GENERALIZED WALSH TRANSFORMS OF SYMMETRIC AND ROTATION SYMMETRIC BOOLEAN FUNCTIONS ARE LINEAR RECURRENT

FRANCIS N. CASTRO, LUIS A. MEDINA, AND PANTELIMON STĂNICĂ

Abstract. Exponential sums of symmetric Boolean functions are linear recurrent with integer coefficients. This was first established by Cai, Green and Thierauf in the mid nineties. Consequences of this result has been used to study the asymptotic behavior of symmetric Boolean functions. Recently, Cusick extended it to rotation symmetric Boolean functions, which are functions with good cryptographic properties. In this article, we put all these results in the general context of Walsh transforms and some of its generalizations (nega-Hadamard transform, for example). Precisely, we show that Walsh transforms, for which exponential sums are just an instance, of symmetric and rotation symmetric Boolean functions satisfy linear recurrences with integer coefficients. We also provide a closed formula for the Walsh transform and nega-Hadamard transform of any symmetric Boolean functions. Moreover, using the techniques presented in this work, we show that some families of rotation symmetric Boolean functions are not bent when the number of variables is sufficiently large and provide asymptotic evidence to a conjecture of Stănică and Maitra.

1. Introduction

The Digital Revolution has brought some branches of Discrete Mathematics to center stage. One of the most notable examples is the Theory of Boolean functions. These beautiful combinatorial objects have applications to different scientific areas, like information theory, electrical engineering, game theory, cryptography and coding theory.

Memory restrictions of current technology have made the problem of efficient implementations of Boolean functions a challenging one. In general, this problem is very hard to tackle, but imposing conditions on these functions may ease the problem. For instance, the class of symmetric Boolean functions and the class of rotation symmetric Boolean functions are good candidates for efficient implementations. These two classes are part of the main focus of this article.

In many applications, especially ones related to cryptography, it is important for Boolean functions to be balanced. A *balanced Boolean function* is one for which the number of zeros and the number of ones are equal in its truth table (output table). Balancedness can be studied from the point of view of Hamming weights or from the point of view of exponential sums. The class of symmetric Boolean functions have been intensively studied in this regard [3, 5, 6, 7, 10, 11, 13]. The problem of balancedness of symmetric Boolean functions is, however, far from settled. There are open problems even for the relatively simple case of elementary symmetric functions (see [11]).

The study of exponential sums of symmetric Boolean functions led to the discovery that these sums, when viewed as integer sequences, are linear recurrent with integer coefficients. This was first established by Cai, Green and Thierauf in the mid nineties. Part of that study was continued in [5] where the recursive nature of these exponential sums was used to analyze the asymptotic behavior of them. In particular, the authors of [5] proved that a conjecture by Cusick, Li and Stănică [11] about balancedness of elementary symmetric polynomials is true asymptotically. The study presented in [5] was later extended to some perturbations of symmetric Boolean functions [6]. Also, the recursive nature of these sums was exploited in [7] to study modular properties of them.

Symmetry, however, is too special a property and may imply that implementations of symmetric Boolean functions, while efficient, may be vulnerable to attacks. Pieprzyk and Qu [20] introduced rotation symmetric Boolean functions (although, they did appear before in the work of Filiol and Fontaine [15] as *idempotents*). These functions, as mentioned before, are good candidates for efficient implementations. However, Pieprzyk

Date: July 12, 2017.

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

Key words and phrases. Walsh transform, nega-Hadamard transform, symmetric Boolean functions, rotation symmetric Boolean functions, linear recurrences.

and Qu showed that these functions are useful, among other things, in the design of fast hashing algorithms with strong cryptographic properties. The combination of efficiency and strong cryptographic properties sparked interest in them and today their study is an active area of research [1, 12, 13, 14, 16, 17, 27, 28].

Weights of rotations symmetric Boolean functions has been a subject of research [1, 12, 13, 27]. As in the symmetric case, early studies hinted the possibility that weights of rotation symmetric Boolean function satisfy linear recurrences with integer coefficients. Specifically, it was observed that weights of cubic rotation symmetric Boolean functions are linear recurrent [1, 12]. Recently, Cusick [9] showed that weights of any rotation symmetric Boolean function satisfy linear recurrences with integer coefficients.

The goal of this article is to put all these results in the more general framework of Walsh transformations and their generalizations. These transformations, for which exponential sums are just an instance, have applications to fields like statistics, modern communications systems, error-correcting codes and cryptography. Walsh transforms are particularly useful in the calculation of nonlinearity (maximum Hamming distance from the set of all affine functions) of Boolean functions – a concept very useful in cryptography. Boolean functions with the highest nonlinearity are known as *bent functions*, which only exist for even dimension. There are various ways to construct some families of bent functions, but their total number or their complete classification is not known.

This article is divided as follows. In the next section we present some preliminaries results. Most of the important results are presented in Section 3. In particular, we show that Walsh transformations of symmetric and rotation symmetric Boolean functions are linear recurrent with integer coefficients. We also provide a closed formula for the Walsh transformation of any symmetric Boolean function. These generalize all the known results about this topic for exponential sums of these functions. Moreover, using the techniques presented in this work, we show that some families of rotation symmetric Boolean functions are not bent when the number of variables is sufficiently large. We also provide asymptotic evidence to a conjecture of Stănică and Maitra [27] and show that roots of the characteristic polynomial of a linear recurrence associated to Walsh transformations of any family of Boolean functions $\{F_n\}_n$ are bounded in modulus by 2. This last result can be used to analyzed the asymptotic behavior of these families. In Section 4 we show that most of these results can be extended to the nega-Hadamard transform. In particular, we provide a closed formula for the nega-Hadamard transform of any symmetric Boolean function. Finally, in the last section, we show that most of these results can be extended further to some generalizations of Walsh transform.

2. Preliminaries

Let $\mathbb{F}_2$, $\mathbb{F}_2^n$ be the binary field, respectively, the n-dimensional vector space over $\mathbb{F}_2$. A function $F : \mathbb{F}_2^n \to \mathbb{F}_2$ is called a *Boolean function*. The set of all n variables Boolean functions will be denoted by $\mathcal{B}_n$.

A function $F \in \mathcal{B}_n$ is said to be *symmetric* if it is invariant under the action of the symmetric group S_n on $\mathbb{F}_2^n$, that is, if

$$F(\sigma(X_1, \dots, X_n)) = F(X_1, \dots, X_n)$$

for every permutation $\sigma \in S_n$. On the other hand, a function $F \in \mathcal{B}_n$ is said to be *rotation symmetric* if it is invariant under the action of the cyclic group C_n on $\mathbb{F}_2^n$. Let us explain this further. Our explanation is similar to the one presented in [27] and uses the notation from [4].

Let $X_i \in \mathbb{F}_2$ for $1 \le i \le n$. Define, for $1 \le k \le n$, the shift function

$$E_n^k(X_i) = \begin{cases} X_{i+k} & \text{if } i+k \le n, \\ X_{i+k-n} & \text{if } i+k > n. \end{cases}$$

Extend this definition to $\mathbb{F}_2^n$ by defining

$$E_n^k(X_1, X_2, \dots, X_n) = (E_n^k(X_1), E_n^k(X_2), \dots, E_n^k(X_n)).$$

The shift function E_n^k can also be extended to monomials via

$$E_n^k(X_{i_1} X_{i_2} \cdots X_{i_t}) = E_n^k(X_{i_1}) E_n^k(X_{i_2}) \cdots E_n^k(X_{i_t}).$$

A Boolean function F in n variables is a rotation symmetric Boolean function if and only if for any $(X_1 \cdots, X_n) \in \mathbb{F}_2^n$,

$$F(E_n^k(X_1, \dots, X_n)) = F(X_1, \dots, X_n),$$

for every $1 \le k \le n$.

Rotation symmetric Boolean functions (by this name) were introduced by Pieprzyk and Qu [20]. As mentioned in the introduction, they showed that these functions are useful, among other things, in the design of fast hashing algorithms with strong cryptographic properties.

A Boolean functions $F \in \mathcal{B}_n$ can be identified with a multi-variable Boolean polynomial, known as the algebraic normal form (or ANF for short) of the Boolean function. The degree of a Boolean function is simply the degree of its ANF. Symmetric and rotation symmetric Boolean functions are very well-structured functions and this is reflected on their ANFs. Let us elaborate more about what we just said. The symbol $\oplus$ is used to denote addition in $\mathbb{F}_2$.

It is a well-established result in the theory of Boolean functions that the ANF of any symmetric Boolean function is a linear combination of elementary symmetric Boolean polynomials. To be more precise, let $\boldsymbol{e}_k(n)$ be the elementary symmetric polynomial in n variables of degree k. For example,

$$\boldsymbol{e}_3(4) = X_1X_2X_3 \oplus X_1X_4X_3 \oplus X_2X_4X_3 \oplus X_1X_2X_4.$$

Every symmetric Boolean function $F \in \mathcal{B}_n$ can be identified with an expression of the form

$$F(\mathbf{X}) = \boldsymbol{e}_{k_1}(n) \oplus \boldsymbol{e}_{k_2}(n) \oplus \cdots \oplus \boldsymbol{e}_{k_s}(n), \tag{2.1}$$

where $0 \leq k_1 < k_2 < \cdots < k_s$ are integers. For the sake of simplicity, the notation $\boldsymbol{e}_{[k_1,\ldots,k_s]}(n)$ is used to denote (2.1). For example,

$$\begin{aligned} \boldsymbol{e}_{[2,1]}(3) &= \boldsymbol{e}_2(3) \oplus \boldsymbol{e}_1(3) \\ &= X_1X_2 \oplus X_3X_2 \oplus X_1X_3 \oplus X_1 \oplus X_2 \oplus X_3. \end{aligned} \tag{2.2}$$

On the other hand, suppose that $R \in \mathcal{B}_n$ is a rotation symmetric Boolean function. For the sake of simplicity, let us say that $n = 5$. Assume that $X_1X_2X_3$ is part of the ANF of the function. Then, the terms

$$\begin{aligned} E_5^1(X_1X_2X_3) &= X_2X_3X_4 \\ E_5^2(X_1X_2X_3) &= X_3X_4X_5 \\ E_5^3(X_1X_2X_3) &= X_4X_5X_1 \\ E_5^4(X_1X_2X_3) &= X_5X_1X_2 \end{aligned}$$

are also part of its ANF. Similarly, suppose that X_1X_3 is also a term of the ANF. Then,

$$X_2X_4, X_3X_5, X_4X_1, X_5X_2$$

are also part of the ANF. An example of a rotation symmetric Boolean function with this property is given by

$$\begin{aligned} R(\mathbf{X}) =& X_1X_2X_3 \oplus X_2X_3X_4 \oplus X_3X_4X_5 \oplus X_4X_5X_1 \oplus X_5X_1X_2 \oplus \\ & X_1X_3 \oplus X_2X_4 \oplus X_3X_5 \oplus X_4X_1 \oplus X_5X_2. \end{aligned} \tag{2.3}$$

