^B(f_n; p)\}$ satisfies the

above discussion, then, using the same technique presented in [8], so does $\{S^B(f_n \oplus F; p)\}$. This, in turns, implies that the same argument holds true if we replace $S^B(f_n; p)$ by the biased Walsh transform $W^B_{f_n}(\boldsymbol{a}; p)$ (same conditions on $\boldsymbol{a}$ as in [12]).

Observe that the argument can be extended further if the probability depends on more than one entry. For instance, if $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ are algebraic numbers such that

$$\alpha_1^n,\ \alpha_2^n,\ \alpha_3^n,\ \frac{1}{2^{n-2}} - \alpha_1^n - \alpha_2^n - \alpha_3^n \in (0,1),$$

for all positive integer n, and define, for $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, the probability distribution

$$p(\mathbf{x}) = \begin{cases} \alpha_1^n, & x_1 = 0, x_2 = 0 \\ \alpha_2^n, & x_1 = 0, x_2 = 1 \\ \alpha_3^n, & x_1 = 1, x_2 = 0 \\ \frac{1}{2^{n-2}} - \alpha_1^n - \alpha_2^n - \alpha_3^n, & x_1 = 1, x_2 = 1, \end{cases}$$

then the same argument follows by requiring the corresponding four partial sums to be linear recurrent. Having said that, for simplicity, we summarize the discussion when the probability depends on only one entry.

Theorem 2.1. *Suppose that $f_n \in \mathcal{B}_n$ is one of the following*

1. $\boldsymbol{e}_{n,[k_1,\ldots,k_s]}$ *(k_i fixed)*
2. $T_{n,[j_1,\ldots,j_s]}$ *(j_i fixed)*
3. $R_{n,[j_1,\ldots,j_s]}$ *(j_i fixed)*
4. *a linear combination or concatenation of the previous three.*

Suppose that $\boldsymbol{a} \in \mathbb{F}_2^j$ is fixed and that $p_\alpha(\mathbf{x})$ is defined as in (2.1). Then $\{W^B_{f_n}(\boldsymbol{a}; p_\alpha)\}$ satisfies a linear recurrence with constant coefficients.

Example 2.2. Consider the elementary symmetric Boolean polynomial $\boldsymbol{e}_{n,3}$ and the rotation symmetric Boolean polynomial

$$R_{n,[2,3]} = X_1X_2X_3 \oplus X_2X_3X_4 \oplus \cdots \oplus X_{n-2}X_{n-1}X_n \oplus X_{n-1}X_nX_1 \oplus X_nX_1X_2.$$

Let $f_n(Y, X_1, \ldots, X_n) \in \mathcal{B}_{n+1}$ be the concatenation of $R_{n,[2,3]}$ and $\boldsymbol{e}_{n,3}$, i.e

$$f_n(Y, \mathbf{X}) = (1 \oplus Y)R_{n,[2,3]}(\mathbf{X}) \oplus Y\boldsymbol{e}_{n,3}(\mathbf{X}).$$

If $\mathbf{x} = (x_1, \ldots, x_\ell) \in \mathbb{F}_2^\ell$, then let

$$p(\mathbf{x}) = \begin{cases} \left(\frac{1}{\sqrt{5}}\right)^\ell, & x_1 = 0 \\ \frac{1}{2^{\ell-1}} - \left(\frac{1}{\sqrt{5}}\right)^\ell, & x_1 = 1. \end{cases}$$

Consider the sequence $\left\{W^B_{f_n}(\mathbf{0}; p)\right\} = \left\{S^B(f_n; p)\right\}$. Observe that

$$\left\{\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f_n(0,\mathbf{x})}\right\} = \left\{\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{R_{n,[2,3]}(\mathbf{x})}\right\}. \tag{2.2}$$

We know that the right-hand side of (2.2) satisfies the homogeneous linear recurrence whose characteristic polynomial is given $X^3 - 2X - 2$ (see [10, 13]). Also

$$\left\{\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f_n(1,\mathbf{x})}\right\} = \left\{\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\boldsymbol{e}_{n,3}(\mathbf{x})}\right\}, \tag{2.3}$$

and again, we know that the right-hand side satisfies a homogeneous linear recurrence, i.e., the one whose characteristic polynomial is given by $(X-2)(X^2-2X-2)$ (see [7]). Therefore, $\{S^B(f_n;p)\}$ satisfies a linear recurrence with integer coefficients.

If we want to calculate an explicit recurrence, then we must study the roots of the polynomials associated to (2.2) and (2.3). The polynomial X^3-2X-2, which is associated to (2.2), is irreducible over $\mathbb{Q}$, and let β represents one of its roots. The roots of $(X-2)(X^2-2X-2)$ are $2, 1\pm i$. Thus, we must find the minimal polynomials of

$$\frac{\beta}{\sqrt{5}},\ \frac{2}{\sqrt{5}},\ \frac{1\pm i}{\sqrt{5}},\ 1,\ \frac{1\pm i}{2}.$$

These polynomials are given by

$$\begin{aligned}
\mu_{\frac{\beta}{\sqrt{5}}}(X) &= 125X^6-100X^4+20X^2-4,\\
\mu_{\frac{2}{\sqrt{5}}}(X) &= 5X^2-4,\\
\mu_{\frac{1\pm i}{\sqrt{5}}}(X) &= 25X^4+4,\\
\mu_1(X) &= X-1,\\
\mu_{\frac{1\pm i}{2}}(X) &= 2X^2-2X+1,
\end{aligned}$$

and the least common multiple of them is their product, i.e.

$$\begin{aligned}
Q(X) &= (X-1)\left(2X^2-2X+1\right)\left(5X^2-4\right)\\
&\quad\times\left(25X^4+4\right)\left(125X^6-100X^4+20X^2-4\right).
\end{aligned}$$

This implies that $\{S^B(f_n;p)\}$ satisfies that linear recurrence whose characteristic polynomial is Q, in other words, $Q(E)(S^B(f_n;p))=0$, where E represents the shift operator, i.e., $E(a_n)=a_{n+1}$.

There are other cases on which biased exponential sums of symmetric and rotation symmetric Boolean functions are C-finite. A similar behavior is exhibit by symmetric Boolean functions when the probability distribution depends on the weight of $\mathbf{x}\in\mathbb{F}_2^n$.

