WALSH-HADAMARD TRANSFORMS OF GENERALIZED p-ARY FUNCTIONS AND C-FINITE SEQUENCES

LUIS A. MEDINA, L. BREHSNER SEPÚLVEDA, AND CÉSAR A. SERNA-RAPELLO

Abstract. In this article we show that Walsh-Hadamard transformations of generalized p-ary functions whose components are symmetric, rotation symmetric or a combination or concatenation of them are C-finite sequences. This result generalized many of the known results for regular p-ary functions. We also present a study of the roots of the characteristic polynomials related to these sequences and show that properties like balancedness and being bent are not shared by the underline p-ary functions.

1. Introduction

An n-variable Boolean function is a map from $\mathbb{F}_2^n \to \mathbb{F}_2$ where $\mathbb{F}_2$ represents the field of two elements. The set of all n-variable Boolean functions is usually denoted by $\mathcal{B}_n$. This branch of combinatorics have applications to different scientific fields including coding theory, cryptography, game theory and information theory.

Every Boolean function $f \in \mathcal{B}_n$ can be identified with a multi-variable polynomial

$$f(X_1, \ldots, X_n) = \bigoplus_{\boldsymbol{a}=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \lambda_{\boldsymbol{a}} \prod_{j=1}^{n} X_j^{a_j}, \tag{1.1}$$

where $\lambda_{\boldsymbol{a}} \in \mathbb{F}_2$ for every $\boldsymbol{a} \in \mathbb{F}_2^n$ and $\oplus$ represents addition mod 2. This polynomial is known as the *algebraic normal form* (or ANF for short) of the Boolean function f. The *algebraic degree* of $f \in \mathcal{B}_n$ is the degree of its ANF.

The *Hamming weight* of a vector $\mathbf{x} \in \mathbb{F}_2^n$, denoted by $wt(\mathbf{x})$, is the number of its entries that are equal to 1. Order the elements of the vector space $\mathbb{F}_2^n$ in lexicographical order. Let $\mathbf{x}_0 = (0, 0, \ldots, 0, 0), \mathbf{x}_1 = (0, 0, \ldots, 0, 1), \mathbf{x}_2 = (0, 0, \ldots, 1, 0), \ldots, \mathbf{x}_{2^n-1} = (1, 1, \ldots, 1, 1)$. The *truth table* of $f \in \mathcal{B}_n$ is the vector $[f(\mathbf{x}_0), f(\mathbf{x}_1), \ldots, f(\mathbf{x}_{2^n-1})]$. The *weight* (or Hamming weight) of a Boolean function $f \in \mathcal{B}_n$, denoted by $wt(f)$, is the number of 1 in its truth table.

Two properties that are very important in some cryptographic applications are non-linearity and balancedness. The *non-linearity* of a Boolean function $f \in \mathcal{B}_n$ is the distance from f to the set of affine functions in n variables,

$$\mathrm{nl}(f) = \min_{g \text{ affine}} \mathrm{dist}(f, g) \tag{1.2}$$

where $\mathrm{dist}(f, g)$ is the Hamming distance (number of bits where they differ) between f and g. A function $f \in \mathcal{B}_n$ is called *balanced* if the number of zeros and the number of ones in its truth table are the same. This is equivalent to say that the Hamming weight of the function $wt(f)$ is 2^{n-1}.

The non-linearity of a Boolean function $f \in \mathcal{B}_n$ is often studied via Walsh-Hadamard transformations. The (unnormalized) *Walsh-Hadamard transformation* of $f \in \mathcal{B}_n$ at $\boldsymbol{a} \in \mathbb{F}_2^n$ is the real-valued function

$$\mathcal{H}_f(\boldsymbol{a}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus \boldsymbol{a}\cdot\mathbf{x}}. \tag{1.3}$$

The non-linearity of a Boolean function f is related to its Hadamard-Walsh transformation via the equation

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2}\left(\max_{\boldsymbol{a}\in\mathbb{F}_2^n} |\mathcal{H}_f(\boldsymbol{a})|\right). \tag{1.4}$$

Date: June 16, 2020.

2010 *Mathematics Subject Classification.* 05E05, 11T23, 11B50.

Key words and phrases. Walsh-Hadamard transform, rotation functions, trapezoid functions, symmetric functions, exponential sums, linear recurrence, generalized p-ary functions.

Highly non-linear Boolean functions are advantageous in some cryptographic applications. Boolean functions with the highest non-linearity, i.e. $2^{n-1} - 2^{n/2-1}$ (n even), are known as *bent functions*. These functions were introduced in the mid 1970's in [30] . Notice that $f \in \mathcal{B}_n$ is bent if

$$\frac{1}{2^{n/2}} |\mathcal{H}_f(\boldsymbol{a})| = 1 \tag{1.5}$$

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

Balancedness of Boolean functions is usually studied via Hamming weights or via exponential sums. The exponential sum of a Boolean function $f \in \mathcal{B}_n$ is defined as

$$S(f) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x})}. \tag{1.6}$$

Observe that a Boolean function is balanced if and only if $S(f) = 0$. Also, the exponential sum of f coincides with its Hadamard-Walsh transform at $\mathbf{0}$, that is, $S(f) = \mathcal{H}_f(\mathbf{0})$. The Hamming weight of a Boolean function and its exponential sum are linked by the equation

$$wt(f) = 2^{n-1} - \frac{1}{2} S(f). \tag{1.7}$$

For more comprehensive information about Boolean functions, please refer to [1, 3, 16].

Balancedness of special families like symmetric and rotation symmetric Boolean functions has been the subject of several studies [4, 5, 6, 7, 11, 12, 13, 15, 17, 19, 28]. A Boolean function $f \in \mathcal{B}_n$ is called symmetric if it is invariant under the action of the symmetric group S_n of n symbols, that is, if

$$f\left(X_{\sigma(1)}, \ldots, X_{\sigma(n)}\right) = f(X_1, \ldots, X_n)$$

for every $\sigma \in S_n$. On the other hand, a Boolean function $f \in \mathcal{B}_n$ is called rotation symmetric if it is invariant under the action of the cyclic group of C_n of n elements, that is, if

$$f\left(X_{\sigma(1)}, \ldots, X_{\sigma(n)}\right) = f(X_1, \ldots, X_n)$$

for every $\sigma \in C_n$.