The above discussion tells us that once a monomial $X_{i_1} \cdots X_{i_t}$ is part of the ANF of a rotation symmetric Boolean function, so is $E_n^k(X_{i_1} \cdots X_{i_t})$ for all $1 \leq k \leq n$. Let $1 < j_1 < \cdots < j_s$ be integers. A rotation symmetric Boolean function of the form

$$R_{j_1,\ldots,j_s}(n) = X_1X_{j_1} \cdots X_{j_s} \oplus X_2X_{j_1+1} \cdots X_{j_s+1} \oplus \cdots \oplus X_nX_{j_1-1} \cdots X_{j_s-1}, \tag{2.4}$$

where the indices are taken modulo n and the complete system of residues is $\{1, 2, \ldots, n\}$, is called a *monomial rotation symmetric* Boolean function. We say that $R_{j_1,\ldots,j_s}(n)$ is *long cycle*, if the period is n, like the one above, and *short cycle*, if the period is a nontrivial divisor of n; for example, $R_3(4) = X_1X_3 \oplus X_2X_4$ is a short cycle.

The rotation symmetric Boolean function (2.3) is given by

$$R(\mathbf{X}) = R_{2,3}(5) \oplus R_3(5).$$

In the literature (see [9]), the notation $(1, j_1, \ldots, j_s)_n$ is often used to represent the monomial rotation Boolean function (2.4).

As mentioned earlier, Boolean functions have applications to many scientific fields. In some applications related to cryptography it is important for Boolean functions to be balanced. Balancedness of Boolean functions is often studied from the point of view of exponential sums. The *exponential sum* of an n-variable Boolean function $F(\mathbf{X})$ is defined as the sum

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

Observe that $F \in \mathcal{B}_n$ is balanced if and only if $S(F) = 0$.

In [2, 5], sequences of the form $\{S(\boldsymbol{e}_{[k_1,\dots,k_s]}(n))\}_n$ were considered. In particular, it was showed – first in [2] and later in [5] – that these sequences satisfies linear recurrences with integer coefficients. To be specific, they proved the following result:

Theorem 2.1. *Let $1 \le k_1 < \cdots < k_s$ be integers and let $r = \lfloor \log_2(k_s)\rfloor + 1$. The sequence $\{S(\boldsymbol{e}_{[k_1,\dots,k_s}(n))\}_n$ satisfies the linear recurrence whose characteristic polynomial is given by*

$$(X-2)\Phi_4(X-1)\Phi_8(X-1)\cdots\Phi_{2^r}(X-1), \tag{2.5}$$

where $\Phi_m(X)$ represents the m-th cyclotomic polynomial.

This theorem was used in [5] to calculate the asymptotic behavior of these sequences and it was later generalized to some perturbations of symmetric Boolean functions (see [6]).

Suppose that $1 \le j < n$ and let $F(\mathbf{X})$ be a binary polynomial in the variables $X_1, \dots, X_j$ (the first j variables in $X_1, \dots, X_n$). The function $\boldsymbol{e}_{[k_1,\dots,k_s]}(n) \oplus F(\mathbf{X})$ is called a *perturbation* of $\boldsymbol{e}_{[k_1,\dots,k_s]}(n)$. In [6], it was proved that the sequence of exponential sums of the perturbation $\boldsymbol{e}_{[k_1,\dots,k_s]}(n) \oplus F(\mathbf{X})$, that is, the sequence

$$\{S(\boldsymbol{e}_{[k_1,\dots,k_s]}(n) \oplus F)\}_n \tag{2.6}$$

also satisfies the recurrence whose characteristic polynomial is (2.5).

Theorem 2.2. *Let $1 \le k_1 < \cdots < k_s$ be integers and let $r = \lfloor \log_2(k_s)\rfloor + 1$. Suppose that $1 \le j < n$ and let $F(\mathbf{X})$ be a binary polynomial in the variables $X_1, \dots, X_j$ (the first j variables in $X_1, \dots, X_n$). The sequence*

$$\{S(\boldsymbol{e}_{[k_1,\dots,k_s}(n) \oplus F)\}_n \tag{2.7}$$

satisfies the linear recurrence whose characteristic polynomial is given by

$$(X-2)\Phi_4(X-1)\Phi_8(X-1)\cdots\Phi_{2^r}(X-1). \tag{2.8}$$

Moreover, if the function $F(\mathbf{X})$ happens to be balanced, that is, if $S(F) = 0$, then sequence (2.7) satisfies the linear recurrence whose characteristic polynomial is given by

$$\Phi_4(X-1)\Phi_8(X-1)\cdots\Phi_{2^r}(X-1). \tag{2.9}$$

In [9], Cusick considered sequences of exponential sums of rotation symmetric Boolean functions. He proved that, as in the case of symmetric Boolean functions, these type of sequences also satisfy linear recurrence with integer coefficients. This result was later generalized in [4] to exponential sums over Galois fields. In particular, it was showed [4] that the linear recurrent behavior of $\{S(R_{j_1,\dots,j_s}(n))\}_n$ is dominated by the linear recurrent behavior of $\{S(T_{j_1,\dots,j_s}(n))\}_n$ where $T_{j_1,\dots,j_s}(n)$ is defined by

$$T_{j_1,\dots,j_s}(n) = X_1X_{j_1}\cdots X_{j_s} \oplus X_2X_{j_1+1}\cdots X_{j_s+1} \oplus \cdots \oplus X_{n+1-j_s}X_{j_1+n-j_s}\cdots X_{j_{s-1}+n-j_s}X_n.$$

As mentioned in the introduction, the main goal of this article is to put all these results in the more general framework of Walsh transformations and their generalizations. In the next section, we consider Walsh transformations of symmetric and rotation symmetric Boolean functions.

3. Walsh transforms of symmetric and rotation symmetric Boolean functions

The (non-normalized) *Walsh transform* of a Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2$ is defined to be the function $W_F : \mathbb{F}_2^n \to \mathbb{Z}$ given by

$$W_F(\boldsymbol{a}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{F(\mathbf{x})\oplus \boldsymbol{a}\cdot\mathbf{x}}, \tag{3.1}$$

where $\boldsymbol{a}\cdot\mathbf{x}$ is the usual scalar product. In the literature, this transformation is often defined as

$$W_F(\boldsymbol{a}) = \frac{1}{2^{n/2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{F(\mathbf{x})\oplus \boldsymbol{a}\cdot\mathbf{x}}.$$

However, one is a rescale of the other, thus we use definition (3.1). Observe that $W_F(\mathbf{0})$ is the regular exponential sum $S(F)$.

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

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

It is known that

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

In some cryptographic applications, highly nonlinear Boolean functions are useful. Boolean functions with the highest nonlinearity, namely, $2^{n-1} - 2^{n/2-1}$ (hence n must be even) are known as bent functions (introduced by Rothaus in mid '60 and published in [22]). An alternative definition is the following: a function $F \in \mathcal{B}_n$ is a bent function if

$$\frac{1}{2^{n/2}}|W_F(\boldsymbol{a})| = 1$$

for all $\boldsymbol{a} \in \mathbb{F}_2^n$.

One of the main goals in this article is to find families of polynomials $\{F_n\}_n$, with $F_n \in \mathcal{B}_n$, such that the behavior of the sequence $\{W_{F_n}(\boldsymbol{a})\}$ as n increases can be analyzed. A necessary condition to be able to do this is that the tuple $\boldsymbol{a}$ must be of dimension n. However we really want $\boldsymbol{a}$ to be "constant". This apparent contradiction can be circumvented by selecting an initial tuple $\boldsymbol{a}$ of dimension, say j, fixing it, and continue right padding zeros to the end of $\boldsymbol{a}$ until its dimension is n. For example, suppose that the initially selected tuple is $\boldsymbol{a} = (1, 0, 1)$. When $n = 4$ we consider the tuple to be $\boldsymbol{a} = (1, 0, 1, 0)$, when $n = 5$ we consider $\boldsymbol{a}$ to be $\boldsymbol{a} = (1, 0, 1, 0, 0)$, and so on. Note that this implies, for example, that if $\boldsymbol{a} = (1, 0, 1)$, then

$$W_{F_n}(\boldsymbol{a}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{F_n(\mathbf{x}) \oplus G_{\boldsymbol{a}}(\mathbf{x})} = W_{F_n \oplus G_{\boldsymbol{a}}}(\mathbf{0}),$$

where $G_{\boldsymbol{a}}(\mathbf{X}) = \boldsymbol{a} \cdot \mathbf{X} = X_1 \oplus X_3$.

The function $F_n(\mathbf{X}) \oplus G_{\boldsymbol{a}}(\mathbf{X})$ can be interpreted as a perturbation of the function $F_n(\mathbf{X})$ by the linear function $G_{\boldsymbol{a}}(\mathbf{X})$. This is important, especially if the function $F_n(\mathbf{X})$ is symmetric, as it will imply that the sequence $\{W_{F_n}(\boldsymbol{a})\}_n$ satisfies linear recurrences with integer coefficients. Thus, from now on, the families of Boolean polynomials $\{F_n(\mathbf{X})\}_n$ that we choose to study are symmetric and rotation symmetric Boolean functions. Of course, one of the motivations behind this choice is our desire to extend previous results to this general setting, but also because these families are good candidate for efficient implementations.

Theorems 2.1 and 2.2 can be re-written in the language of Walsh transforms. We include them here in order to ease the reading of the article.

Proposition 3.1. *Let $1 \le k_1 < \cdots < k_s$ be integers and let $r = \lfloor \log_2(k_s) \rfloor + 1$. The sequence $\{W_{e_{[k_1,\ldots,k_s]}(n)}(\mathbf{0})\}_n$ satisfies the linear recurrence whose characteristic polynomial is given by*

$$(X-2)\Phi_4(X-1)\Phi_8(X-1)\cdots\Phi_{2^r}(X-1), \tag{3.2}$$

where $\Phi_m(X)$ represents the m-th cyclotomic polynomial.