Suppose that $\alpha\in\mathbb{R}$ is an algebraic number and $0<j<n$ be such that

$$\alpha^n,\ \ \frac{1-\alpha^n\binom{n}{j}}{2^n-\binom{n}{j}}\in(0,1)$$

for all $n\geq 1$. Define, for $\mathbf{x}\in\mathbb{F}_2^n$, the probability distribution

$$p_\alpha^{(j)}(\mathbf{x})=\begin{cases}\alpha^n, & wt(\mathbf{x})=j,\\ \frac{1-\alpha^n\binom{n}{j}}{2^n-\binom{n}{j}}, & \text{otherwise.}\end{cases}\tag{2.4}$$

When j is fixed, the scaled biased exponential sum

$$\left\{\left(2^n-\binom{n}{j}\right)S^B\left(\boldsymbol{e}_{n,k};\,p_\alpha^{(j)}\right)\right\}$$

is C-finite. The argument for the proof of this claim is somewhat similar to the previous one. However, when the weight j is not fixed, we still get recurrences, but the coefficients are no longer constants. Instead, they are polynomials in n. In other words, the sequences are holonomic or P-recursive. We show an example of the last claim.

Let $A(n)=2^{2n}-\binom{2n}{n}$, $L_{k,\alpha}(n)=A(n)\,S^B\left(\boldsymbol{e}_{2n,k};\,p_\alpha^{(n)}\right)$ and consider the sequence $\{L_{k,\alpha}(n)\}_n$. Observe that

$$L_{k,\alpha}(n) = A(n)\sum_{\mathbf{x}\in\mathbb{F}_2^{2n}} p_\alpha^{(n)}(\mathbf{x})(-1)^{\boldsymbol{e}_{2n,k}(\mathbf{x})}$$

$$\begin{aligned} &= \alpha^{2n} A(n) \sum_{wt(\mathbf{x})=n} (-1)^{e_{2n,k}(\mathbf{x})} + \left(\frac{1-\alpha^{2n}\binom{2n}{n}}{2^{2n}-\binom{2n}{n}} \right) A(n) \sum_{wt(\mathbf{x})\neq n} (-1)^{e_{2n,k}(\mathbf{x})} \\ &= (-1)^{\binom{n}{k}} \alpha^{2n} A(n) \binom{2n}{n} + \left(1-\alpha^{2n}\binom{2n}{n}\right) \sum_{\ell=0,\ell\neq n}^{2n} (-1)^{\binom{\ell}{k}} \binom{2n}{\ell}. \end{aligned}$$

Since $(-1)^{\binom{n}{k}}$ and α^{2n} are C-finite and $A(n)$ and $\binom{2n}{n}$ are P-recursive, the terms

$$(-1)^{\binom{n}{k}} \alpha^{2n} A(n) \binom{2n}{n} \quad \text{and} \quad 1-\alpha^{2n}\binom{2n}{n}$$

are P-recursive. On the other hand,

$$\sum_{\ell=0,\ell\neq n}^{2n} (-1)^{\binom{j}{k}} \binom{2n}{j} = \sum_{\ell=0}^{2n} (-1)^{\binom{j}{k}} \binom{2n}{j} - (-1)^{\binom{n}{k}} \binom{2n}{n}. \tag{2.5}$$

The first term on the right-hand side of (2.5) is C-finite and we already know that the second term is P-recursive. Since the sum and product of P-recursive sequences is P-recursive, $\{L_{k,c,\alpha}(n)\}$ is P-recursive. An explicit formula for its recursion can be obtained using Zeilberger's Algorithm [32].

There are other instances for which we obtain P-recursive sequences, but the argument is similar to the one presented. Of course, for general probability distributions, we might not get recursions. In the next section we show that something similar happens for some restricted domains.

3. Recurrences over restricted domain

Boolean functions over restricted domains have been a subject of study recently. In particular, some cryptographic applications have been found over the restricted domain $E_{n,j} = \{\mathbf{x} \in \mathbb{F}_2^n : wt(\mathbf{x}) = j\}$, see [6, 22, 25]. When $E = E_{n,j}$, we relabel the restricted exponential sum and the restricted Walsh transform as $S^{(j)}(f)$ and $W_f^{(j)}(\boldsymbol{a})$, respectively.

The study of symmetric Boolean functions over the restricted domain $E_{n,j}$ is rather simple. In that case, the scaled restricted exponential sum is given by

$$S^{(j)}(\boldsymbol{e}_{n,k}) = (-1)^{\binom{j}{k}} \binom{n}{j}.$$

Thus, it is given by a polynomial in n of degree j and so it satisfies the linear recurrence whose characteristic polynomial is given by

$$(X-1)^{j+1}.$$

In this section we will show that a similar behavior is exhibited by $R_{n,[2,3,\ldots,k]} \in \mathcal{B}_n$, that is, $S^{(j)}(R_{n,[2,3,\ldots,k]})$, for $n \geq j+k$, is given by a polynomial in n variables of degree j.

We start with trapezoid functions, which were introduced in [10]. Recall that if $j_1 < \cdots < j_s$ are positive integers, then the trapezoid function is defined by

$$T_{n,[j_1,\ldots,j_s]} = X_1 X_{j_1} \cdots X_{j_s} \oplus X_2 X_{j_1+1} \cdots X_{j_s+1} \oplus \cdots \oplus X_{n+1-j_s} X_{j_1+n-j_s} \cdots X_{j_{s-1}+n-j_s} X_n.$$

Consider the restricted exponential sum $S^{(j)}(T_{n,[2,\ldots,k]})$. Assign first the value 0 and then the value 1 to X_n. Doing that produces

$$S^{(j)}(T_{n,[2,\ldots,k]}) = S^{(j)}(T_{n-1,[2,\ldots,k]}) + S^{(j-1)}(T_{n-1,[2,\ldots,k]} \oplus X_{n-k+1} \cdots X_{n-1}).$$