It is well-known that ANF of a symmetric Boolean function $f \in \mathcal{B}_n$ has the form

$$f = \boldsymbol{e}_{n,k_1} \oplus \boldsymbol{e}_{n,k_2} \oplus \cdots \oplus \boldsymbol{e}_{n,k_s} \tag{1.8}$$

where $0 \leq k_1 < \cdots < k_s$ are integers and $\boldsymbol{e}_{n,k}$ represents the n-variable elementary symmetric polynomial of degree k. For simplicity, we often use the notation $\boldsymbol{e}_{n,[k_1,\ldots,k_s]}$ to represent the right-hand side of (1.8). It is known that if $0 \leq k_1 < \cdots < k_s$ are fixed integers, then the sequence $\{S(\boldsymbol{e}_{n,[k_1,\ldots,k_s]})\}_n$ satisfies a linear recurrence with constant coefficients [2, 4], in other words, it is a C-finite sequence. To be more specific, the sequence $\{S(\boldsymbol{e}_{n,[k_1,\ldots,k_s]})\}_n$ satisfies the recurrence whose characteristic polynomial is given by

$$(X-2)\Phi_4(X-1)\Phi_8(X-1)\cdots\Phi_{2^r}(X-1), \tag{1.9}$$

where $r = \lfloor \log_2(k_s) \rfloor + 1$ and $\Phi_n(X)$ represents the n-th cyclotomic polynomial. This result was extended to Walsh transformations of symmetric Boolean functions in [7] and to every finite field in [9].

Rotation symmetric Boolean functions were introduced by Pieprzyk and Qu [28] (although, they did appear before in the work of Filiol and Fontaine [18] as idempotents). They 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. Rotation symmetric Boolean functions of the form

$$R_{n,[j_1,\cdots,j_s]} = X_1 X_{j_1} \cdots X_{j_s} \oplus X_2 X_{j_1+1} \cdots X_{j_s+1} \oplus \cdots \oplus X_n X_{j_1-1} \cdots X_{j_s-1}, \tag{1.10}$$

where none of the terms overlap or

$$R_{n,[j_1,\cdots,j_s]} = X_1 X_{j_1} \cdots X_{j_s} \oplus \cdots \oplus X_k X_{j_1+k} \cdots X_{j_s+k} \tag{1.11}$$

where $X_{k+1} X_{j_1+k+1} \cdots X_{j_s+k+1}$ is the first term overlapping one of the previous terms; are called a monomial rotation symmetric Boolean function (the indices are taken modulo n and the complete system of residues mod n is $\{1, 2, \cdots, n\}$) . We say that $R_{n,[j_1,\cdots,j_s]}$ is *long cycle* if the period is n and *short cycle* if the period is a nontrivial divisor of n. The rotation

$$R_{4,[2,3]} = X_1 X_2 X_3 \oplus X_2 X_3 X_4 \oplus X_3 X_4 X_1 \oplus X_4 X_1 X_2$$

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. In [11], T. Cusick proved that, as in the case of symmetric Boolean functions, sequences of weights of rotation symmetric Boolean functions are C-finite. Cusick's result was later generalized to Walsh transformations [7] and to every finite field [8]. In the particular case of [8], their approach introduced an auxiliary function which they called trapezoid function. Let $1 < j_1 < \cdots < j_s$ be postive integers. The function

$$T_{n,[j_1,\ldots,j_k]} = X_1X_{j_1}\cdots X_{j_s} + X_2X_{j_1+1}\cdots X_{j_s+1} + \cdots + X_{n+1-j_s}X_{j_1+n-j_s}\cdots X_{j_{s-1}+n-j_s}X_n, \tag{1.12}$$

is called a *trapezoid function*.

In this article, we generalize these results to some generalizations of Boolean functions. There are various ways on which the concept of a Boolean function can be generalized. One of the most common ones is the concept of a generalized Boolean function. A *generalized Boolean function* in n variables is a function from the vector space $\mathbb{F}_2^n$ to $\mathbb{Z}_m$, where $\mathbb{Z}_m$ represents the integers mod m. The set of all these functions is usually denoted by $\mathcal{GB}_n^{(m)}$. In the case when m is a power of two, that is, when $m = 2^\ell$ for ℓ a positive integer, then we can associate to any $f \in \mathcal{GB}_n^{(2^\ell)}$ a unique sequence of Boolean functions $a_j \in \mathcal{B}_n$, $0 \le j \le \ell - 1$, such that

$$f(\mathbf{X}) = \sum_{j=0}^{\ell-1} a_j(\mathbf{X})2^j.$$

The concept of Hadamard-Walsh transformation can be carried over generalized Boolean functions. If $f \in \mathcal{GB}_n^{(m)}$, then its *generalized Hadamard-Walsh* transformation at $\boldsymbol{a} \in \mathbb{F}_2^n$ is definded as the complex-valued function

$$\mathcal{H}_f^{(m)}(\boldsymbol{a}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \xi_m^{f(\mathbf{x})}(-1)^{\boldsymbol{a}\cdot\mathbf{x}}, \tag{1.13}$$

where $\xi_m = \exp(2\pi i/m)$. The concept of bent function can also be generalized to these functions. We say that $f \in \mathcal{GB}_n^{(m)}$ is a *generalized bent function* if

$$\frac{1}{2^{n/2}}\left|\mathcal{H}_f^{(m)}(\boldsymbol{a})\right| = 1 \tag{1.14}$$

for every $\boldsymbol{a} \in \mathbb{F}_2^n$. Generalized bent functions is the subject of active research [20, 25, 29, 31, 32, 33].

Many cryptographic properties, like correlation immune functions, resilient functions and bent functions have been extended to other finite fields [14, 21, 22, 23, 24]. Let p be a prime and $r > 0$. Let $\mathbb{F}_q$, $q = p^r$, represent the finite field of q elements. A function from the vector space $\mathbb{F}_q^n$ to the field $\mathbb{F}_q$ is called an n-variable q-*ary function*. The set of all n-variable q-ary functions will be denoted by $\mathcal{B}_{n,q}$. As in the case of their binary counterpart, every q-ary function $f \in \mathcal{B}_{n,q}$ can be indentify with a multivariable polynomial known as its *algebraic normal form* (or ANF for short)

$$f(X_1, X_2, \ldots, X_n) = \sum_{\boldsymbol{a}=(a_1,\ldots,a_n)\in\mathbb{F}_p^n} \lambda_{\boldsymbol{a}} \left(\prod_{i=1}^{n} x_i^{a_i}\right), \quad \lambda_{\boldsymbol{a}} \in \mathbb{F}_q. \tag{1.15}$$

In (1.15), addition and multiplication is understood to be made in $\mathbb{F}_q$. The algebraic degree of $f \in \mathcal{B}_{n,q}$ is defined as the degree of the algebraic normal form of f.