Proposition 3.2. *Let $1 \le k_1 < \cdots < k_s$ be integers and let $r = \lfloor \log_2(k_s) \rfloor + 1$. Suppose that $1 \le j < n$ and let $F(\mathbf{X})$ be a binary polynomial in the variables $X_1, \ldots, X_j$ (the first j variables in $X_1, \ldots, X_n$). The sequence*

$$\{W_{\boldsymbol{e}_{[k_1,\ldots,k_s]}(n) \oplus F}(\mathbf{0})\}_n \tag{3.3}$$

satisfies the linear recurrence whose characteristic polynomial is given by

$$(X-2)\Phi_4(X-1)\Phi_8(X-1)\cdots\Phi_{2^r}(X-1). \tag{3.4}$$

Moreover, if the function $F(\mathbf{X})$ happens to be balanced, that is, if $S(F) = 0$, then sequence (3.3) satisfies the linear recurrence whose characteristic polynomial is given by

$$\Phi_4(X-1)\Phi_8(X-1)\cdots\Phi_{2^r}(X-1). \tag{3.5}$$

This information implies the following result. For a tuple $\mathbf{x} \in \mathbb{F}_2^n$, the expression $w(\mathbf{x})$ represents the *Hamming weight* of $\mathbf{x}$, that is, the number of 1's in $\mathbf{x}$.

Theorem 3.3. *Let $0 \leq k_1 < k_2 < \cdots < k_s$ be integers and $r = \lfloor \log_2(k_s) \rfloor + 1$. Let j be an integer and $\boldsymbol{a} \in \mathbb{F}_2^j$ fixed. The sequence*

$$\{W_{\boldsymbol{e}_{[k_1,k_2,\ldots,k_s]}(n)}(\boldsymbol{a})\}_n$$

satisfies the homogeneous linear recurrence whose characteristic polynomial is

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

Moreover, if $\boldsymbol{a} \neq \mathbf{0}$, then the sequence satisfies the lower order homogeneous linear recurrence whose characteristic polynomial is

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

Finally, we have the closed formula

$$W_{\boldsymbol{e}_{[k_1,k_2,\ldots,k_s]}(n+w(\boldsymbol{a}))}(\boldsymbol{a}) = d_0(\boldsymbol{a})2^n + \sum_{\ell=1}^{2^r-1} d_\ell(\boldsymbol{a})\lambda_\ell^n,$$

where

$$d_\ell(\boldsymbol{a}) = \frac{1}{2^r}\sum_{q=0}^{2^r-1}\left(\sum_{m=0}^{w(\boldsymbol{a})}(-1)^m\binom{w(\boldsymbol{a})}{m}(-1)^{\binom{q+m}{k_1}+\cdots+\binom{q+m}{k_s}}\right)\xi_\ell^q$$

$\lambda_\ell = 1+\xi_\ell^{-1}$ and $\xi_\ell = e^{\frac{\pi i \ell}{2^{r-1}}}$.

Proof. The first claim is a direct consequence of the above discussion and Proposition 3.2. The second claim follows from the fact that if $\boldsymbol{a} \neq \mathbf{0}$, then $W_{\boldsymbol{a}\cdot\mathbf{X}}(\mathbf{0}) = 0$. Thus, $W_{\boldsymbol{e}_{[k_1,k_2,\ldots,k_s]}(n)}(\boldsymbol{a})$ can be identify with the exponential sum of the perturbation $\boldsymbol{e}_{[k_1,k_2,\ldots,k_s]}(n) \oplus \boldsymbol{a}\cdot\mathbf{X}$ with $\boldsymbol{a}\cdot\mathbf{X}$ balanced.

The final claim follows from a series of identities. The first one is the formula of Cai, Green and Thierauf [2] for exponential sums of elementary symmetric Boolean functions, specifically,

$$S(\boldsymbol{e}_{[k_1,\ldots,k_s]}(n)) = c_0(k_1,\ldots,k_s)2^n + \sum_{\ell=1}^{2^r-1} c_\ell(k_1,\ldots,k_s)\lambda_\ell^n, \tag{3.6}$$

where

$$c_\ell(k_1,\ldots,k_s) = \frac{1}{2^r}\sum_{q=0}^{2^r-1}(-1)^{\binom{q}{k_1}+\cdots+\binom{q}{k_s}}\xi_\ell^q.$$

The second identity states that if $F(\mathbf{X})$ is a Boolean polynomial in the variables $X_1,\ldots,X_j$, then (see [6])

$$S(\boldsymbol{e}_{[k_1,\ldots,k_s]}(n) \oplus F) = \sum_{m=0}^{j} C_m(F) S\left(\sum_{t=0}^{m}\binom{m}{t}\boldsymbol{e}_{[k_1-t,\ldots,k_s-t]}(n-j)\right), \tag{3.7}$$

where $C_m(F)$ is defined as

$$C_m(F) = \sum_{\mathbf{x}\in\mathbb{F}_2^j\,:\,w(\mathbf{x})=m}(-1)^{F(\mathbf{x})}.$$

The identification of $W_{\boldsymbol{e}_{[k_1,k_2,\ldots,k_s]}(n)}(\boldsymbol{a})$ with $S(\boldsymbol{e}_{[k_1,k_2,\ldots,k_s]}(n) \oplus \boldsymbol{a}\cdot\mathbf{x})$, which in turns can be identified with the following exponential sum

$$S(\boldsymbol{e}_{[k_1,k_2,\ldots,k_s]}(n) \oplus X_1 \oplus X_2 \oplus \cdots \oplus X_{w(\boldsymbol{a})}),$$

together with (3.6) and (3.7) tell us that

$$W_{\boldsymbol{e}_{[k_1,k_2,\ldots,k_s]}(n)}(\boldsymbol{a}) = d_0(\boldsymbol{a})2^n + \sum_{l=1}^{2^r-1} d_\ell(\boldsymbol{a})\lambda_\ell^n,$$

where

$$d_\ell(\boldsymbol{a}) = \sum_{m=0}^{w(\boldsymbol{a})} C_m(X_1 \oplus X_2 \oplus \cdots \oplus X_{w(\boldsymbol{a})})\left(\frac{1}{2^r}\sum_{q=0}^{2^r-1}(-1)^{\sum_{t=0}^{m}\binom{m}{t}\left(\binom{q}{k_1-t}+\cdots+\binom{q}{k_s-t}\right)}\right).$$

The identities

$$C_m(X_1 \oplus X_2 \oplus \cdots \oplus X_{w(\boldsymbol{a})}) = (-1)^m \binom{w(\boldsymbol{a})}{m}$$

and

$$\sum_{t=0}^{m} \binom{m}{t}\binom{q}{k-t} = \binom{q+m}{k}$$

complete the proof. □

Example 3.4. Consider the symmetric Boolean function $F_n(\mathbf{X}) = \boldsymbol{e}_{[2,5]}(n)$ and let $\boldsymbol{a} = (0,1,1)$. Theorem 3.3 implies that $\{W_{\boldsymbol{e}_{[2,5]}(n)}(\boldsymbol{a})\}_n$ satisfies the linear recurrence whose characteristic polynomial is given by

$$\left(X^2 - 2X + 2\right)\left(X^4 - 4X^3 + 6X^2 - 4X + 2\right). \tag{3.8}$$

Using this recurrence, it is not hard to show that the first few values of $\{W_{\boldsymbol{e}_{[2,5]}(n)}(\boldsymbol{a})\}_{n\geq 6}$ are

$$4, 0, 0, 12, 40, 72, 64, -72, -464, -1248, -2496, -4080, -5408, -4896, 1024, \ldots.$$

Moreover, recurrence (3.8) and some elementary linear algebra produces the closed formula,

$$\begin{aligned} W_{\boldsymbol{e}_{[2,5]}(n)}(\boldsymbol{a}) \quad = \quad & \left(2 - \frac{3}{\sqrt{2}}\right)\left(2+\sqrt{2}\right)^{n/2} \cos\left(\frac{\pi n}{8}\right) - 2^{n/2}\cos\left(\frac{\pi n}{4}\right) + \\ & \left(2 + \frac{3}{\sqrt{2}}\right)\left(2-\sqrt{2}\right)^{n/2} \cos\left(\frac{3\pi n}{8}\right). \end{aligned}$$

Walsh transforms of symmetric Boolean functions are not the only ones that are linear recurrent with integer coefficients. Recently, Cusick [9] showed that exponential sums of rotation symmetric Boolean functions satisfy linear recurrences with integer coefficients. This result was extended to exponential sums over Galois fields in [4]. It can also be extended to Walsh transforms of rotation symmetric Boolean polynomials. For instance, Lemma 2.2 in [4] can be extended without too much effort to show that if $F(\mathbf{X})$ is a Boolean polynomial in j variables (j fixed), then $\{S(R_{j_1,\ldots,j_s}(n) \oplus F(\mathbf{X}))\}_n$ satisfies the same linear recurrence that $\{S(R_{j_1,\ldots,j_s}(n))\}_n$ satisfies. In particular, this implies that for n sufficiently large, the sequence $\{W_{R_{j_1,\ldots,j_s}(n)}(\boldsymbol{a})\}_n$ satisfies the same linear recurrence as $\{W_{R_{j_1,\ldots,j_s}(n)}(\mathbf{0})\}_n$.