The process of assigning values to a variable X_j was referred [10] as turning the variable *OFF* and *ON*. Now turn *OFF* and *ON* the variable X_{n-1} to get

$$\begin{aligned} &S^{(j-1)}(T_{n-1,[2,\ldots,k]} \oplus X_{n-k+1} \cdots X_{n-1}) \\ =&S^{(j-1)}(T_{n-2,[2,\ldots,k]}) + S^{(j-2)}(T_{n-2,[2,\ldots,k]} \oplus X_{n-k+1} \cdots X_{n-2} \oplus X_{n-k} \cdots X_{n-2}). \end{aligned}$$

Continuing with this process (as in [10]) we get

$$\begin{aligned} S^{(j)}(T_{n,[2,\ldots,k]}) &= S^{(j)}\left(T_{k+1,[2,\ldots,k]}\right) \\ &+ \sum_{\ell=2}^{n-2k+3}\sum_{s=1}^{k-2} S^{(j-s)}\left(T_{n+1-s-\ell,[2,\ldots,k]}\right) \\ &+ \sum_{\ell=0}^{j-2k+1}(-1)^{\ell}\sum_{s=k}^{n-k-\ell} S^{(j-k+1-\ell)}\left(T_{n-s-\ell,[2,\ldots,k]}\right). \end{aligned} \tag{3.1}$$

Equation (3.1) holds for $S^{(j)}(T_{n,[2,\ldots,k]} \oplus F(\mathbf{X}))$ when $F(\mathbf{X})$ is a Boolean polynomial in the first $r < k$ variables. With this information at hand, we are ready to prove the next series of results. These results use the *restricted support* of a Boolean function, which is defined as

$$\operatorname{supp}_{n,j}(f) = \{\mathbf{x} \in E_{n,j} : f(\mathbf{x}) = 1\}.$$

It is not hard to see that, if f_1 and f_2 are Boolean functions, then the principle of inclusion and exclusion leads to

$$\left|\operatorname{supp}_{n,j}(f_1 \oplus f_2)\right| = \left|\operatorname{supp}_{n,j}(f_1)\right| + \left|\operatorname{supp}_{n,j}(f_2)\right| - 2\left|\operatorname{supp}_{n,j}(f_1) \cap \operatorname{supp}_{n,j}(f_2)\right|.$$

Lemma 3.1. *Let n, j and r be positive integers. Suppose that $n \geq j \geq r$ and let $f \in \mathcal{B}_r$ be a polynomial. Then, $\left|\operatorname{supp}_{n,j}(f)\right|$ is given by a polynomial in n of degree at most j.*

Proof. We will prove the result for f of the form $X_{i_1}\cdots X_{i_s} \oplus X_{h_1}\cdots X_{h_\ell}$, where

$$\{i_1, \ldots, i_s\} \cup \{h_1, \ldots, h_\ell\} = \{1, 2, \ldots, r\}.$$

The general case follows a similar argument.

Let $f_1 = X_{i_1}\cdots X_{i_s}$ and $f_2 = X_{h_1}\cdots X_{h_\ell}$, so that $f = f_1 \oplus f_2$ and

$$\left|\operatorname{supp}_{n,j}(f)\right| = \left|\operatorname{supp}_{n,j}(f_1)\right| + \left|\operatorname{supp}_{n,j}(f_2)\right| - 2\left|\operatorname{supp}_{n,j}(f_1) \cap \operatorname{supp}_{n,j}(f_2)\right|. \tag{3.2}$$

Observe that f_1 returns 1 if and only if the value of each of the variables $X_{i_1}, \ldots, X_{i_s}$ is 1. Therefore, if $\mathbf{x} \in E_{n,j}$, then $f_1(\mathbf{x}) = 1$ if and only if the entries of $\mathbf{x}$ at the $i_1, \ldots, i_s$ positions are 1. That means that the other $n - s$ entries of $\mathbf{x}$ are free and we need to position $j - s$ ones on them. Therefore,

$$\left|\operatorname{supp}_{n,j}(f_1)\right| = \binom{n-s}{j-s}. \tag{3.3}$$

Similarly,

$$\left|\operatorname{supp}_{n,j}(f_2)\right| = \binom{n-\ell}{j-\ell}. \tag{3.4}$$

Finally, $\mathbf{x} \in E_{n,j}$ is in $\operatorname{supp}_{n,j}(f_1) \cap \operatorname{supp}_{n,j}(f_2)$ if and only if its first r entries are 1. Therefore,

$$\left|\operatorname{supp}_{n,j}(f_1) \cap \operatorname{supp}_{n,j}(f_2)\right| = \binom{n-r}{j-r}. \tag{3.5}$$

Together, equations (3.2), (3.3), (3.4) and (3.5) imply

$$\left|\operatorname{supp}_{n,j}(f)\right| = \binom{n-s}{j-s} + \binom{n-s}{j-\ell} - 2\binom{n-r}{j-r},$$

which is a polynomial in n of degree at most j. The general case follows similarly. □

Lemma 3.2. *Let $k \geq r$ be fixed integers and n be any integer such that $n \geq 2k-1$. Suppose that $F(\mathbf{X})$ is a Boolean polynomial in the first r variables of $T_{n;[2,3,\ldots,k]}$. Then,*

$$\left|\operatorname{supp}_{n,k}(T_{n,[2,3,\ldots,k]}) \cap \operatorname{supp}_{n,k}(F)\right|$$

is constant.

Proof. Recall that

$$T_{n,[2,\ldots,k]} = X_1X_2\cdots X_k \oplus X_2X_3\cdots X_{k+1} \oplus \cdots \oplus X_{n-k+1}X_{n-k+2}\cdots X_n.$$

Therefore, if $\mathbf{u}$ has weight k, then $T_{n,[2,\ldots,k]}(\mathbf{u}) = 1$ if an only if exactly one of its terms is 1. Thus, it is clear that if

$$\mathbf{u}_\ell^{(n)} = (\underbrace{0,\cdots,0}_{\ell-1},\underbrace{1,\cdots,1}_{k},\underbrace{0,\cdots,0}_{n-k-\ell+1}),\ \ 1 \leq \ell \leq n-k+1,$$

then

$$\operatorname{supp}_{n,k}(T_{n,[2,3,\ldots,k]}) = \left\{\mathbf{u}_1^{(n)}, \mathbf{u}_2^{(n)}, \ldots, \mathbf{u}_{n-k+1}^{(n)}\right\}.$$