The Hadamard-Walsh transform at $\boldsymbol{a} \in \mathbb{F}_q^n$ of an n-variable q-ary function f is given by complex-valued function

$$\mathcal{H}_{f,\mathbb{F}_q}(\boldsymbol{a}) = \sum_{\mathbf{x}\in\mathbb{F}_q^n} \xi_p^{\mathrm{Tr}(f(\mathbf{x})+\boldsymbol{a}\cdot\mathbf{x})}, \tag{1.16}$$

where $\xi_p = \exp(2\pi i/p)$, $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ is the field trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$, and $\boldsymbol{a}\cdot\mathbf{x}$ represents the dot product on $\mathbb{F}_q^n$. A function $f \in \mathcal{B}_{n,q}$ is called *bent* if

$$\frac{1}{q^{n/2}}\left|\mathcal{H}_{f,\mathbb{F}_q}(\boldsymbol{a})\right| = 1 \tag{1.17}$$

for every $\boldsymbol{a} \in \mathbb{F}_q^n$.

The exponential sum of an n-variable q-ary function f is defined as

$$S_{\mathbb{F}_q}(f) = \sum_{\mathbf{x}\in\mathbb{F}_q^n} \xi_p^{\mathrm{Tr}(f(\mathbf{x}))}. \tag{1.18}$$

As in the Boolean case, exponential sums could be used to detect balancedness of these functions. We also have $\mathcal{H}_{f,\mathbb{F}_q}(\mathbf{0}) = S_{\mathbb{F}_q}(f)$. In [9] it was proved that the sequence $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})\}_n$ is C-finite and it satisfies the recurrence whose characteristic polynomial is given by

$$\prod_{a_1=0}^{D-1}\prod_{a_2=0}^{a_1}\cdots\prod_{a_{q-1}=0}^{a_{q-2}}\left(X-\left(1+\xi_D^{a_1}+\cdots+\xi_D^{a_{q-1}}\right)\right), \tag{1.19}$$

where $D = p^{\lfloor \log_p(k)\rfloor+1}$. This is a generalization of (1.9). Recently, the results presented of [9] were used to study the value distribution of elementary symmetric polynomials over finite fields [26].

In this article, we study generalized p-ary functions. A function from $\mathbb{F}_p^n$ to $\mathbb{Z}_m$ is called a *generalized p-ary function*. The set of all n-variable generalized p-ary functions will be denoted by $\mathcal{GB}_{n,p}^{(m)}$. As in the Boolean case, if m is a power of p, that is, if $m = p^\ell$, then for every $f \in \mathcal{GB}^{(p^\ell)}$ there is a unique sequence of p-ary functions $a_j \in \mathcal{B}_{n,p}$, $0 \le j \le \ell-1$, such that

$$f(\mathbf{X}) = \sum_{j=0}^{\ell-1} a_j(\mathbf{X})p^j.$$

The *generalized Walsh transform at* $\boldsymbol{a} \in \mathbb{F}_p^n$ of a generalized p-ary function $f \in \mathcal{GB}_{n,p}^{(m)}$ is given by

$$\mathcal{H}_{f,\mathbb{F}_p}^{(m)}(\boldsymbol{a}) = \sum_{\mathbf{x}\in\mathbb{F}_p^n} \xi_m^{f(\mathbf{x})}\xi_p^{\boldsymbol{a}\cdot\mathbf{x}}, \tag{1.20}$$

where $\xi_m = \exp(2\pi i/m)$. Our main goal is to show that sequences of Walsh transformations of generalized p-ary functions whose components are symmetric, rotation symmetric and combinations or concatenations of them are C-finite sequences. This will generalize all known results in this area to this set of functions.

2. Recursions associated to generalized Walsh-Hadamard transformations over $\mathbb{F}_p$

As mentioned in the introduction, our goal is to show that sequences of Walsh-Hadamard transformations of generalized p-ary functions whose components are either symmetric, rotation symmetric or a combination or concatenation of them, are C-finite sequences. We start with some known results.

In [9], it is shown that the exponential sum $S_{\mathbb{F}_p}(\boldsymbol{e}_{n,k})$ can be written as

$$S_{\mathbb{F}_p}(\boldsymbol{e}_{n,k}) = \sum_{j_1=0}^{D-1}\sum_{j_2=0}^{j_1}\cdots\sum_{j_{q-1}=0}^{j_{p-2}} c_{j_1,j_2,\ldots,j_{q-1}}(k)\left(1+\xi_D^{-j_1}+\cdots+\xi_D^{-j_{q-1}}\right)^n, \tag{2.1}$$

where $D = p^{\lfloor \log_p(k)\rfloor+1}$, $\xi_D = \exp(2\pi i/D)$ and $c_{j_1,j_2,\ldots,j_{q-1}}(k)$ are some constants depending on k. Equation (2.1) is a generalization to the one provided by Cai et al. [2] for the binary field. One of its consequence is the fact that the sequence $\{S_{\mathbb{F}_p f}(\boldsymbol{e}_{n,k})\}_n$ satisfies the recurrence whose characteristic polynomial is given by (1.19).

In [26], it is proved that a formula similar to (2.1) exists for exponential sums of perturbations of the elementary symmetric polynomial $\boldsymbol{e}_{n,k}$ (the only change are the values of the constants $c_{j_1,j_2,\ldots,j_{q-1}}(k)$). Let j be a fixed positive integer and $F(\mathbf{X}) \in \mathbb{F}_p[X_1,\ldots,X_j]$. The function $\boldsymbol{e}_{n,k} + F(\mathbf{X})$ is called a perturbation of $\boldsymbol{e}_{n,k}$. Since $S_{\mathbb{F}_p}(\boldsymbol{e}_{n,k} + F(\mathbf{X}))$ has a formula similar to (2.1), then the sequence $\{S_{\mathbb{F}_p}(\boldsymbol{e}_{n,k} + F(\mathbf{X}))\}$ is C-finite and satisfies the recurrence whose characteristic polynomial is given by (1.19) as well.