Example 3.5. It was showed in [4] that $\{W_{R_{2,\ldots,k}(n)}(\mathbf{0})\}_n$ satisfies the linear recurrence with constant coefficients whose characteristic polynomial is given by

$$p_k(X) = X^k - 2(X^{k-2} + X^{k-3} + \cdots + X + 1). \tag{3.9}$$

Let $\boldsymbol{a} \in \mathbb{F}_2^j$ be such that its last entry is 1 (if that is not the case, say its last 1 is at position $\ell < j$, then view $\boldsymbol{a}$ as a tuple in a vector space $\mathbb{F}_2^\ell$). Then the sequence $\{W_{R_{2,\ldots,k}(n)}(\boldsymbol{a})\}_{n\geq \max(k,j)}$ satisfies the linear recurrence whose characteristic polynomial is given by (3.9). For instance, if $\boldsymbol{a} = (1,1,0,0,1)$, then $\{W_{R_{2,3}(n)}(\boldsymbol{a})\}_{n\geq 5}$ satisfies the linear recurrence whose characteristic polynomial is $X^3 - 2X - 2$. Using this recurrence, it is not hard to see that the first few values of $\{W_{R_{2,3}(n)}(\boldsymbol{a})\}_{n\geq 5}$ are given by

$$4, -4, 16, 0, 24, 32, 48, 112, 160, 320, 544, 960, 1728, 3008, 5376, 9472, 16768, 29696, \ldots.$$

The closed formula for $W_{R_{2,3}(n)}(\boldsymbol{a})$, however, is not as simple as the one from Example 3.4. In this case, the closed formula is given by

$$W_{R_{2,3}(n)}(\boldsymbol{a}) = \beta_1\alpha_1^n + \beta_2\alpha_2^n + \beta_3\alpha_3^n,$$

where the α_j's are the roots of $X^3 - 2X - 2$, with

$$\alpha_1 \in \mathbb{R},\ \alpha_3 = \overline{\alpha_2} \text{ and } \mathrm{Im}(\alpha_2) > 0,$$

and the β_j are the roots of $19X^3 - 57X^2 + 225X - 23$, with

$$\beta_1 \in \mathbb{R},\ \beta_3 = \overline{\beta_2} \text{ and } \mathrm{Im}(\beta_2) > 0.$$

Example 3.6. The sequence $\{W_{R_{2,\dots,k-1,k}(n)\oplus R_{2,\dots,k-2,k}(n)}(\mathbf{0})\}_n$ satisfies the linear recurrence with constant coefficients whose characteristic polynomial is given by (see [4])

$$q_k(X) = X^k - 2X^{k-1} + 2X - 2. \tag{3.10}$$

Therefore, if $\boldsymbol{a} \in \mathbb{F}_2^j$ where j is fixed, then $\{W_{R_{2,\dots,k-1,k}(n)\oplus R_{2,\dots,k-2,k}(n)}(\boldsymbol{a})\}_{n\geq N(j,k)}$, where $N(j,k)$ is a sufficiently large integer depending on j and k, satisfies the linear recurrence whose characteristic polynomial is given by (3.10). For example, suppose that $\boldsymbol{a} = (1,0,1,1)$. Then, the sequence $\{W_{R_{2,3,4}(n)\oplus R_{2,4}(n)}(\boldsymbol{a})\}$ satisfies the linear recurrence whose characteristic polynomial is

$$X^4 - 2X^3 + 2X - 2.$$

Using this recurrence we can compute the value of $W_{R_{2,3,4}(n)\oplus R_{2,4}(n)}(\boldsymbol{a})$ for big values of n. For instance,

$$W_{R_{2,3,4}(200)\oplus R_{2,4}(200)}(\boldsymbol{a}) = -29033604282578723548878452629909624952134303744,$$

and $W_{R_{2,3,4}(100000)\oplus R_{2,4}(100000)}(\boldsymbol{a})$ is a negative integer with 23469 digits with the 2-valuation 25002 (that is, 2^{25002} does and 2^{25003} does not divide it). A closed formula similar to the ones presented in Examples 3.4 and 3.5 is very complicated and impractical, thus we do not include such formula.

The fact that rotation symmetric Boolean functions are linear recurrent can be used to provide asymptotic analysis of their behavior. For example, we have the following result.

Theorem 3.7. *Let $k \geq 5$. Then, for all sufficiently large n, the rotation symmetric Boolean function $R_{2,3,\dots,k}(n) \oplus R_{2,3,\dots,k-1}(n)$ is not bent.*

Proof. Let $F_n(\mathbf{X}) = R_{2,3,\dots,k}(n) \oplus R_{2,3,\dots,k-1}(n)$. Recall that a Boolean function $F \in \mathcal{B}_n$ is bent if

$$|W_F(\boldsymbol{b})| = 2^{n/2},$$

for all $\boldsymbol{b} \in \mathbb{F}_2^n$. We use the fact that, for a fixed tuple $\boldsymbol{a} \in \mathbb{F}_2^j$, the sequence $\{W_{F_n}(\boldsymbol{a})\}$ is linear recurrent with characteristic polynomial (see [4])

$$q_k(X) = X^k - 2X^{k-1} + 2.$$

to prove the result.

For any polynomial $f(X) = a_m X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0$, define

$$M(f) = |a_m| \prod_{j=1}^{m} \max\{1, |\beta_j|\},$$

where $\beta_1, \beta_2, \dots, \beta_m$ are the roots of $f(X)$. Landau's inequality states that

$$M(f) \leq \sqrt{|a_0|^2 + |a_1|^2 + \cdots + |a_n|^2}.$$

Let α_t, for $1 \leq t \leq k$, be the roots of $q_k(X)$. Observe that Landau's inequality implies

$$M(q_k) \leq \sqrt{2^2 + 2^2 + 1} = \sqrt{9} = 3. \tag{3.11}$$

Choose α to be the root of $q_k(X)$ with the biggest modulus, that is, $|\alpha_t| \leq |\alpha|$ for all $1 \leq t \leq k$. Without loss of generality, assume $\alpha = \alpha_k$. Observe that $q_k(2) = 2$ and

$$q_k\left(\frac{7}{4}\right) = 2 - \frac{1}{7}\left(\frac{7}{4}\right)^k < 0.$$

Therefore, by the intermediate value theorem, there is a real root of $q_k(X)$ between $7/4$ and 2. This implies

$$|\alpha| > \frac{7}{4} > \sqrt{2}.$$

Moreover, α is the real root between $7/4$ and 2 and no other root has the same modulus as α. To see this, suppose, on the contrary, that there is another root, say α_{t_0} with $t_0 < k$, such that $|\alpha_{t_0}| = |\alpha|$. Then,

$$M(q_k) = \prod_{t=1}^{k} \max\{1, |\alpha_t|\} > \left(\frac{7}{4}\right)^2 > 3,$$

which is a contradiction to (3.11). Therefore, $|\alpha_t| < |\alpha|$ for every $t = 1, 2, \dots, k-1$ and α is the real root that lies between $7/4$ and 2.

Now, by the theory of linear recurrences, we know that

$$W_{F_n}(\boldsymbol{a}) = \sum_{t=0}^{k} c_t(\boldsymbol{a})\alpha_t^n,$$

for some constants $c_t(\boldsymbol{a})$. Eisenstein criterion, with the choice of the prime 2, implies that $q_k(X)$ is irreducible over $\mathbb{Q}[X]$. Since $W_{F_n}(\boldsymbol{a})$ is always an integer, then the irreducibility of $q_k(X)$ over $\mathbb{Q}[X]$ implies that $c_t(\boldsymbol{a}) \neq 0$ for every $1 \leq t \leq k$. But then,

$$\lim_{n\to\infty} \left|\frac{W_{F_n}(\boldsymbol{a})}{\alpha^n}\right| = |c_k(\boldsymbol{a})| \neq 0.$$

Therefore, asymptotically,

$$|W_{F_n}(\boldsymbol{a})| \sim |c_k(\boldsymbol{a})|\alpha^n.$$

But $|c_k(\boldsymbol{a})|\alpha^n > (\sqrt{2})^n = 2^{n/2}$ for all sufficiently large n. Therefore, for this fixed tuple $\boldsymbol{a}$, one has

$$|W_{F_n}(\boldsymbol{a})| > 2^{n/2},$$

for all sufficiently large n. We conclude that $F_n(\mathbf{X}) = R_{2,3,\ldots,k}(n) \oplus R_{2,3,\ldots,k-1}(n)$ is not bent for all sufficiently large n. □

Observe that the above discussion implies that $S(R_{2,3,\ldots,k}(n) \oplus R_{2,3,\ldots,k-1}(n)) = W_{R_{2,3,\ldots,k}(n)\oplus R_{2,3,\ldots,k-1}(n)}(\mathbf{0})$ satisfies

$$\lim_{n\to\infty} \frac{1}{2^n} S(R_{2,3,\ldots,k}(n) \oplus R_{2,3,\ldots,k-1}(n)) = 0.$$

In [5], functions with this property were good candidates for the search of balanced Boolean functions. However, we have the following result.

Corollary 3.8. *Let $k > 2$. The polynomial $R_{2,3,\ldots,k}(n) \oplus R_{2,3,\ldots,k-1}(n)$ is not balanced for all sufficiently large n.*

Proof. Choose $\boldsymbol{a} = \mathbf{0}$ in the proof of Theorem 3.7. □

We point out that Theorem 3.7 can be extended to other families. For example, it applies to the sequence

$$\{W_{R_{2,3,\ldots,k}(n)}(\boldsymbol{a})\}_n \tag{3.12}$$

with characteristic polynomial

$$X^k - 2(X^{k-2} + X^{k-3} + \cdots + X + 1) \tag{3.13}$$

and to the sequences

$$\{W_{R_{2,3,\ldots,k-2,k}(n)}(\boldsymbol{a})\}_n \text{ and } \{W_{R_{2,3,\ldots,k-2,k+1}(n)}(\boldsymbol{a})\}_n \tag{3.14}$$

both with characteristic polynomial

$$X^{k+1} - 2X^{k-1} - 2X^{k-2} - \cdots - 2X^3 - 4. \tag{3.15}$$

In fact the proof follows almost verbatim. The the only differences are that Eisenstein-Dumas criterion must be used in place of Eisenstein criterion and that to show that there is a unique real root with maximum modulus, that is, all other roots have modulus less than the modulus of this real root, might not be an easy task.

Examples (3.12) and (3.14) provide asymptotic evidence to the following conjecture of Stănică and Maitra [27]:

There are no homogeneous rotation symmetric bent functions of degree bigger than 2.

However, we point out that Stănică showed that $R_{2,3,\ldots,k}(n)$ is never bent [24] and that the results of [18] imply that these families of rotation polynomials are asymptotically not bent. Thus, we do not pursue a proof for these examples. However, it looks like the key in all these examples is that their Walsh transforms satisfy linear recurrences with integer coefficients for which the characteristic polynomial always has a root with modulus bigger than $\sqrt{2}$. It would be interesting if the ideas of this paper would be used to settle this conjecture.