By assumption, the polynomial $F(\mathbf{X})$ is formed by adding terms of the form $X_{i_1}\cdots X_{i_t}$ with $i_1 < \cdots < i_t \leq r$ (remember that $r \leq k$). Let us study

$$\operatorname{supp}_{n,k}(T_{n,[2,3,\ldots,k]}) \cap \operatorname{supp}_{n,k}(X_{i_1}\cdots X_{i_t}).$$

Observe that $X_{i_1}\cdots X_{i_t}$ returns 1 at $\mathbf{u}_\ell^{(n)}$ if and only if the entries of $\mathbf{u}_\ell^{(n)}$ at positions $i_1,\ldots,i_t$ are all 1. By hypothesis on n, only on the vectors $\mathbf{u}_1^{(n)}, \mathbf{u}_2^{(n)}, \ldots, \mathbf{u}_{i_s}^{(n)}$ the number 1 appears as the entry at position i_s. Therefore,

$$\left|\operatorname{supp}_{n,k}(T_{n,[2,3,\ldots,k]}) \cap \operatorname{supp}_{n,k}(X_{i_1}\cdots X_{i_t})\right| = i_1,$$

and so $\left|\operatorname{supp}_{n,k}(T_{n,[2,3,\ldots,k]}) \cap \operatorname{supp}_{n,k}(X_{i_1}\cdots X_{i_t})\right|$ is constant. The general case follows by applying the principle of inclusion and exclusion. □

Lemma 3.3. *Let $1 < k \leq j$ be integers. Suppose that $F(\mathbf{X})$ is a Boolean polynomial in the first $r < k$ variables of $T_{n;[2,3,\ldots,k]}$. Suppose that $n > k+j-1$. Then $S^{(j)}(T_{n,[2,3,\ldots,k]} \oplus F(\mathbf{X}))$ is given by a polynomial in n of degree at most j. In particular $\{S^{(j)}(T_{n,[2,3,\ldots,k]} \oplus F(\mathbf{X}))\}_{n \geq k+j}$ satisfies the homogeneous linear recurrence whose characteristic polynomial is given by*

$$(X-1)^{j+1}.$$

Proof. The argument is by induction on j. Consider first $S^{(k)}\left(T_{n,[2,\ldots,k]} \oplus F(\mathbf{X})\right)$. Note that

$$S^{(k)}\left(T_{n,[1,2,\ldots,k]} \oplus F(\mathbf{X})\right) = \binom{n}{k} - 2\left|\operatorname{supp}_{n,k}(T_{n,[1,2,\ldots,k]} \oplus F(\mathbf{X}))\right|.$$

Recall that

$$\begin{aligned}\left|\operatorname{supp}_{n,k}(T_{n,[1,2,\ldots,k]} \oplus F(\mathbf{X}))\right| &= \left|\operatorname{supp}_{n,k}(T_{n,[1,2,\ldots,k]})\right| + \left|\operatorname{supp}_{n,k} F(\mathbf{X}))\right| \\ &\quad - 2\left|\operatorname{supp}_{n,k}(T_{n,[1,2,\ldots,k]}) \cap \operatorname{supp}_{n,k} F(\mathbf{X}))\right|.\end{aligned} \tag{3.6}$$

We know that $\left|\operatorname{supp}_{n,k}(T_{n,[1,2,\ldots,k]} \oplus F(\mathbf{X}))\right| = n-k+1$. Lemma 3.1 implies that $\left|\operatorname{supp}_{n,k} F(\mathbf{X}))\right|$ is a polynomial in n of degree at most k and Lemma 3.2 implies that

$$\left|\operatorname{supp}_{n,k}(T_{n,[1,2,\ldots,k]}) \cap \operatorname{supp}_{n,k} F(\mathbf{X}))\right|$$

is constant. Therefore, (3.6) is a polynomial in n of degree at most k. Since $\binom{n}{k}$ is a polynomial in n of degree k, then it follows that $S^{(k)}(T_{n,[1,2,\ldots,k]} \oplus F(\mathbf{X}))$ is a polynomial in n of degree at most k.

Suppose that for an arbitrary j we have that $S^{(i)}(T_{n,[2,\ldots,k]} \oplus F(\mathbf{X}))$ is given by a polynomial on n of degree at most i for every $k \leq i \leq j-1$. Then, by (3.1), $S^{(j)}(T_{n,[2,\ldots,k]} \oplus F(X))$ is given by a polynomial in n variables of degree at most

$$\begin{aligned}&\deg\left(\sum_{l=2}^{n-2k+3}\sum_{s=1}^{k-2} S^{(j-s)}(T_{n+1-s-l,[2,\ldots,k]} \oplus F(\mathbf{X}))\right) \\ &= 1 + \deg\left(\sum_{s=1}^{k-2} S^{(j-s)}(T_{n+1-s-l,[2,\ldots,k]} \oplus F(\mathbf{X}))\right) \leq 1 + (j-1) = j.\end{aligned}$$

This concludes the proof. □

Consider now the rotation symmetric monomial $R_{n,[2\ldots,k]}$. Using the method of turning variables *OFF* and *ON* yields

$$S^{(j)}(R_{n,[2,3,\ldots,k]}) = S^{(j)}(T_{n-1,[2,3,\ldots,k]}) + \sum_{i=1}^{k-2} S^{(j-i)}\left(T_{n-1-i,[2,3,\ldots,k]} \oplus \sum_{l=1}^{i}\prod_{s=1}^{k-l} X_s\right) + \sum_{i=0}^{j-2k+1} (-1)^i S^{(j-k+1-i)}\left(T_{n-k-i,[2,3,\cdots,k]} \oplus F(\mathbf{X})\right), \tag{3.7}$$

where $F(\mathbf{X}) = X_1 \oplus X_1X_2 \oplus X_1X_2\cdots X_{k-1}$. Putting together Lemma 3.3 and Equation (3.7), we have the following result.