The last result can be carried over Walsh-Hadamard transformations in the following manner. We want to study the sequence $\{\mathcal{H}_{\boldsymbol{e}_{n,k}}^{(p)}(\boldsymbol{a})\}_n$. A necessary condition to be able to do that is that the tuple $\boldsymbol{a}$ must be of dimension n. However we want $\boldsymbol{a}$ to be constant. This can be achieved by selecting an initial tuple $\boldsymbol{a}$ of fixed dimension, say $j < n$, and continue right padding zeros to the end of a until its dimension is n. For example, suppose that the initially selected tuple is $\boldsymbol{a} = (0,2,1,3)$. When $n = 5$ we consider the tuple to be

$\boldsymbol{a} = (0, 2, 1, 3, 0)$, when $n = 6$ we consider the tuple $\boldsymbol{a} = (0, 2, 1, 3, 0, 0)$, and so on. Note that this implies, for example, that if $\boldsymbol{a} = (0, 2, 1, 3)$, then

$$\begin{aligned}\mathcal{H}_{\boldsymbol{e}_{n,k},\mathbb{F}_q}(\boldsymbol{a}) &= \sum_{\mathbf{x}\in\mathbb{F}_q^n} \xi_p^{\mathrm{Tr}(\boldsymbol{e}_{n,k}(\mathbf{x})+\boldsymbol{a}\cdot\mathbf{x})} \\ &= \sum_{\mathbf{x}\in\mathbb{F}_q^n} \xi_p^{\mathrm{Tr}(\boldsymbol{e}_{n,k}(\mathbf{x})+2x_2+x_3+3x_4)} \\ &= S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k} + 2X_2 + X_3 + 3X_4).\end{aligned}$$

Therefore, under this assumption on $\boldsymbol{a}$, $\mathcal{H}_{\boldsymbol{e}_{n,k}}(\boldsymbol{a})$ can be viewed as a perturbation of $\boldsymbol{e}_{n,k}$. Thus the sequence $\{\mathcal{H}^{(q)}_{\boldsymbol{e}_{n,k}}(\boldsymbol{a})\}$ is C-finite and satisfies the recurrence whose characteristic polynomial is given by (1.19). A similar argument can be done for rotation symmetric polynomials. There is a difference though, the results from [8] can be used to prove that $\{\mathcal{H}_{R_{n,[j_1,\cdots,j_s]},\mathbb{F}_q}(\boldsymbol{a})\}$ is a C-finite sequence, but cannot be used to give explicit recurrences for them.

Recall that every generalized p-ary function $f \in \mathcal{GB}^{(p^\ell)}_{n,\mathbb{F}_p}$ can be written as

$$f(\mathbf{X}) = a_0(\mathbf{X}) + a_1(\mathbf{X})p + \cdots + a_{\ell-1}(\mathbf{X})p^{\ell-1} \tag{2.2}$$

where $a_j \in \mathcal{B}_{n,p}$. Suppose that Z is an indeterminate and $m, s \in \mathbb{F}_p$. The well-known identity

$$\sum_{j=0}^{p-1} \xi_p^{j(m-s)} = \begin{cases} 0, & s \neq m \\ p, & s = m \end{cases}$$

implies

$$\begin{aligned}\sum_{s=0}^{p-1}\sum_{j=0}^{p-1} \xi_p^{j(m-s)} Z^s &= \sum_{s=0}^{p-1} \left(\sum_{j=0}^{p-1} \xi_p^{j(m-s)} \right) Z^s \\ &= pZ^m.\end{aligned} \tag{2.3}$$

Therefore, if $m \in \mathbb{F}_p$ and Z is an indeterminate, then

$$Z^m = \frac{1}{p} \sum_{s=0}^{p-1}\sum_{j=0}^{p-1} \xi_p^{j(m-s)} Z^s \tag{2.4}$$

Equation (2.4) leads to the following lemma. Before stating the result, we introduce some notations. We denote the list $k_0, \ldots, k_t$ by $[k_t]$. A multiple sum like

$$\sum_{k_0=0}^{m}\sum_{k_1=0}^{m}\cdots\sum_{k_t=0}^{m} a_{k_0,k_1,\ldots,k_t} \tag{2.5}$$

will be denoted by

$$\sum_{[k_t]=0}^{m} a_{[k_t]} \tag{2.6}$$

and a multiple sum like

$$\sum_{k_0=0}^{m}\sum_{k_1=0}^{m}\cdots\sum_{k_t=0}^{m}\sum_{j_0=0}^{m}\sum_{j_1=0}^{m}\cdots\sum_{j_t=0}^{m} a_{k_0,k_1,\ldots,k_t;j_0,j_1,\ldots,j_t} \tag{2.7}$$

by

$$\sum_{[k_t],[j_t]=0}^{m} a_{[k_t];[j_t]}. \tag{2.8}$$

Lemma 2.1. *Let $Z = Z_0 + Z_1 p + \cdots + Z_t p^t$ with Z_j indeterminates, $l > t \geq 0$ and p a prime integer, then*

$$\xi_{p^\ell}^{Z} = \sum_{[j_t],[k_t]=0}^{p-1} \mathcal{C}_{[j_t];[k_t]}(\xi_p)\, \xi_p^{\sum_{m=0}^{t} j_m Z_m}$$

where $\mathcal{C}_{[j_t];[k_t]}(\xi_p) = \frac{1}{p^{t+1}}\left(\prod_{s=0}^{t}\xi_{p^{l-s}}^{k_s}\right)\xi_p^{-\sum_{m=0}^{t} j_m k_m}$

Proof. Observe that $\zeta_{p^\ell}^{Z} = \prod_{s=0}^{t}\zeta_{p^{l-s}}^{Z_s}$. Equation (2.4) implies

$$\begin{aligned}
\xi_{p^\ell}^{Z} &= \prod_{s=0}^{t}\left(\frac{1}{p}\sum_{j_s=0}^{p-1}\sum_{k_s=0}^{p-1}\xi_p^{j_s(Z_s-k_s)}\xi_{p^{l-s}}^{k_s}\right)\\
&= \sum_{[j_t];[k_t]=0}^{p-1}\left(\frac{1}{p^{t+1}}\left(\prod_{s=0}^{t}\xi_{p^{\ell-s}}^{k_s}\right)\xi_p^{-\sum_{m=0}^{t} j_m k_m}\right)\xi_p^{\sum_{m=0}^{t} j_m Z_m}\\
&= \sum_{[j_t];[k_t]=0}^{p-1}\mathcal{C}_{[j_t];[k_t]}(\xi_p)\xi_p^{\sum_{m=0}^{t} j_m Z_m},
\end{aligned}$$

where $\mathcal{C}_{[j_t];[k_t]}(\xi_p) = \frac{1}{p^{t+1}}\left(\prod_{s=0}^{t}\xi_{p^{l-s}}^{k_s}\right)\xi_p^{-\sum_{m=0}^{t} j_m k_m}$. □

The previous lemma implies that the generalized Walsh-Hadamard transform $\mathcal{H}_{f,\mathbb{F}_p}^{(p^\ell)}(\boldsymbol{a})$ of a generalized p-ary function $f \in \mathcal{GB}_{n,\mathbb{F}_p}^{(p^\ell)}$ can be expressed as linear combination of Walsh-Hadamard transform of p-ary functions in $\mathcal{B}_{n,\mathbb{F}_p}$.