For completeness purposes, we present the following proposition. It bounds the roots of the characteristic polynomials of linear recurrences associated to Walsh transforms of Boolean polynomials. This is an upper bound, thus it does not help in the search of roots with modulus bigger than $\sqrt{2}$, but it does help as to the value of the limit

$$\lim_{n\to\infty} \frac{1}{2^n} S(F_n).$$

Proposition 3.9. *Let $F_n \in \mathcal{B}_n$ be a family of Boolean functions. Suppose that for some fixed tuple $\boldsymbol{a}$, the sequence $\{W_{F_n}(\boldsymbol{a})\}_n$ satisfies a linear recurrence with integer coefficients. Suppose $P(X)$ is the characteristic polynomial of the minimal of such recurrence. Then, the roots β_j of $P(X)$ satisfy $|\beta_j| \leq 2$. Moreover, if $P(X)$ is irreducible in $\mathbb{Q}[X]$, then equality is attained only if $P(2X)$ is a palindromic polynomial of even degree.*

Proof. Let β be the root of $P(X)$ with the highest modulus. If $|\beta| > 2$, then eventually $|W_{F_n}(\boldsymbol{a})|$ surpasses 2^n because

$$W_{F_n}(\boldsymbol{a}) = \sum_{\beta_j\,:\,P(\beta_j)=0} c_j(\boldsymbol{a})\beta_j^n.$$

for some suitable constants $c_j(\boldsymbol{a})$. Clearly, this is impossible since by definition $|W_f(\boldsymbol{a})| \leq 2^n$ for every $f \in \mathcal{B}_n$. This shows the first claim.

For the second claim, suppose that $P(X)$ is irreducible in $\mathbb{Q}[X]$ and β is a root with $|\beta| = 2$. Then $\beta = 2e^{2\pi i\theta}$, for $0 \leq \theta \leq 1$. That is,

$$P(2e^{2\pi i\theta}) = 0.$$

In other words, $e^{2\pi i\theta}$ is a root of $P(2X)$. Therefore, $P(2X)$ is irreducible and has a root in the unit circle. But if an irreducible polynomial in $\mathbb{Q}[X]$ has a root in the unit circle, then the polynomial is palindromic of even degree [8, Th. 1.1]. This concludes the proof. □

***Remark* 3.10.** Observe that Proposition 3.9 is true in general, regardless if the family $\{F_n\}_n$ is or is not symmetric or rotation symmetric.

Example 3.11. Let $P_1(X)$ and $P_2(X)$ be the polynomials (3.13) and (3.15) (resp.). Both polynomials are irreducible in $\mathbb{Q}[X]$, but $P_1(2X)$ and $P_2(2X)$ are not palindromic. Therefore, the roots of both polynomials lie in $|z| < 2$.

The approach presented in [4] can also be used to see that Walsh transforms of linear combinations of rotation symmetric Boolean polynomials and symmetric Boolean polynomials satisfy linear recurrences with integer coefficients. We will not repeat the argument in this article, however, for completeness purposes, we provide the definition (taken from [4]) of a recursive generating set for a sequence, which was the main tool used in the article [4].

Definition 3.12. Let $\{b(n)\}$ be a sequence on an integral domain D. A set of sequences

$$\{\{a_1(n)\}, \{a_2(n)\}, \ldots, \{a_s(n)\}\},$$

where s is some natural number, is called a *recursive generating set for* $\{b(n)\}$ if

(1) there is an integer ℓ such that for every n, $b(n)$ can be written as a linear combination of the form

$$b(n) = \sum_{j=1}^{s} c_j \cdot a_j(n-\ell),$$

where c_j's are constants that belong to D, and

(2) for each $1 \leq j_0 \leq s$ and every n, $a_{j_0}(n)$ can be written as a linear combination of the form

$$a_{j_0}(n) = \sum_{j=1}^{s} d_j \cdot a_j(n-1),$$

where d_j's are also constants that belong to D.

The sequences $\{a_j(n)\}$'s are called *recursive generating sequences for* $\{b(n)\}$.

It is clear that if we find a generating set for a sequence $\{b(n)\}$, then such sequence is linear recurrent. This is because equations from (2) in Definition 3.12 can be written in matrix form and any annihilating polynomial for the corresponding matrix is the characteristic polynomial of a linear recurrence satisfied by the $\{a_j(n)\}$'s.

Let us provide an example to show how this method works. We state such example for exponential sums, but it can be extended to Walsh transforms without too much efforts.

Example 3.13. Observe that

$$\begin{aligned} S(R_{2,3}(n) \oplus \boldsymbol{e}_2(n)) =& S(T_{2,3}(n-2) \oplus \boldsymbol{e}_2(n-2))+ \\ & S(T_{2,3}(n-2) \oplus X_{n-3}X_{n-2} \oplus \boldsymbol{e}_2(n-2) \oplus \boldsymbol{e}_1(n-2))+ \\ & S(T_{2,3}(n-2) \oplus \boldsymbol{e}_2(n-2) \oplus \boldsymbol{e}_1(n-2) \oplus X_1X_2)- \\ & S(T_{2,3}(n-2) \oplus \boldsymbol{e}_2(n-2) \oplus X_1 \oplus X_1X_2 \oplus X_{n-2} \oplus X_{n-3}X_{n-2}). \end{aligned} \tag{3.16}$$

Also, if

$$a_{\beta_1,\beta_2,\beta_3,\beta_4,\beta_5}(n) = S(T_{2,3}(n) \oplus \beta_1 X_1 \oplus \beta_2 X_1X_2 \oplus \beta_3 X_n \oplus \beta_4 X_{n-1}X_n \oplus \boldsymbol{e}_2(n) \oplus \beta_5 \boldsymbol{e}_1(n)),$$

then

$$a_{\beta_1,\beta_2,\beta_3,\beta_4,\beta_5}(n) = a_{\beta_1,\beta_2,0,0,\beta_5}(n-1) + (-1)^{\beta_3\oplus\beta_5} a_{\beta_1,\beta_2,\beta_4,\beta_1,\beta_5\oplus 1}(n-1). \tag{3.17}$$

Equations (3.16) and (3.17) imply that the sequences $\{a_{\beta_1,\beta_2,\beta_3,\beta_4,\beta_5}(n)\}$ form a recursive generating set for $\{S(R_{2,3}(n) \oplus \boldsymbol{e}_2(n))\}_n$. Moreover, the minimal polynomial of the 32×32 matrix associated to (3.17) is

$$X^7 - 2X^6 + 2X^5 + 4X.$$

This implies that $\{S(R_{2,3}(n) \oplus \boldsymbol{e}_2(n))\}$ satisfies the linear recurrence with characteristic polynomial

$$X^6 - 2X^5 + 2X^4 + 4.$$

This recurrence can be used to show that the first few values of $\{S(R_{2,3}(n) \oplus \boldsymbol{e}_2(n))\}_{n\geq 3}$ are given by

$$2, 4, 0, -20, -40, -48, -24, 32, 112, 240, 416, 544, 352, -512, -2176, -4288, -5888, -5376, \ldots.$$

This example leads to the following result.

Theorem 3.14. *Suppose that k_1, k_2 are natural numbers with $k_1 > 1$. The sequence*

$$\{S(R_{2,3,\ldots,k_1}(n) \oplus \boldsymbol{e}_{k_2}(n))\}_n$$

satisfies a linear recurrence with integer coefficients of order less than or equal to $2^{2(k_1-1)+k_2-1}$.

Proof. Define

$$\begin{aligned} a_{(\beta_1,\beta_2,\ldots,\beta_{2k_1+k_2-3})}(n;k_1,k_2) = S(& T_{2,3,\ldots,k_1}(n) \oplus \beta_1 X_1 \oplus \beta_2 X_1X_2 \oplus \cdots \oplus \beta_{k_1-1} X_1X_2\cdots X_{k_1-1} \oplus \\ & \beta_{k_1} X_n \oplus \beta_{k_1+1} X_nX_{n-1} \oplus \cdots \oplus \beta_{2(k_1-1)} X_nX_{n-1}\cdots X_{n-k_1+1} \oplus \\ & \boldsymbol{e}_{k_2}(n) \oplus \beta_{2k_1-1}\boldsymbol{e}_{k_2-1}(n) \oplus \cdots \oplus \beta_{2k_1+k_2-3}\boldsymbol{e}_1(n)). \end{aligned} \tag{3.18}$$

The sequences $\{a_{(\beta_1,\beta_2,\ldots,\beta_{2k_1+k_2-3})}(n;k_1,k_2)\}$ form a recursive generating set for the sequence

$$\{S(R_{2,3\ldots,k_1}(n) \oplus \boldsymbol{e}_{k_2}(n))\},$$

thus, $\{S(R_{2,3\ldots,k_1}(n) \oplus \boldsymbol{e}_{k_2}(n))\}$ is linear recurrent. Now, we observe that the corresponding matrix for the recursive generating set is of dimension $2^{2(k_1-1)+k_2-1} \times 2^{2(k_1-1)+k_2-1}$. Therefore, its minimal polynomial is of degree less than or equal to $2^{2(k_1-1)+k_2-1}$. This concludes the proof. □

Theorem 3.14 can be extended to Walsh transforms of linear combinations of terms of the form $R_{j_1,\ldots,j_r}(n)$ and/or the form $\boldsymbol{e}_{k_s}(n)$. However, we omit the proof of this claim – the approach is the same as the one in the proof of Theorem 3.14.

We conclude this section by studying the nonlinearity of symmetric and rotation symmetric Boolean functions. After all, the nonlinearity of a Boolean function is related to the Walsh transform of said function and we know that Walsh transforms of symmetric and rotation symmetric Boolean functions are linear recurrent. It appears that the same is true for the nonlinearity of symmetric and some rotation Boolean functions, that is, the nonlinearity of a symmetric and some rotation Boolean function appears to be linear recurrent with integer coefficients. In particular, we have the following conjectures.