Theorem 3.4. *Let j and k be fixed positive integers. Then $S^{(j)}(R_{n,[2,3,\ldots,k]})$, for $n \geq j+k$, is given by a polynomial in n of degree j. In particular, the sequence $\left\{S^{(j)}\left(R_{n,[2,3,\ldots,k]}\right)\right\}_{n\geq j+k}$ is C-finite and satisfies the homogeneous linear recurrence whose characteristic polynomial is given by*

$$(X-1)^{j+1}.$$

Corollary 3.5. *Let j and k be fixed positive integers. Suppose that $F(\mathbf{X})$ is a polynomial in the first $r < k$ variables of $R_{n,[2,3,\ldots,k]}$. Then $S^{(j)}(R_{n,[2,3,\ldots,k]} + F(\mathbf{X}))$, for $n \geq j+k-1$, is given by a polynomial in n of degree j. In particular, the sequence $\left\{S^{(j)}\left(R_{n,[2,3,\ldots,k]} + F(\mathbf{X})\right)\right\}_{n\geq j+k}$ is C-finite and satisfies the homogeneous linear recurrence whose characteristic polynomial is given by*

$$(X-1)^{j+1}.$$

Example 3.6. Consider the rotation symmetric $R_{n;[2,3,4]}$. According to Theorem 3.4, $S^{(6)}(R_{n;[2,3,4]})$ is given by a polynomial of degree at most 6 (for $n \geq 4+6-1 = 9$). In other words, $S^{(6)}(R_{n;[2,3,4]}) = f(n)$ with

$$f(n) = a_0 + a_1n + a_2n^2 + a_3n^3 + a_4n^4 + a_5n^5 + a_6n^6.$$

Solving the system

$$\begin{aligned} f(9) &= S^{(6)}(R_{9;[2,3,4]}) = 12 \\ f(10) &= S^{(6)}(R_{10;[2,3,4]}) = 70 \\ f(11) &= S^{(6)}(R_{11;[2,3,4]}) = 220 \\ f(12) &= S^{(6)}(R_{12;[2,3,4]}) = 540 \\ f(13) &= S^{(6)}(R_{13;[2,3,4]}) = 1144 \\ f(14) &= S^{(6)}(R_{14;[2,3,4]}) = 2191 \\ f(15) &= S^{(6)}(R_{15;[2,3,4]}) = 3895, \end{aligned}$$

we find that

$$S^{(6)}(R_{n;[2,3,4]}) = \frac{n^6}{720} - \frac{n^5}{48} + \frac{17n^4}{144} - \frac{21n^3}{16} + \frac{4817n^2}{360} - \frac{265n}{6}.$$

A similar behavior is exhibit by $S^{(6)}(R_{n;[2,3,4]} + X_1X_2 + X_2X_3)$, according to Corollary 3.5. In this case,

$$S^{(6)}(R_{n;[2,3,4]} + X_1X_2 + X_2X_3) = \frac{n^6}{720} - \frac{n^5}{48} + \frac{5n^4}{144} - \frac{7n^3}{48} + \frac{4847n^2}{360} - \frac{316n}{3} + 234.$$

Observe that Corollary 3.5 implies that $W^{(j)}_{R_{n;[2,\ldots,k]}}(\boldsymbol{a})$, for $n \geq k+j-1$ and $\boldsymbol{a} \in \mathbb{F}_2^r$ with $r < k$, is also given by a polynomial in n of degree at most j. We will not state that result as a theorem, as it is included in Corollary 3.5. Also, some adjustments to the argument can be used to prove that we have the same behavior for other rotation symmetric Boolean functions. For example,

$$W^{(7)}_{R_{n;[2,3,5]}}(\boldsymbol{a}) = \frac{n^7}{5040} - \frac{7n^6}{720} + \frac{133n^5}{720} - \frac{305n^4}{144} + \frac{4063n^3}{180} - \frac{35527n^2}{180} + \frac{30406n}{35} - 1116,$$

where $\boldsymbol{a} = (1,0,1)$ and $n \geq 11$.

In the next section we study the asymptotic behavior of biased exponential sums of symmetric Boolean functions. We show that their behavior almost surely the same as the regular exponential sum.

4. Asymptotic behavior for symmetric Boolean functions

In this section we study the asymptotic behavior of symmetric Boolean functions under biased exponential sums. It turns out that this behavior is related to the behavior of the regular exponential sum of symmetric Boolean functions. In [7], it is showed that

$$\lim_{n\to\infty} \frac{1}{2^n} S(\boldsymbol{e}_{n,k}) = c_0(k) \tag{4.1}$$

where $c_0(k)$ is defined as (see [3])

$$c_0(k) = \frac{1}{2^r} \sum_{j=0}^{2^r-1} (-1)^{\binom{j}{k}}, \tag{4.2}$$

where $r = \lfloor \log_2(k) \rfloor + 1$. The constant $c_0(k)$ also appears in the behavior of symmetric Boolean functions under biased exponential sums.

We start with the behavior of $S^B(\boldsymbol{e}_{n,k}; p)$ when $p(\mathbf{x})$ is defined by (2.4). Observe that the conditions on (2.4) imply that $\alpha \leq 1/2$. Consider the case of $S^B(\boldsymbol{e}_{2n,k}; p)$, which is one of the cases when j is not fixed (the case when j is fixed follows in a similar manner). Observe that

$$\begin{aligned}
S^B(\boldsymbol{e}_{2n,k}; p) &= \sum_{wt(\mathbf{x})=n} p(\mathbf{x})(-1)^{\boldsymbol{e}_{2n,k}(\mathbf{x})} + \sum_{wt(\mathbf{x})\neq n} p(\mathbf{x})(-1)^{\boldsymbol{e}_{2n,k}(\mathbf{x})} \\
&= c\alpha^{2n}(-1)^{\binom{n}{k}}\binom{2n}{n} + \left(\frac{1-\binom{2n}{n}c\alpha^{2n}}{2^{2n}-\binom{2n}{n}}\right) \sum_{j=0, j\neq n}^{2n} (-1)^{\binom{j}{k}}\binom{2n}{j} \\
&= c\alpha^{2n}(-1)^{\binom{n}{k}}\binom{2n}{n} + \left(\frac{1-\binom{2n}{n}c\alpha^{2n}}{2^{2n}-\binom{2n}{n}}\right) \left(\sum_{j=0}^{2n} (-1)^{\binom{j}{k}}\binom{2n}{j} - (-1)^{\binom{n}{k}}\binom{2n}{n}\right).
\end{aligned}$$