Proposition 2.2. *The generalized Walsh-Hadamard transform of a generalized p-ary function*

$$f(\mathbf{X}) = b_0(\mathbf{X}) + b_1(\mathbf{X})p + \cdots + b_{\ell-1}(\mathbf{X})p^{\ell-1},$$

where each $b_j \in \mathcal{B}_{n,\mathbb{F}_p}$, is a linear combination of Walsh-Hadamard transforms of linear combinations of the p-ary functions $b_j(\mathbf{X})$'s.

Proof. Suppose that $f \in \mathcal{GB}_{n,\mathbb{F}_p}^{(p^\ell)}$ has the form

$$f(\mathbf{X}) = b_0(\mathbf{X}) + b_1(\mathbf{X})p + \cdots + b_{\ell-1}(\mathbf{X})p^{\ell-1} \tag{2.9}$$

where $b_j \in \mathcal{B}_{n,\mathbb{F}_p}$, $j = 0, 1, \cdots, \ell-1$. Let $\boldsymbol{a} \in \mathbb{F}_p^n$. Observe that Lemma 2.1 implies

$$\begin{aligned}
\mathcal{H}_{f,\mathbb{F}_p}^{(p^\ell)}(\boldsymbol{a}) &= \sum_{\mathbf{x}\in\mathbb{F}_p^n}\xi_{p^\ell}^{f(\mathbf{x})}\xi_p^{\boldsymbol{a}\cdot\mathbf{x}}\\
&= \sum_{\mathbf{x}\in\mathbb{F}_p^n}\xi_p^{b_{\ell-1}(\mathbf{x})}\xi_{p^\ell}^{b_0(\mathbf{x})+b_1(\mathbf{x})p+\cdots+b_{\ell-2}(\mathbf{x})p^{\ell-2}}\xi_p^{\boldsymbol{a}\cdot\mathbf{x}}\\
&= \sum_{\mathbf{x}\in\mathbb{F}_p^n}\xi_p^{b_{\ell-1}(\mathbf{x})}\left(\sum_{[j_{\ell-2}];[k_{\ell-2}]=0}^{p-1}\mathcal{C}_{[j_{\ell-2}];[k_{\ell-2}]}(\xi_p)\xi_p^{\sum_{m=0}^{\ell-2} j_m b_m(\mathbf{x})}\right)\xi_p^{\boldsymbol{a}\cdot\mathbf{x}}\\
&= \sum_{[j_{\ell-2}];[k_{\ell-2}]=0}^{p-1}\mathcal{C}_{[j_{\ell-2}];[k_{\ell-2}]}(\xi_p)\left(\sum_{\mathbf{x}\in\mathbb{F}_p^n}\xi_p^{b_{\ell-1}(\mathbf{x})+\sum_{m=0}^{\ell-2} j_m b_m(\mathbf{x})+\boldsymbol{a}\cdot\mathbf{x}}\right)\\
&= \sum_{[j_{\ell-2}];[k_{\ell-2}]=0}^{p-1}\mathcal{C}_{[j_{\ell-2}];[k_{\ell-2}]}(\xi_p)\mathcal{H}_{G_{\ell,[j_{\ell-2}]},\mathbb{F}_p}(\boldsymbol{a})
\end{aligned}$$

where $G_{\ell,[j_{\ell-2}]}(\mathbf{X}) = b_{\ell-1}(\mathbf{X}) + \sum_{m=0}^{\ell-2} j_m b_m(\mathbf{X})$ and $\mathcal{C}_{[j_{\ell-2}];[k_{\ell-2}]}(\xi_p)$ as in Lemma 2.1. □

With Proposition 2.2 at hand, we are ready to stay the main result of this section.

Theorem 2.3. *Let p be a prime. Suppose that $f_n \in \mathcal{GB}_{n,\mathbb{F}_p}^{(p^\ell)}$ can be written as*

$$f_n(\mathbf{X}) = b_0(\mathbf{X}) + b_1(\mathbf{X})p + \cdots + b_{\ell-1}(\mathbf{X})p^{\ell-1} \tag{2.10}$$

where each component b_j is symmetric, rotation symmetric or a combination and/or concatenation of them. Suppose that $\boldsymbol{a} \in \mathbb{F}_p^j$ is fixed. Then the sequence $\left\{\mathcal{H}_n^{(p^\ell)}(\boldsymbol{a})\right\}_n$ is C-finite. In the particular case when each $b_j = \boldsymbol{e}_{n,k_j}$, then $\left\{\mathcal{H}_n^{(p^\ell)}(\boldsymbol{a})\right\}_n$ satisfies the recurrence whose characteristic polynomial is given by

$$\prod_{a_1=0}^{D-1} \prod_{a_2=0}^{a_1} \cdots \prod_{a_{p-1}=0}^{a_{p-2}} \left(X - \left(1 + \xi_D^{a_1} + \cdots + \xi_D^{a_{p-1}}\right)\right), \tag{2.11}$$

where $D = p^{\left\lfloor \log_p(\max\{k_0,\ldots,k_{\ell-1}\}) \right\rfloor + 1}$.

Proof. This is a direct application of Proposition 2.2 and the discussion so far. □

Example 2.4. Consider the prime $p = 3$ and the generalized 3-ary function given by $f_n = \boldsymbol{e}_{n,5} + 3R_{n,[2,3]}$. Consider the vector $\boldsymbol{a} = (1, 2, 1)$. Theorem 2.3 tells us that $\left\{\mathcal{H}_{f_n}^{(3^2)}(\boldsymbol{a})\right\}$ is a C-finite sequence.