Conjecture 3.15. *Let $k > 1$ be a fixed integer. The nonlinearity of $\boldsymbol{e}_k(n)$, as n increases, satisfies a linear recurrence with integer coefficients.*

As further evidence for the above conjecture, from [3, Table 1], we can infer that the nonlinearity of $\boldsymbol{e}_2(n)$ satisfies the linear recurrence whose characteristic polynomial is given by

$$X^2-2.$$

From [3, Prop. 19], since the nonlinearity of $\boldsymbol{e}_3(n)$ is

$$\begin{aligned}\mathrm{nl}(\boldsymbol{e}_3(n)) &= \begin{cases} 2^{n-2} & \text{if } n\equiv 0 \pmod 4\\ 2^{n-2}-2^{\frac{n-3}{2}} & \text{if } n\equiv 1 \pmod 4\\ 2^{n-2}-2^{\frac{n-2}{2}} & \text{if } n\equiv 2 \pmod 4\\ 2^{n-2}-2^{\frac{n-3}{2}} & \text{if } n\equiv 3 \pmod 4\end{cases}\\ &= 2^{n-2}+2^{\frac{n}{2}-3}\left(2\cos\left(\frac{n\pi}{2}\right)+\left(\sqrt{2}-1\right)(-1)^n-\sqrt{2}-1\right),\end{aligned}$$

we easily infer that $\{\mathrm{nl}(\boldsymbol{e}_3(n))\}_n$ satisfies the linear recurrence whose characteristic polynomial is given by

$$X^5-2X^4-4X+8=(X-2)\left(X^2-2\right)\left(X^2+2\right).$$

Conjecture 3.16. *Let $k>1$ be a fixed integer. The sequence of $\{\mathrm{nl}(R_{2,3,\ldots,k}(n))\}_{n\geq k}$ satisfies the linear recurrence whose characteristic polynomial is given by*

$$X^k-2(X^{k-2}+X^{k-3}+\cdots+X+1).$$

The key for the proof of Conjecture 3.16 may be the apparent identity

$$\mathrm{Spec}(R_{2,3,\ldots,k}(n))=W_{R_{2,3,\ldots,k}(n)}(\mathbf{0}).$$

In other words, the maximum value of $|W_{R_{2,3,\ldots,k}(n)}(\boldsymbol{a})|$ appears to be attained at $\boldsymbol{a}=(0,0,\ldots,0)$.

In the next sections, we generalize (further) the results presented so far. In particular, we show that many of these results carry over to generalizations of Walsh transforms.

4. nega-Hadamard transform

The Walsh transform can be generalized in various ways. In this article, we work with three of such generalizations. The first generalization is known as the nega-Hadamard transform. For any Boolean function $F(\mathbf{X})$, the *nega-Hadamard transform* of F is defined as the complex valued function given by

$$\mathcal{N}_F(\boldsymbol{a})=\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{F(\mathbf{x})\oplus\boldsymbol{a}\cdot\mathbf{x}}\, i^{w(\mathbf{x})}, \tag{4.1}$$

where $i=\sqrt{-1}$ and $w(\mathbf{x})$ is the Hamming weight of the vector $\mathbf{x}$. According to Riera and Parker [21], the nega-Hadamard transform is central to the structural analysis of pure n-qubit stabilizer quantum states. The nega-Hadamard transform is invertible, in particular, for $F\in\mathcal{B}_n$, one has

$$(-1)^{F(\mathbf{y})}=2^{-n}i^{-w(\mathbf{y})}\sum_{\mathbf{x}\in\mathbb{F}_2^n}\mathcal{N}_F(\mathbf{x})(-1)^{\mathbf{y}\cdot\mathbf{x}}.$$

See [19, 21] and [25, Lemma 1].

Many properties and concepts known for Walsh transforms can be generalized to nega-Hadamard transforms. One of such examples is the concept of bent functions. In this case, a Boolean function $F\in\mathcal{B}_n$ is said to be *negabent* if

$$\frac{1}{2^{n/2}}|\mathcal{N}_F(\boldsymbol{a})|=1.$$

The reader interested in this concept is invited to read [21, 25, 26]. In this article, we show that the linear recursive nature of the Walsh transform of symmetric and rotation symmetric Boolean functions carry over to the nega-Hadamard transform. In particular, we have the following results.

Theorem 4.1. *Let $0\leq k_1<k_2<\cdots<k_s$ be integers and $r=\lfloor\log_2(k_s)\rfloor+1$. Suppose that j is a natural number and $\boldsymbol{a}\in\mathbb{F}_2^j$ is fixed. The sequence $\{\mathcal{N}_{\boldsymbol{e}_{[k_1,k_2,\ldots,k_s]}(n)}(\boldsymbol{a})\}$ satisfies the linear recurrence whose characteristic polynomial is given by*

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

Moreover, if $\boldsymbol{a} \neq \mathbf{0}$, then it satisfies the lower order recurrence whose characteristic polynomial is given by

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

Finally, a closed formula is given by

$$\mathcal{N}_{\boldsymbol{e}_{[k_1,k_2,\ldots,k_s]}(n)}(\boldsymbol{a}) = d_0^{neg}(\boldsymbol{a})2^n + \sum_{\ell=1}^{2^r-1} d_\ell^{neg}(\boldsymbol{a})\lambda_\ell^n,$$

where

$$d_\ell^{neg}(\boldsymbol{a}) = \frac{1}{2^{r+1}}\sum_{q=0}^{2^r-1}\left(\sum_{m=0}^{w(\boldsymbol{a})}(-1)^m\binom{w(\boldsymbol{a})}{m}(-1)^{\binom{q+m}{2}+\binom{q+m}{k_1}+\cdots+\binom{q+m}{k_s}}\left((1+i)+(-1)^{q+m}(1-i)\right)\right)\xi_\ell^q,$$

and, as before, $\xi_\ell = e^{\frac{\pi i \ell}{2^{r-1}}}$ and $\lambda_\ell = 1+\xi^{-1}$.

Proof. The idea of the proof is to show that the nega-Hadamard transform can be expressed as a linear combinations of Walsh transforms using some known "tricks" in the theory of Boolean functions. Observe that once this is done, some results from the previous section carry over to the nega-Hadamard transform.

One of the tricks to use is the following congruence of Hamming weights

$$w(\mathbf{x}) \equiv \sum_{j=0}^{k-1}\boldsymbol{e}_{2^j}(\mathbf{x})2^j \mod 2^k, \tag{4.2}$$

where the elementary polynomials $\boldsymbol{e}_{2^j}(\mathbf{X})$ are Boolean, that is, their output is either 0 or 1 [23, Lemma 5]. Observe that this congruence yields

$$\begin{aligned}\mathcal{N}_F(\boldsymbol{a}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{F(\mathbf{x})\oplus\boldsymbol{a}\cdot\mathbf{x}}\, i^{\boldsymbol{e}_1(\mathbf{x})+2\boldsymbol{e}_2(\mathbf{x})}\\ &= \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{F(\mathbf{x})\oplus\boldsymbol{e}_2(\mathbf{x})\oplus\boldsymbol{a}\cdot\mathbf{x}}\, i^{\boldsymbol{e}_1(\mathbf{x})}.\end{aligned}\tag{4.3}$$

Now we use a second trick [23, Lemma 4]. In this case, we use the fact that if b a Boolean variable, then

$$z^b = \frac{1+(-1)^b}{2} + \frac{1-(-1)^b}{2}z. \tag{4.4}$$

This identity leads to

$$\begin{aligned}\mathcal{N}_F(\boldsymbol{a}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{F(\mathbf{x})\oplus\boldsymbol{e}_2(\mathbf{x})\oplus\boldsymbol{a}\cdot\mathbf{x}}\left(\frac{1+(-1)^{\boldsymbol{e}_1(\mathbf{x})}}{2} + \frac{1-(-1)^{\boldsymbol{e}_1(\mathbf{x})}}{2}i\right)\\ &= \frac{1+i}{2}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{F(\mathbf{x})\oplus\boldsymbol{e}_2(\mathbf{x})\oplus\boldsymbol{a}\cdot\mathbf{x}} + \frac{1-i}{2}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{F(\mathbf{x})\oplus\boldsymbol{e}_2(\mathbf{x})\oplus\boldsymbol{e}_1(\mathbf{x})\oplus\boldsymbol{a}\cdot\mathbf{x}}\\ &= \frac{1+i}{2}W_{F\oplus\boldsymbol{e}_2}(\boldsymbol{a}) + \frac{1-i}{2}W_{F\oplus\boldsymbol{e}_2\oplus\boldsymbol{e}_1}(\boldsymbol{a}).\end{aligned}\tag{4.5}$$

Thus, the nega-Hadamard transform can be expressed as a linear combination of two Walsh transforms. Moreover, both of these Walsh transforms involve the original function plus some symmetric Boolean polynomials. Therefore, the results presented in the previous section applies to the nega-Hadamard transform. This takes care of the first two claims. The last claim follows by combining equation (4.5) and the closed formula from Theorem 3.3. This concludes the proof. ☐

We get for free the following corollary.

Corollary 4.2. *Let $F_n(\mathbf{X})$ be a Boolean function that is a linear combinations of terms of the form $R_{j_1,\ldots,j_r}(n)$ and/or the form $\boldsymbol{e}_{k_s}(n)$. Let j be a fixed integer and $\boldsymbol{a}\in\mathbb{F}_2^j$. The sequence $\{\mathcal{N}_{F_n}(\boldsymbol{a})\}_n$ satisfies a linear recurrence with integer coefficients.*

Example 4.3. Consider the Boolean function $\boldsymbol{e}_{[7,4]}(n)$ and the tuple $\boldsymbol{a} = (1, 0, 1)$. Theorem 4.1 implies that $\{\mathcal{N}_{\boldsymbol{e}_{[7,4]}(n)}(\boldsymbol{a})\}_n$ satisfies the linear recurrence whose characteristic polynomial is

$$\Phi_4(X-1)\Phi_8(X-1) = \left(X^2 - 2X + 2\right)\left(X^4 - 4X^3 + 6X^2 - 4X + 2\right).$$

After simplification, the closed formula for $\mathcal{N}_{\boldsymbol{e}_{[7,4]}(n+w(\boldsymbol{a}))}(\boldsymbol{a})$ is given by

$$\begin{aligned}\mathcal{N}_{\boldsymbol{e}_{[7,4]}(n+w(\boldsymbol{a}))}(\boldsymbol{a}) =& \sqrt{2}\left(2+\sqrt{2}\right)^{\frac{n}{2}-1}\sin\left(\frac{\pi n}{8}\right) + \sqrt{2}\left(2-\sqrt{2}\right)^{\frac{n}{2}-1}\sin\left(\frac{3\pi n}{8}\right)\\ &- i\left(2+\sqrt{2}\right)^{\frac{n}{2}-1}\cos\left(\frac{\pi n}{8}\right) - i\left(2-\sqrt{2}\right)^{\frac{n}{2}-1}\cos\left(\frac{3\pi n}{8}\right) - i\,2^{n/2}\cos\left(\frac{\pi n}{4}\right).\end{aligned}$$