The well-known inequality

$$\frac{4^n}{\sqrt{4n}} \leq \binom{2n}{n} \leq \frac{4^n}{\sqrt{3n+1}},$$

implies

$$\lim_{n\to\infty} c\alpha^{2n}(-1)^{\binom{n}{k}}\binom{2n}{n} = 0.$$

Also,

$$\lim_{n\to\infty} \left(\frac{1-\binom{2n}{n}c\alpha^{2n}}{2^{2n}-\binom{2n}{n}}\right) \left(\sum_{j=0}^{2n} (-1)^{\binom{j}{k}}\binom{2n}{j} - (-1)^{\binom{n}{k}}\binom{2n}{n}\right)$$

$$
\begin{aligned}
&= \lim_{n\to\infty} \left(\frac{1 - \binom{2n}{n} c\alpha^{2n}}{2^{2n} - \binom{2n}{n}} \right) \sum_{j=0}^{2n} (-1)^{\binom{j}{k}} \binom{2n}{j} \\
&= \lim_{n\to\infty} \left(\frac{1 - \binom{2n}{n} c\alpha^{2n}}{2^{2n}(1 - \frac{1}{2^{2n}}\binom{2n}{n})} \right) \sum_{j=0}^{2n} (-1)^{\binom{j}{k}} \binom{2n}{j} \\
&= \lim_{n\to\infty} \frac{1}{2^{2n}} \sum_{j=0}^{2n} (-1)^{\binom{j}{k}} \binom{2n}{j} \\
&= c_0(k).
\end{aligned}
$$

The same holds true if $p(\mathbf{x})$ is defined as in (2.1), that is,

$$\lim_{n\to\infty} S^B(\boldsymbol{e}_{n,k}; p) = c_0(k).$$

In other words, in both cases, the behavior of the elementary symmetric Boolean polynomial $\boldsymbol{e}_{n,k}$ under the biased exponential sum is dominated by $c_0(k)$. Furthermore, in both cases, the elementary symmetric Boolean polynomial $\boldsymbol{e}_{n,k}$ is asymptotically not balanced if and only if k is a power of two. That is, if k is not a power of two, then $\boldsymbol{e}_{n,k}$ can only be "sporadically balanced" under the probability distributions considered so far. That is the same behavior when the domain is not biased.

This behavior might be a bit surprising. However, the next theorem reveals that it is somewhat expected. That is, if you choose uniformly at random a probability distribution, then almost surely the biased exponential sums of $\boldsymbol{e}_{n,k}$ converges to $c_0(k)$ as n increases.

Theorem 4.1. *For each positive integer n, suppose that $a_j^{(n)}$, $j = 0, 1, \ldots, n$, were chosen uniformly at random from the set of nonnegative real numbers such that*

$$\sum_{j=0}^{n} a_j^{(n)} \binom{n}{j} = 1. \tag{4.3}$$

For $\mathbf{x} \in \mathbb{F}_2^n$, let the probability distribution be given by $p^{(n)}(\mathbf{x}) = a_j^{(n)}$, when $wt(\mathbf{x}) = j$. Then, almost surely

$$S^B(\boldsymbol{e}_{n,k}; p^{(n)}) \to c_0(k), \text{ as } n \to \infty.$$

Proof. Observe that

$$S^B(\boldsymbol{e}_{n,k}; p^{(n)}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} p^{(n)}(\mathbf{x})(-1)^{\boldsymbol{e}_{n,k}(\mathbf{x})} = \sum_{j=0}^{n} a_j^{(n)} (-1)^{\binom{j}{k}} \binom{n}{j}.$$

Let $r = \lfloor \log_2(k) \rfloor + 1$. Recall that by Lucas' Theorem,

$$\binom{j + m \cdot 2^r}{k} \equiv \binom{j}{k} \pmod 2,$$

for every natural number m. Let $j_1, \ldots, j_s$ be all integers between 1 and $2^r - 1$ such that $\binom{j}{k}$ is odd. Then,

$$
\begin{aligned}
S^B(\boldsymbol{e}_{n,k}; p^{(n)}) &= \sum_{j=0}^{n} a_j^{(n)} \binom{n}{j} - 2 \sum_{\ell=1}^{s} \sum_{t \equiv j_\ell \bmod 2^r} a_t^{(n)} \binom{n}{t} \\
&= 1 - 2 \sum_{\ell=1}^{s} \sum_{m\geq 0} a_{j_\ell + m\cdot 2^r}^{(n)} \binom{n}{j_\ell + m \cdot 2^r}.
\end{aligned}
$$

Since $a_j^{(n)}$ were chosen uniformly at random such that (4.3) holds, then by the Law of Large Numbers

$$\sum_{m\geq 0} a_{j_\ell+m\cdot 2^r}^{(n)} \binom{n}{j_\ell+m\cdot 2^r} \sim \frac{1}{2^r}\sum_{j=0}^{n} a_j^{(n)}\binom{n}{j} \to \frac{1}{2^r},$$

as n grows. This implies that

$$\begin{aligned} S^B(\boldsymbol{e}_{n,k};p^{(n)}) &= 1-2\sum_{\ell=1}^{s}\sum_{m\geq 0} a_{j_\ell+m\cdot 2^r}^{(n)}\binom{n}{j_\ell+m\cdot 2^r} \\ &\to 1-2\sum_{\ell=1}^{s}\frac{1}{2^r} = 1-s\cdot 2^{1-r} \\ &= c_0(k) \end{aligned}$$

as n grows. This concludes the proof. □

The previous theorem tells us that if we chose a probability distribution p on the elements of $\mathbb{F}_2^n$ randomly, then almost surely

$$S^B(\boldsymbol{e}_{n,k};p) \sim c_0(k). \tag{4.4}$$

This, of course, does not mean that (4.4) holds for every probability distribution. We can design a probability distribution that specifically targets the behavior of $\boldsymbol{e}_{n,k}$.