3. A study of the Walsh-Hadamard transform when $\{H_{f_n,\mathbb{F}_p}(\boldsymbol{a})\}$ is a C-finite sequence

We know that the study of Walsh-Hadamard transforms of generalized p-ary functions $\mathcal{H}_{f,\mathbb{F}_p}^{(p^\ell)}(\boldsymbol{a})$ can be reduced to the study of Walsh-Hadamard transforms of regular p-ary functions. In this section we study sequences of the form $\{\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a})\}$ where $f_n \in \mathcal{B}_{n,p}$. We start with a result about their closed formulas.

Proposition 3.1. *Let p be a prime and $E = \mathbb{Q}(\xi_p)$, where $\xi_p = \exp(2\pi i/p)$ is a p-th primitive root of unity. Let $f_n \in \mathcal{B}_{n,p}$ be a family of p-ary functions. Suppose that for some fixed tuple $\boldsymbol{a}$, the sequence $\left\{\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a})\right\}_n \subseteq E$ satisfies a linear recurrence with integral coefficients in E whose characteristic polynomial is given by $q(X)$. If $q(X)$ is monic and irreducible and $\beta_1, \beta_2, \ldots, \beta_\ell$ are the distinct roots of $q(X)$, then*

$$\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a}) = \sum_{j=1}^{\ell} c_j(\boldsymbol{a})\beta_j^n \tag{3.1}$$

where each $c_j(\boldsymbol{a}) \in E$ is a non-zero constant depending on $\boldsymbol{a}$.

Proof. Since $q(X)$ is irreducible, it does not have repeated roots. Using classic results in the theory of linear recurrences yields

$$\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a}) = \sum_{j=1}^{n} c_j(\boldsymbol{a})\,\beta_j^n \tag{3.2}$$

for some constants $c_j(\boldsymbol{a}) \in E$. It remains to prove that $c_j(\boldsymbol{a}) \neq 0$ for every j.

Let $G = \mathrm{Gal}_E(q(X))$ be the Galois group of the polynomial $q(X) \in E[X]$. Since $q(X)$ is irreducible, we know that G is transitive, that is, for every $i \neq j$ in $\{1, 2, \ldots, \ell\}$, there is a $\sigma \in G$ such that $\sigma(\beta_i) = \beta_j$. We know that $\left\{\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a})\right\}_{n\in\mathbb{N}}$ is a sequence of integral numbers that is not identically zero, which means that there is a $j_0 \in \{1, 2, \ldots, \ell\}$ such that $c_{j_0}(\boldsymbol{a}) \neq 0$. Consider $j_1 \in \{1, 2, \ldots, \ell\}$ with $j_1 \neq j_0$ and let $\sigma_{j_0,j_1} \in G$ be such that $\sigma_{j_0,j_1}(\beta_{j_0}) = \beta_{j_1}$. Apply σ_{j_0,j_1} to equation (3.2) to get

$$\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a}) = \sigma_{j_0,j_1}\left(\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a})\right) = \sum_{j=1}^{n} \sigma_{j_0,j_1}\left(c_j(\boldsymbol{a})\right)\sigma_{j_0,j_1}(\beta_j)^n, \tag{3.3}$$

where we used the fact that $\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a}) \in E$ and so it is fixed by σ_{j_0,j_1}. Equation (3.3) is equation (3.2), but written in different order. However, since $\sigma_{j_0,j_1}(\beta_{j_0}) = \beta_{j_1}$, then

$$c_{j_1}(\boldsymbol{a}) = \sigma_{j_0,j_1}(c_{j_0}(\boldsymbol{a})) \neq 0.$$

This concludes the proof. □

Proposition 3.2 remains true if instead of requiring $q(X)$ to be irreducible, we require it to have a square-free irreducible factorization in $E[X]$. The next result bounds the roots of the characteristic polynomial of the sequence $\left\{\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a})\right\}$.

Theorem 3.2. *Let p be a prime and $E = \mathbb{Q}(\xi_p)$ with $\xi_p = \exp(2\pi i/p)$. Let $f_n \in \mathcal{B}_{n,p}$ be a family of p-ary functions. Suppose that for some fixed tuple $\boldsymbol{a}$, the sequence $\left\{\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a})\right\}_n \subseteq E$, satisfies a linear recurrence with integral coefficients. Let $q(X) \in E[X]$ be the characteristic polynomial of the minimal of such recurrences. Suppose that $q(X)$ has a square-free irreducible factorization in $E[X]$, that is,*

$$q(X) = q_1(X)\cdots q_s(X),$$

where each $q_j(X)$ is irreducible in $E[X]$. Then, every root β of $q(X)$ satisfies $|\beta| \leq p$. Moreover, if each $q_j(X)$ also happens to be in $\mathbb{Q}[X]$ and $\deg(q_j(X)) > 1$, then equality is attained only if there is a j such that $q_j(pX)$ is a palindromic polynomial of even degree.

Proof. Let $\beta_1, \ldots, \beta_\ell$ be the roots of $q(X)$. Suppose that β_1 is the root with the highest modulus. We will prove the first statement by showing that $|\beta_1| > p$ leads to a contradiction.

Suppose first that β_1 is unique with this property, that is, $|\beta_j| < |\beta_1|$ for $j = 2, \ldots, \ell$. We know that

$$\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a}) = \sum_{j=1}^{\ell} c_j(\boldsymbol{a})\beta_j^n,$$

where each $c_j(\boldsymbol{a})$ is a non-zero constant. Thus, as n increases,

$$\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a}) \sim c_1(\boldsymbol{a})\beta_1^n.$$

If it is true that $|\beta_1| > p$, then there is an $n_0 \in \mathbb{N}$ such that for $n > n_0$, we have $|\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a})| > p^n$. This is clearly impossible because the definition of $\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a})$ implies $|\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a})| \leq p^n$. We conclude that $|\beta_1| \leq p$ and so the first statement of the theorem is true in this case.