Example 4.4. Consider the Boolean function $F_n(\mathbf{X}) = R_{2,3,4}(n)$ and $\boldsymbol{a} = (1, 1, 0)$. The sequences $\{W_{F_n \oplus \boldsymbol{e}_2}(\boldsymbol{a})\}_n$ and $\{W_{F_n \oplus \boldsymbol{e}_2 \oplus \boldsymbol{e}_1}(\boldsymbol{a})\}_n$ both have the same recursive generating set (see Theorem 3.14). The associated matrix for the recursive generating set is a 128×128 matrix and its minimal polynomial is

$$X^{10} - 2X^9 + 2X^8 + 4X^5 - 4X^4 + 4X^2.$$

This implies that $\{\mathcal{N}_{F_n}(\boldsymbol{a})\}_{n\geq 5}$ satisfies the homogeneous linear recurrence with characteristic polynomial

$$X^8 - 2X^7 + 2X^6 + 4X^3 - 4X^2 + 4.$$

Using this recurrence we can obtain the first few values of $\{\mathcal{N}_{F_n}(a)\}_{n\geq 5}$, which are

$$2+2i, -4+8i, -8+12i, -16, -28-20i, -16-40i, 40-64i, 112-64i, 168+40i, 176+256i, 464i, \ldots.$$

The polynomial $q(X) = X^8 - 2X^7 + 2X^6 + 4X^3 - 4X^2 + 4$ is irreducible in $\mathbb{Z}[X]$. This means that this recurrence is the minimal homogeneous linear recurrence with integer coefficients satisfied by $\{\mathcal{N}_{F_n}(\boldsymbol{a})\}_{n\geq 5}$. However, the values of $\{\mathcal{N}_{F_n}(\boldsymbol{a})\}_{n\geq 5}$ lie in $\mathbb{Z}[i]$, thus it is more natural to consider recurrences over $\mathbb{Z}[i]$. But if the coefficients of the linear recurrence are allowed to be Gaussian integers, then the recurrence we just found might not be minimal. However, the characteristic polynomial of the minimal recurrence must be a factor of $q(X)$ in $\mathbb{Z}[i][X]$. Indeed, the minimal homogeneous linear recurrence with Gaussian integer coefficients satisfied by $\{\mathcal{N}_{F_n}(\boldsymbol{a})\}_{n\geq 5}$ has characteristic polynomial $X^4-(1-i)X^3-2iX^2+2X+2i$. Observe that $q(X) = \left(X^4 - (1+i)X^3 + 2iX^2 + 2X - 2i\right)\left(X^4 - (1-i)X^3 - 2iX^2 + 2X + 2i\right)$.

In the next section, we show that these results can be extended further to some generalizations of Walsh transform.

5. Other generalizations

One of the reasons that Boolean functions are important in Information Theory is the fact that every information encoded in a computer can be reduced to a sequence of 0's and 1's (bits). However, as we all well know, the output of a Boolean function is either 0 or 1. Thus, we could say that Boolean functions "take care" of one bit at the time. In this section, we consider generalized Boolean functions $F : \mathbb{F}_2^n \to \mathbb{Z}_{2^\ell}$, that is, functions from the vector space $\mathbb{F}_2^n$ to the ring of integers modulo 2^ℓ. These functions consider ℓ bits at the same time.

The concept of Walsh transform can be generalized for this type of functions. Let ζ_{2^ℓ} be a primitive 2^ℓ-th root of unity. We define the generalized Walsh transform of F as

$$W_{F;\ell}(\boldsymbol{a}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta_{2^\ell}^{F(\mathbf{x})}(-1)^{\boldsymbol{a}\cdot\mathbf{x}}.$$

Observe that $W_{F;1}(\boldsymbol{a}) = W_F(\boldsymbol{a})$, thus $W_{F;\ell}$ is indeed a generalization of the Walsh transform. Moreover, $W_{F;\ell}$ is invertible.

Any element of $\mathbb{Z}_{2^\ell}$ can be identified with an expression of the form

$$b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + \cdots + b_{\ell-1} \cdot 2^{\ell-1},$$

where $b_j \in \mathbb{F}_2$. This means that any function $F : \mathbb{F}_2^n \to \mathbb{Z}_{2^\ell}$ can be expressed in the form

$$F(\mathbf{X}) = b_0(\mathbf{X}) + b_1(\mathbf{X}) \cdot 2 + b_2(\mathbf{X}) \cdot 2^2 + \cdots + b_{\ell-1}(\mathbf{X}) \cdot 2^{\ell-1},$$

where $b_j(\mathbf{X}) \in \mathcal{B}_n$. Thus, using this identification, the generalized Walsh transform can be expressed as

$$W_{F;\ell}(\boldsymbol{a}) \quad = \quad \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\boldsymbol{a}\cdot\mathbf{x}} \prod_{j=0}^{\ell-1} \zeta_{2^\ell}^{2^j b_j(\mathbf{x})} = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\boldsymbol{a}\cdot\mathbf{x}} \prod_{j=0}^{\ell-1} \zeta_{2^{\ell-j}}^{b_j(\mathbf{x})}. \tag{5.1}$$

This expression for the generalized Walsh transform can be used to express $W_{F;\ell}(\boldsymbol{a})$ as a linear combination of regular Walsh transforms. We briefly repeat an argument of [29] (with slight changes). Observe that equation (4.4) implies

$$\begin{aligned}
W_{F;\ell}(\boldsymbol{a}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\boldsymbol{a}\cdot\mathbf{x}} \prod_{j=0}^{\ell-1} \zeta_{2^{\ell-j}}^{b_j(\mathbf{x})} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\boldsymbol{a}\cdot\mathbf{x}} \prod_{j=0}^{\ell-1} \left(\frac{1+(-1)^{b_j(\mathbf{x})}}{2} + \frac{1-(-1)^{b_j(\mathbf{x})}}{2} \zeta_{2^{\ell-j}} \right) \\
&= c_{\ell-1}(\boldsymbol{a}) \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{b_{\ell-1}(\mathbf{x})\oplus\boldsymbol{a}\cdot\mathbf{x}} + \sum_{j=0}^{\ell-2} c_{\ell-1,j}(\boldsymbol{a}) \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{b_{\ell-1}(\mathbf{x})\oplus b_j(\mathbf{x})\oplus\boldsymbol{a}\cdot\mathbf{x}} \\
&+ \sum_{j_1<j_2<\ell-1} c_{\ell-1,j_1,j_2}(\boldsymbol{a}) \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{b_{\ell-1}(\mathbf{x})\oplus b_{j_1}(\mathbf{x})\oplus b_{j_2}(\mathbf{x})\oplus\boldsymbol{a}\cdot\mathbf{x}} \\
&+ \cdots + c_{\ell-1,0,1,\ldots,\ell-2}(\boldsymbol{a}) \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{b_{\ell-1}(\mathbf{x})\oplus\boldsymbol{a}\cdot\mathbf{x}\bigoplus_{j=0}^{\ell-2} b_j(\mathbf{x})} \\
&= c_{\ell-1}(\boldsymbol{a}) W_{b_\ell}(\boldsymbol{a}) + \sum_{j=0}^{\ell-2} c_{\ell-1,j}(\boldsymbol{a}) W_{b_\ell\oplus b_j}(\boldsymbol{a}) + \sum_{j_1<j_2<\ell-1} c_{\ell-1,j_1,j_2}(\boldsymbol{a}) W_{b_\ell\oplus b_{j_1}\oplus b_{j_2}}(\boldsymbol{a}) \\
&+ \cdots + c_{\ell-1,0,1,\ldots,\ell-2}(\boldsymbol{a}) W_{b_\ell\oplus b_0\oplus b_1\oplus\cdots\oplus b_{\ell-2}}(\boldsymbol{a}).
\end{aligned} \tag{5.2}$$

Equation (5.2) implies that, as in the case of the nega-Hadamard transform, all the results about linear recurrences of Walsh transforms carry over to generalized Walsh transforms. In particular, we have the following results.

Theorem 5.1. *Let $\ell > 0$ be an integer. Suppose that $F : \mathbb{F}_2^n \to \mathbb{Z}_{2^\ell}$ is such that*

$$F_n(\mathbf{X}) = b_0(\mathbf{X}) + b_1(\mathbf{X}) \cdot 2 + b_2(\mathbf{X}) \cdot 2^2 + \cdots + b_{\ell-1}(\mathbf{X}) \cdot 2^{\ell-1}$$

where $b_t(\mathbf{X}) \in \mathcal{B}_n$ is such that

$$b_t(\mathbf{X}) = \boldsymbol{e}_{[k_1^{(t)},k_2^{(t)},\ldots,k_{s_t}^{(t)}]}(n),$$

and $0 \le k_1^{(t)} < k_2^{(t)} < \cdots < k_{s_t}^{(t)}$ are integers. Let $K = \max\{k_{s_t}^{(t)} : 0 \le t \le \ell-1\}$ and $r = \lfloor \log_2(K) \rfloor + 1$. Suppose that j is a fixed natural number and $\boldsymbol{a} \in \mathbb{F}_2^j$. Then, the sequence $\{W_{F_n;\ell}(\boldsymbol{a})\}_n$ satisfies the linear recurrence whose characteristic polynomial is given by

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

In particular, if $\boldsymbol{a} \neq \mathbf{0}$, then it satisfies the lower order recurrence whose characteristic polynomial is given by

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

Theorem 5.2. *Let $F_n : \mathbb{F}_2^n \to \mathbb{Z}_{2^\ell}$ be such that its components are linear combinations of terms of the form $R_{j_1,\ldots,j_r}(n)$ and/or the form $\boldsymbol{e}_{k_s}(n)$. Let j be a fixed integer and $\boldsymbol{a} \in \mathbb{F}_2^j$. The sequence $\{W_{F_n;\ell}(\boldsymbol{a})\}_n$ satisfies a linear recurrence with integer coefficients. Moreover, if $q_{\ell-1,j_1,j_2,\ldots,j_t}(X)$ is the characteristic polynomial associated to the minimal homogeneous linear recurrence with integer coefficients satisfied by $\{W_{b_{\ell-1}\oplus b_{j_1}\oplus b_{j_2}\oplus\cdots\oplus b_{j_t}}(\boldsymbol{a})\}_n$, then $\{W_{F_n;\ell}(\boldsymbol{a})\}_n$ satisfies the homogeneous linear recurrence whose characteristic polynomial is*

$$\operatorname{lcm}(q_{\ell-1,j_1,j_2,\ldots,j_t}(X)).$$

Equation (5.2) tells us more. Observe that if $F(\mathbf{X}) = b_0(\mathbf{X}) + b_1(\mathbf{X}) \cdot 2 + b_2(\mathbf{X}) \cdot 2^2 + \cdots + b_{\ell-1}(\mathbf{X}) \cdot 2^{\ell-1}$, then the $\ell-1$ component, that is, $b_{\ell-1}(\mathbf{X})$, dominates the behavior of $\{W_{F;\ell}(\boldsymbol{a})\}_n$ in the sense that it appears in every Walsh transform on the right hand side of (5.2). In particular, we have the following corollary.