Example 4.2. Recall that $\boldsymbol{e}_{n,2^r-1}(\mathbf{x}) = 1$ if and only if $wt(\mathbf{x}) \equiv 2^r-1 \pmod{2^r}$. We can use this information to design a probability distribution p such that

$$S^B(\boldsymbol{e}_{n,2^r-1};p) \not\sim c_0(2^r-1) = \frac{2^{r-1}-1}{2^{r-1}}.$$

Suppose that α is a nonnegative real number. Let $\mathbf{x}\in\mathbb{F}_2^n$ and define

$$p(\mathbf{x}) = \begin{cases} \dfrac{\alpha}{\alpha\lceil (n+1)/2\rceil + \lceil n/2\rceil + 1}\binom{n}{wt(\mathbf{x})}^{-1}, & wt(\mathbf{x})\equiv 0 \pmod 2 \\ \dfrac{1}{\alpha\lceil (n+1)/2\rceil + \lceil n/2\rceil + 1}\binom{n}{wt(\mathbf{x})}^{-1}, & wt(\mathbf{x})\equiv 1 \pmod 2. \end{cases} \tag{4.5}$$

Choose $j\in\{0,1,\ldots,n\}$. There are $\binom{n}{j}$ vectors $\mathbf{x}\in\mathbb{F}_2^n$ such that $wt(\mathbf{x})=j$. Also, there are $\lceil (n+1)/2\rceil$ integers $j\in\{0,1,\ldots,n\}$ that are congruent to 0 (mod 2) and $\lceil n/2\rceil$ that are congruent to 1 (mod 2). Therefore, (4.5) is a well-defined probability distribution on $\mathbb{F}_2^n$. Observe that this distribution is designed in such a way that there is a different scale factor on the probability when $wt(\mathbf{x})$ is even and we know that every $\mathbf{x}\in\mathbb{F}_2^n$ such that $\boldsymbol{e}_{n,2^r-1}(\mathbf{x})=1$ lies in the case when $wt(\mathbf{x})$ is odd.

Observe that

$$\begin{aligned} S^B(\boldsymbol{e}_{n,2^r-1};p) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} p(\mathbf{x})(-1)^{\boldsymbol{e}_{n,2^r-1}(\mathbf{x})} \\ &= \sum_{wt(\mathbf{x})\equiv 0 \bmod 2} p(\mathbf{x})(-1)^{\boldsymbol{e}_{n,2^r-1}(\mathbf{x})} \\ &\quad + \sum_{wt(\mathbf{x})\not\equiv 2^r-1 \bmod 2^r;\ \text{odd}} p(\mathbf{x})(-1)^{\boldsymbol{e}_{n,2^r-1}(\mathbf{x})} \\ &\quad + \sum_{wt(\mathbf{x})\equiv 2^r-1 \bmod 2^r} p(\mathbf{x})(-1)^{\boldsymbol{e}_{n,2^r-1}(\mathbf{x})} \end{aligned}$$

$$= \sum_{j\equiv 0 \bmod 2}^{n} \frac{\alpha}{\alpha\lceil (n+1)/2\rceil) + \lceil n/2\rceil + 1} + \sum_{j\not\equiv 2^r-1 \bmod 2^r;\ \text{odd}}^{n} \frac{1}{\alpha\lceil (n+1)/2\rceil) + \lceil n/2\rceil + 1} - \sum_{j\equiv 2^r-1 \bmod 2^r}^{n} \frac{1}{\alpha\lceil (n+1)/2\rceil) + \lceil n/2\rceil + 1}.$$

However, we know that

$$\#\{0 \le j \le n \,:\, j \equiv j_0 \pmod{2^\ell}\} = \left\lceil \frac{n-j_0+1}{2^\ell} \right\rceil,$$

where $j_0 \in \{0,1,2,\ldots,2^\ell-1\}$. Therefore,

$$\begin{aligned} S^B(\boldsymbol{e}_{n,2^r-1};p) &= \frac{\alpha}{\alpha\lceil (n+1)/2\rceil) + \lceil n/2\rceil + 1} \left\lceil \frac{n+1}{2} \right\rceil \\ &+ \frac{1}{\alpha\lceil (n+1)/2\rceil) + \lceil n/2\rceil + 1} \sum_{j=1;\ \text{odd}}^{2^r-3} \left\lceil \frac{n-j+1}{2^r} \right\rceil \\ &- \frac{1}{\alpha\lceil (n+1)/2\rceil) + \lceil n/2\rceil + 1} \left\lceil \frac{n-2^r+2}{2^r} \right\rceil. \end{aligned}$$

Since

$$\lim_{n\to\infty} \frac{1}{\alpha\lceil (n+1)/2\rceil) + \lceil n/2\rceil + 1} \left\lceil \frac{n-j+1}{2^r} \right\rceil = \frac{1}{2^{r-1}\alpha + 2^{r-1}},$$

this closed formula implies

$$\lim_{n\to\infty} S^B(\boldsymbol{e}_{n,2^r-1};p) = \frac{2^{r-2}\alpha + 2^{r-2} - 1}{2^{r-2}\alpha + 2^{r-2}}.$$

This limit is different than $c_0(2^r)$ if and only if $\alpha \neq 1$. In the particular case when $r = 2$ and $\alpha = 0$, the limit is 0 and $S^B(\boldsymbol{e}_{n,3};p) = 0$ if and only if $n \equiv 0, 3 \pmod 4$. In other words, the elementary symmetric polynomial $\boldsymbol{e}_{n,3}$ is balanced over this biased domain when $n \equiv 0, 3 \pmod 4$.

5. Concluding remarks

In this work we showed that under some conditions, biased and restricted exponential sums and Walsh transforms of symmetric and rotation symmetric polynomials are C-finite or P-recursive sequences. This is a generalization of the known results for non-biased domains. We also showed that exponential sums and Walsh transforms of some families of rotation symmetric monomials over the restricted domain $E_{n,j} = \{\mathbf{x} \in \mathbb{F}_2^n \,:\, wt(\mathbf{x}) = j\}$ ($wt(\mathbf{x})$ is the weight of the vector $\mathbf{x}$) are given by polynomials of degree at most j. Finally, we also studied the asymptotic behavior of biased exponential sums of symmetric Boolean functions and showed that their behavior is almost surely the same as the regular exponential sum. We hope and expect to see applications of our results, as well as continued progress toward covering other classes of functions, using our methods or new ones to fit the specific purpose.

Acknowledgments. The research of the second author was supported by The Puerto Rico Science, Technology and Research Trust under agreement number 2020-00124. This content is only the responsibility of the authors and does not necessarily represent the official views of The Puerto Rico Science, Technology and Research Trust. The first author was also supported as a student by the same grant.