Suppose now that the highest modulus is achieved on more than one root. Suppose that $\beta_1, \beta_2, \ldots, \beta_t$ are the roots on which the highest modulus is achieved, that is,

$$|\beta_j| < |\beta_1| = |\beta_2| = \cdots = |\beta_t|$$

for $j = t+1, \ldots, \ell$. Write

$$\beta_1 = |\beta_1|e^{2\pi\theta_1}, \quad \beta_2 = |\beta_1|e^{2\pi\theta_2}, \quad \cdots, \quad \beta_t = |\beta_1|e^{2\pi\theta_t},$$

where $\theta_1, \theta_2, \ldots, \theta_t \in [0, 1)$. Then, as n increases,

$$\begin{aligned}\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a}) &\sim c_1(\boldsymbol{a})\beta_1^n + c_2(\boldsymbol{a})\beta_2^n + \cdots + c_t(\boldsymbol{a})\beta_t^n \\ &\sim |\beta_1|^n\left(c_1(\boldsymbol{a})e^{2\pi in\theta_1} + c_2(\boldsymbol{a})e^{2\pi in\theta_2} + \cdots + c_t(\boldsymbol{a})e^{2\pi in\theta_t}\right).\end{aligned}$$

Let $\varepsilon > 0$ and

$$M = \sup\left\{\left|c_1(\boldsymbol{a})e^{2\pi in\theta_1} + c_2(\boldsymbol{a})e^{2\pi in\theta_2} + \cdots + c_t(\boldsymbol{a})e^{2\pi in\theta_t}\right| : n \in \mathbb{N}\right\}.$$

There is a subsequence $\{n_k\}_{k=1}^{\infty}$ of positive integers such that

$$M - \varepsilon < \left|c_1(\boldsymbol{a})e^{2\pi in_k\theta_1} + c_2(\boldsymbol{a})e^{2\pi in_k\theta_2} + \cdots + c_t(\boldsymbol{a})e^{2\pi in\theta_t}\right| \leq M$$

for every k. Therefore,

$$\left|\mathcal{H}_{f_{n_k},\mathbb{F}_p}(\boldsymbol{a})\right| \sim |\beta_1|^n\left|c_1(\boldsymbol{a})e^{2\pi in_k\theta_1} + c_2(\boldsymbol{a})e^{2\pi in_k\theta_2} + \cdots + c_t(\boldsymbol{a})e^{2\pi in\theta_t}\right| > |\beta_1|^{n_k}(M - \varepsilon).$$

If it is true that $|\beta_1| > p$, then there is an $k_0 \in \mathbb{N}$ such that for $k > k_0$, we have $|\mathcal{H}_{f_{n_k},\mathbb{F}_p}(\boldsymbol{a})| > p^n$, which is impossible. Therefore, the first statement is also true for this case and therefore true in general.

We now prove the second statement. Suppose that each $q_j(X)$ also happens to have rational coefficients. Suppose that $|\beta_1| = p$. Then $\beta_1 = pe^{2\pi i\theta}$ for $0 \leq \theta < 1$ and

$$0 = q\left(pe^{2\pi i\theta}\right) = q_1(pe^{2\pi i\theta})\cdots q_s(pe^{2\pi i\theta}).$$

Therefore $e^{2\pi i\theta}$ is a root of one of the polynomials $q_j(pX)$. Suppose that such polynomial is $q_{j_0}(pX)$. Then, $q_{j_0}(pX)$ is irreducible, its degree is bigger than 1 and has a root in the unit circle. But if an irrediculbe polynomial in $\mathbb{Q}[X]$ of degree bigger than 1 has a root in the unit circle, then the polynomial is palindromic of even degree [10, Th. 1.1]. □

Corollary 3.3. *Let p be a prime, $E = \mathbb{Q}(\xi_p)$ and $f_n \in \mathcal{GB}_{n,\mathbb{F}_p}^{(p^\ell)}$ a family of generalized p-ary functions. Suppose that for some fixed tuple $\boldsymbol{a}$ the sequence $\{\mathcal{H}_{f_n,\mathbb{F}_p}^{(p^\ell)}(\boldsymbol{a})\}$ satisfies a linear recurrence with characteristic polynomial $q(X) \in E[X]$. Suppose that $q(X)$ has a square-free irreducible factorization. Then, every root β of $q(X)$ satisfies $|\beta| \leq p$.*

Example 3.4. Consider the sequence $\{\mathcal{H}_{R_{n,[2,3]},\mathbb{F}_3}(\mathbf{0})\}$. In [8] it was showed that this sequence satisfies the recurrence whose characteristic polynomial is given by

$$X^6 - 3X^4 - 9X^3 + 9X + 18 = \left(X^3 - 3\right)\left(X^3 - 3X - 6\right).$$

This polynomial has a unique root β with the highest modulus. This root satisfies $|\beta| \approx 2.355301397608$, which is less than or equal to 3, as predicted.

Example 3.5. Consider now the sequence $\{\mathcal{H}_{\boldsymbol{e}_{n,3},\mathbb{F}_5}(\boldsymbol{a})\}$ where $\boldsymbol{a} = (1, 0, 2)$. This sequence satisfies the recurrence whose characteristic polynomial is given by

$$m(X) = \left(X^2 - 5\right)\left(X^2 - 5X + 5\right)\left(X^4 + 10X^2 + 25X + 25\right)\left(X^4 - 5X^3 + 15X^2 - 25X + 25\right).$$

This polynomial is a proper divisor of

$$\prod_{a_1=0}^{4}\prod_{a_2=0}^{a_1}\prod_{a_3=0}^{a_2}\prod_{a_4=0}^{a_3}(X - (1 + \xi_5^{a_1} + \xi_5^{a_2} + \xi_5^{a_3} + \xi_5^{a_4})).$$

The highest modulus of the roots of $m(X)$ occurs at varios roots and it is approximately equal to 3.618033989. This value is less than or equal to 5, as predicted by our theorem.

One consequence of the above theorem is that if $f_n \in \mathcal{B}_{n,p}$ is a family of p-ary functions such that for some fixed tuple $\boldsymbol{a}$ the sequence $\{\mathcal{H}_{f_n}(\boldsymbol{a})\}_n$ satisfies a linear recurrence with integral coefficients in $E = \mathbb{Q}(\xi)$, then the limit

$$\lim_{n\to\infty} \frac{1}{p^n}\left|\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a})\right| \tag{3.4}$$

is 0 most of the time. Therefore, the idea presented in [4] about using the limit

$$\lim_{n\to\infty} \frac{1}{2^n} S(\boldsymbol{e}_{n,k}) = \lim_{n\to\infty} \frac{1}{2^n} \mathcal{H}_{\boldsymbol{e}_{n,k}}(\mathbf{0}), \tag{3.5}$$