Corollary 5.3. *Let $F_n : \mathbb{F}_2^n \to \mathbb{Z}_{2^\ell}$ be such that $F(\mathbf{X}) = b_0(\mathbf{X}) + b_1(\mathbf{X}) \cdot 2 + b_2(\mathbf{X}) \cdot 2^2 + \cdots + b_{\ell-1}(\mathbf{X}) \cdot 2^{\ell-1}$ and its components $b_t(\mathbf{X})$ are linear combinations of terms of the form $R_{j_1,\ldots,j_r}(n)$ and/or the form $\boldsymbol{e}_{k_s}(n)$. Let j be a fixed integer and $\boldsymbol{a} \in \mathbb{F}_2^j$. Let $q(X)$ and $q_{\ell-1}(X)$ be the characteristic polynomial associated to the minimal homogeneous linear recurrences satisfied by $\{W_{F;\ell}(\boldsymbol{a})\}_n$ and $\{W_{b_{\ell-1}}(\boldsymbol{a})\}_n$, respectively. Then,*

$$q_{\ell-1}(X) \,|\, q(X).$$

Example 5.4. Consider the function $F_n : \mathbb{F}_2^n \to \mathbb{Z}_4$ given by $F_n(\mathbf{X}) = \boldsymbol{e}_2(n) + R_{2,3}(n) \cdot 2$. Let $\boldsymbol{a} = (0,1,1)$. In this case,

$$W_{F_n;2}(\boldsymbol{a}) = \frac{1+i}{2} W_{R_{2,3}(n)}(\boldsymbol{a}) + \frac{1-i}{2} W_{R_{2,3}(n) \oplus \boldsymbol{e}_2(n)}(\boldsymbol{a})$$

The characteristic polynomial associated to the minimal linear recurrence satisfied by $\{W_{R_{2,3}(n)}(\boldsymbol{a})\}_n$ is given by

$$X^3 - 2X - 2,$$

while the characteristic polynomial associated to $\{W_{R_{2,3}(n) \oplus \boldsymbol{e}_2(n)}(\boldsymbol{a})\}_n$ is

$$X^6 - 2X^5 + 2X^4 + 4. \tag{5.3}$$

Theorem 5.2 implies that $\{W_{F_n;2}(\boldsymbol{a})\}_n$ satisfies the linear recurrence with characteristic polynomial given by

$$\operatorname{lcm}(X^3 - 2X - 2, X^6 - 2X^5 + 2X^4 + 4) = (X^3 - 2X - 2)(X^6 - 2X^5 + 2X^4 + 4).$$

On the other hand, consider the function $G_n : \mathbb{F}_2^n \to \mathbb{Z}_4$ given by $G_n(\mathbf{X}) = R_{2,3}(n) + \boldsymbol{e}_2(n) \cdot 2$. The function $G_n(\mathbf{X})$ is very similar to $F_n(\mathbf{X})$, with the only difference being that the roles of the first and second components are interchanged. Again, let $\boldsymbol{a} = (0,1,1)$. Observe that the characteristic polynomial associated to the minimal linear recurrence satisfied by $\{W_{\boldsymbol{e}_2(n)}(\boldsymbol{a})\}$ is given by

$$X^2 - 2X + 2,$$

while the one for $\{W_{\boldsymbol{e}_2(n) \oplus R_{2,3}(n)}(\boldsymbol{a})\}_n$ is (5.3). This implies that $\{W_{G_n;2}(\boldsymbol{a})\}$ satisfies the linear recurrence with characteristic polynomial given by

$$\operatorname{lcm}(X^2 - 2X + 2, X^6 - 2X^5 + 2X^4 + 4) = (X^2 - 2X + 2)(X^6 - 2X^5 + 2X^4 + 4).$$

Example 5.5. Consider now the Boolean function $F_n : \mathbb{F}_2^n \to \mathbb{Z}_4$ given by $F_n(\mathbf{X}) = \boldsymbol{e}_3(n) + \boldsymbol{e}_5(n) \cdot 2$. Let $\boldsymbol{a} = (0,1,1)$ Observe that $K = \max\{3,5\} = 5$, thus Theorem 5.1 tell us that $\{W_{F_n;2}(\boldsymbol{a})\}_n$ satisfies the linear recurrence whose characteristic polynomial is

$$\Phi_4(X-1)\Phi_8(X-1) = X^6 - 6X^5 + 16X^4 - 24X^3 + 22X^2 - 12X + 4.$$

Of course, this might not be the minimal homogeneous linear recurrence with integer coefficients satisfied by $\{W_{F_n;2}(\boldsymbol{a})\}_n$, however, Corollary 5.3 tell us that the minimal of such recurrence has characteristic polynomial divisible by the characteristic polynomial associated to the sequence $\{W_{\boldsymbol{e}_5(n);2}(\boldsymbol{a})\}_n$, which is $\Phi_8(X-1)$. Indeed, the polynomial

$$\Phi_8(X-1) = X^4 - 4X^3 + 6X^2 - 4X + 2$$

is the characteristic polynomial associated to the minimal linear recurrence with integer coefficients satisfied by $\{W_{F_n;2}(\boldsymbol{a})\}_n$. Moreover, if Gaussian integers are allowed as coefficients of the linear recurrence, then the minimal recurrence has characteristic polynomial

$$X^2 - 2X + (1-i),$$

which is a factor of $\Phi_8(X-1)$ in $\mathbb{Z}[i]$.

Consider now the function $G_n : \mathbb{F}_2^n \to \mathbb{Z}_4$ given by $G_n(\mathbf{X}) = \boldsymbol{e}_5(n) + \boldsymbol{e}_3(n) \cdot 2$. As in the previous example, the function $G_n(\mathbf{X})$ is very similar to $F_n(\mathbf{X})$, with the only difference being that the roles of the first and second components are interchanged. Again, Theorem 5.1 tell us that $\{W_{G_n;2}(\boldsymbol{a})\}_n$ satisfies the linear recurrence whose characteristic polynomial is

$$\Phi_4(X-1)\Phi_8(X-1) = X^6 - 6X^5 + 16X^4 - 24X^3 + 22X^2 - 12X + 4.$$

This recurrence turns out to be minimal over both $\mathbb{Z}$ and $\mathbb{Z}[i]$.

Finally, we point out that nega-Hadamard transform can also be generalized. As in the case of the generalized Walsh transform, consider a function $F : \mathbb{F}_2^n \to \mathbb{Z}_{2^\ell}$. Also, as before, let ζ_{2^ℓ} be a primitive 2^ℓ-th root of unity. We define the *generalized nega-Hadamard transform* of F as

$$\mathcal{N}_{F;\ell}(\boldsymbol{a}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{F(\mathbf{x})+\boldsymbol{a}\cdot\mathbf{x}} \zeta_{2^\ell}^{w(\mathbf{x})}.$$

Observe that $\mathcal{N}_{F;2}(\boldsymbol{a}) = \mathcal{N}_F(\boldsymbol{a})$. Congruence (4.2) and equation (4.4) can be used to express the generalized nega-Hadamard transform as a linear combination of Walsh transforms. Therefore, all the results discussed through out the article carry over to this transform.

6. Concluding remarks

In this work we developed techniques that generalized previous work on the subject. In particular, we presented a method for finding recurrence relations for Walsh transformations of symmetric and rotation symmetric Boolean functions. We also extended this result to some generalizations of Walsh transformations (the nega-Hadamard transform being one of them). In the particular case of symmetric Boolean functions, we provided a closed formula for the Walsh and nega-Hadamard transformations of these functions. We also showed how the results discussed in this paper could be used to obtain information about the asymptotic behavior of these transformations. It would be interesting if the expert readers in the field find useful applications to our results.

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

[3] A. Canteaut and M. Videau. Symmetric Boolean Functions. *IEEE Trans. on Inform. Theory* **51** (2005), 2791–2811.

[4] F. N. Castro, R. Chapman, L. A. Medina, and L. B. Sepúlveda. Recursions associated to trapezoid, symmetric and rotation symmetric functions over Galois fields. arXiv:1702.08038, 2017.

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

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

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

[8] K. Conrad. Roots on a circle. *Expository note available at* `http://www.math.uconn.edu/ kconrad/blurbs/`.

[9] T. W. Cusick. Weight recursions for any rotation symmetric Boolean functions. arXiv:1701.06648 [math.CO]

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

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

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

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

[14] 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.

[15] E. Filiol, C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation immunity. In: *Eurocrypt* 1998, LNCS **1403**, Springer, Berlin, 1998, pp. 475–488.

[16] 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.

[17] 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.

[18] Q. Meng, L. Chen, F.-W. Fu. On homogeneous rotation symmetric bent functions. *Discr. Appl. Math.* **158** (2010), 1111–1117.

[19] M.G. Parker and A. Pott. On Boolean functions which are bent and negabent. In: Golomb, S.W., Gong, G., Helleseth, T., Song, H.-Y. (eds.) SSC 2007. LNCS 4893, 9–23. Springer, Heidelberg, 2007.

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

[21] C. Riera and M. G. Parker. Generalized bent criteria for Boolean functions. *IEEE Trans. Inform. Theory*, **52:9** (2006), 4142–4159.

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

[23] P. Stănică. Weak and strong 2^k-bent functions. *IEEE Trans. Inform. Theory* **62:5** (2016), 2827–2835.

[24] P. Stănică. On the nonexistence of homogeneous rotation symmetric bent Boolean functions of degree greater than two. *Proc. NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security*, IOS Press, Amsterdam (2008), 214–218.

[25] P. Stănică, P., S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay, S. Maitra. Nega–Hadamard Transform, Bent and Negabent Functions. In: Carlet C., Pott A. (eds) Sequences and Their Applications – SETA 2010. LNCS 6338, Springer, Berlin, Heidelberg, 2010.

[26] P. Stănică, P., S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay, S. Maitra. Investigations on bent and negabent functions via nega-Hadamard transform. *IEEE Trans. Inform. Theory* **58 (6)** (2012) 4064–4072.

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

[28] 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.

[29] P. Stănică, T. Martinsen, S. Gangopadhyay, B. Kumar Singh. Bent and Generalized Bent Boolean Functions. *Designs, Codes and Cryptography* **69:1** (2013), 77–94.

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

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