References

[1] M. L. Bileschi, T. W. Cusick, and D. Padgett. Weights of Boolean cubic monomial rotation symmetric functions. *Cryptogr. Commun.* 4 (2012) 105–130.

[2] L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer-Verlag, 2014.

[3] J. Cai, F. Green, and T. Thierauf. On the correlation of symmetric functions. *Math. Systems Theory* 29 (1996) 245–258.

[4] A. Canteaut and M. Videau. Symmetric Boolean Functions. *IEEE Trans. Inf. Theory* 51 (2005) 2791–2811.

[5] C. Carlet, *Boolean functions for cryptography and error correcting codes*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 257–397, 2010.

[6] C. Carlet, P. Méaux, and Y. Rotella. Boolean functions with restricted input and their robustness; Application to the FLIP cipher. *IACR Trans. Symmetric Cryptol.* 3 (2017) 192–227.

[7] F. Castro and L. A. Medina. Linear Recurrences and Asymptotic Behavior of Exponential Sums of Symmetric Boolean Functions. *Elec. J. Combin.* 18 (2011), #P8.

[8] F. Castro and L. A. Medina. Asymptotic Behavior of Perturbations of Symmetric Functions. *Annals of Combin.* 18 (2014) 397–417.

[9] F. Castro and L. A. Medina. Modular periodicity of exponential sums of symmetric Boolean functions. *Discrete Appl. Math.* 217 (2017) 455–473.

[10] F. N. Castro, R. Chapman, L. A. Medina, and L. B. Sepúlveda. Recursions associated to trapezoid, symmetric and rotation symmetric functions over Galois fields. *Discrete Mathematics* 341(7) (2018) 1915–1931.

[11] F. N. Castro, L. A. Medina, and L. B. Sepúlveda. Closed formulas for exponential sums of symmetric polynomials over Galois fields. *Journal Algebraic Combinatorics* 50(1) (2019) 73-98.

[12] F. Castro, L. A. Medina, and P. Stănică. Generalized Walsh transforms of symmetric and rotation symmetric Boolean functions are linear recurrent. *Appl. Algebr. Eng. Comm.* 29(5) (2018) 433–453.

[13] T. W. Cusick. Weight recursions for any rotation symmetric Boolean functions. *IEEE Trans. Inf. Theory* 64(4) (2018) 2962–2968.

[14] T. W. Cusick and Y. Li. k-th order symmetric SAC Boolean functions and bisecting binomial coefficients. *Discrete Appl. Math.* 149 (2005) 73–86.

[15] T. W. Cusick, Y. Li, and P. Stănică. Balanced Symmetric Functions over $GF(p)$. *IEEE Trans. Inf. Theory* 5 (2008) 1304–1307.

[16] T. W. Cusick and B. Johns. Recursion orders for weights of Boolean cubic rotation symmetric functions. *Discr. Appl. Math.* 186 (2015) 1–6.

[17] T. W. Cusick and P. Stănică. Fast evaluation, weights and nonlinearity of rotation symmetric functions. *Discr. Math.* 258 (2002) 289–301.

[18] T. W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications* (Ed. 2), Academic Press, San Diego, CA, 2017.

[19] D. K. Dalai, S. Maitra, and S. Sarkar. Results on rotation symmetric bent functions. *Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA'06*, publications of the universities of Rouen and Havre (2006) 137–156.

[20] E. Filiol and C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation immunity. In: *Adv. in Cryptology – EUROCRYPT* 1998, LNCS 1403, Springer, Berlin, 1998, pp. 475–488.

[21] M. Hell, A. Maximov, and S. Maitra. On efficient implementation of search strategy for rotation symmetric Boolean functions. *Ninth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT 2004*, Black Sea Coast, Bulgaria, 2004.

[22] S. Maitra, B. Mandal, T. Martinsen, D. Roy, and P. Stănică. Analysis on Boolean Function in a Restricted (Biased) Domain. *IEEE Trans. Inf. Theory* 66(2) (2020) 1219–1231.

[23] P. Méaux, A. Journault, F.-X. Standaert, and C. Carlet. Towards stream ciphers for efficient FHE with low-noise ciphertexts. *Adv. in Cryptology – EUROCRYPT* 2016, LNCS 9665, Springer, Berlin, 2016, pp. 311–343.

[24] A. Maximov, M. Hell, and S. Maitra. Plateaued Rotation Symmetric Boolean Functions on Odd Number of Variables. *First Workshop on Boolean Functions: Cryptography and Applications, BFCA'05*, publications of the universities of Rouen and Havre (2005) 83–104.

[25] S. Mesnager, Z. Zhou, and C. Ding. On the nonlinearity of Boolean functions with restricted input. *Cryptography and Communications* (2018), 1–14.

[26] J. Pieprzyk and C.X. Qu. Fast hashing and rotation-symmetric functions. *J. Universal Comput. Sci.* 5(1) (1999) 20–31.

[27] O. S. Rothaus. On bent functions. *J. Combin. Theory Ser. A* 20 (1976) 300–305.

[28] P. Stănică and S. Maitra. Rotation Symmetric Boolean Functions – Count and Cryptographic Properties. *Discr. Appl. Math.* 156 (2008) 1567–1580.

[29] P. Stănică, S. Maitra, and J. Clark. Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions. *Fast Software Encryption, FSE* 2004, LNCS 3017, 161–177. Springer–Verlag, 2004.
[30] R. Stanley. Differentiably Finite Power Series. *European J. Combin.* 1 (1980) 175–188.
[31] D. Zeilberger. A Holonomic Systems Approach to Special Functions Identities. *J. Comput. Appl. Math.* 32(3) (1990) 321–368.
[32] D. Zeilberger. A Fast Algorithm for Proving Terminating Hypergeometric Identities. *Discrete Math.* 80 (2) (1990) 207–211.

Department of Mathematics, University of Puerto Rico, San Juan, PR 00925
Email address: axel.gomez@upr.edu

Department of Mathematics, University of Puerto Rico, San Juan, PR 00925
Email address: luis.medina17@upr.edu

Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943
Email address: pstanica@nps.edu