to prove that when k is not a power of two the elementary symmetric Boolean polynomial $\boldsymbol{e}_{n,k}$ is not balanced for n sufficiently big does not carry over very well for general p-ary functions. Some adjustments can be made, but they depend on the particular characteristic polynomial of the sequence. For example, suppose that $q(X)$ is the characteristic polynomial associated to $\{\mathcal{H}_{f_n}(\mathbf{0})\}_n$. Moreover, suppose that it is irreducible on $E = \mathbb{Q}(\xi_p)$. Then,

$$\mathcal{H}_{f_n}(\mathbf{0}) = \sum_{\alpha:\, q(\alpha)=0} c_\alpha\, \alpha^n$$

where c_α is a non-zero constant for each α. If $q(X)$ has root β such that $|\alpha| < \beta$ for α any other root different than β, then the limit

$$\lim_{n\to\infty} \frac{1}{|\beta|^n}\left|\mathcal{H}_{f_n,\mathbb{F}_p}(\mathbf{0})\right| = |c_\beta| \neq 0$$

and therefore, the p-ary function f_n is not balanced for all sufficiently large n. The same argument works if the irreducibility of the characteristic polynomial $q(X)$ is relaxed to having a square-free irreducible factorization. The polynomial in Example 3.4 is an example of a polynomial with a squarefree fractorization and with a unique root of maximum modulus. Therefore, $R_{n,[2,3]}$ is not balanced over $\mathbb{F}_3$ for all sufficiently large n.

Let us study the characteristic polynomial of $\{\mathcal{H}_{R_{n,[2,3]},\mathbb{F}_3}(\mathbf{0})\}$ in more detail. The characteristic polynomial is given by

$$X^6 - 3X^4 - 9X^3 + 9X + 18 = \left(X^3 - 3\right)\left(X^3 - 3X - 6\right).$$

Out of all its roots, the one with the biggest modulus is a root of the factor X^3-3X-6. This factor belongs to the following family of polynomials. Let p be a prime and $q=p^\ell$. Define $Q_{k,q}(X)$ by

$$Q_{k,q}(X)=X^k-q\sum_{j=0}^{k-2}(q-1)^jX^{k-2-j}. \tag{3.6}$$

Observe that $Q_{3,3}(X)=X^3-3X-6$. The polynomial (3.6) appeared in the study of $S_{\mathbb{F}_q}(R_{n,[2,3,\cdots,k]})$. In particular, it is the characteristic polynomial of the minimal recurrence of $S_{\mathbb{F}_q}(T_{n,[2,3,\cdots,k]})$, where $T_{n,[2,3,\cdots,k]})$ is the trapezoid function associated to the rotation $R_{n,[2,3,\cdots,k]}$. Trapezoid functions are very interesting objects and seems to have some special properties. For example, the function $T_{4,[2]}=X_1X_2+X_2X_3+X_3X_4$ is known to be bent and negabent Boolean function [27].

The polynomial $Q_{k,q}(X)$ is very interesting. It has a unique positive real root and such root has the biggest modulus among all its roots. That is a consequence of Ostrovsky's Theorem.

Theorem 3.6 (Ostrovsky)**.** *Let $f(X)=X^n-b_1X^{n-1}-\cdots-b_n$, where all the numbers b_i are non-negative and at least one of the them is nonzero. If the greatest common divisor of the indices of the positive integers b_i is equal to 1, then f has a unique positive root α and the absolute value of the other roots (they may be complex) are less than α.*

The polynomial $Q_{k,q}(X)$ also appears to be irreducible over $\mathbb{Q}$ for every k and q. If $q=p$, then the polynomial $Q_{k,p}(X)$ is irreducible over $\mathbb{Q}$ by Eisenstein Criterion. However, in our study, we are interested in irreducibility over $E=\mathbb{Q}(\xi_p)$. The irreducibiliy of $Q_{k,p}(X)$ over E is discussed next and it depends on the Eisenstein-Dumas criterion.

Theorem 3.7 (Eisenstein-Dumas criterion)**.** *Let R be a unique factorization domain and*

$$f(x)=a_0+a_1X+\cdots+a_nX^n\in R[X]$$

with $a_0a_n\neq 0$. Assume that $f(X)$ is primitive, i.e. $\gcd(a_0,\cdots,a_n)=1$. If the Newton polygon of $f(X)$ with respect to some prime $p\in R$ consists of only the line segment from $(0,m)$ to $(n,0)$ and $gcd(n,m)=1$, then $f(X)$ is irreducible in $R[X]$.

Theorem 3.8. *Let p be a prime, $k\geq 2$ an integer and $E=\mathbb{Q}(\xi_p)$. If $\gcd(p-1,k)=1$, then $Q_{k,p}(X)$ is irreducible over E.*

Proof. The ring of integers of E is $R=\mathbb{Z}[\xi_p]$ (the ring R is a Dedekind domain). The ideal $(1-\xi_p)$ is a prime ideal of $\mathbb{Z}[\xi_p]$ and $(p)=(1-\xi_p)^{p-1}$, thus $\pi=1-\xi_p$ is a prime in $\mathbb{Z}[\xi_p]$ and p is totally ramified in E.

Let ν_π denote the valuation corresponding to the ideal (π). Then, $\nu_\pi(p)=\nu_\pi(p(p-1)^j)=p-1$. Therefore, the Newton polygon of $Q_{k,p}(X)$ with respect to π consists of only the line segment from $(0,p-1)$ to $(k,0)$. By hypothesis, $\gcd(p-1,k)=1$. Therefore, the Eisenstein-Dumas criterion implies that $f(X)$ is irreducible in $R[X]$ and therefore in $E[X]$. □

Combining the fact that $Q_{k,p}(X)$ has a unique positive root β and every other root of $Q_{k,p}(X)$ has absolute value less than β with the fact that $Q_{k,p}(X)$ is irreducible over E when $\gcd(k,p-1)=1$ implies that $T_{n,[2,3,\cdots,k]}$ is not balanced over $\mathbb{F}_p$ for n sufficiently large when $\gcd(p-1,k)=1$. We also have the following result.

Theorem 3.9. *Let p be an odd prime and $k>2$ an integer such that $\gcd(k,p-1)=1$. Then, for all sufficiently large n, the p-ary trapezoid function $T_{n,[2,\cdots,k]}$ is not bent over $\mathbb{F}_p$.*

Proof. We know that $Q_{k,p}(X)$ is irreducible over $E=\mathbb{Q}(\xi_p)$, therefore, if $\beta_1,\cdots,\beta_k$ are the roots of $Q_{k,p}(X)$, then

$$\mathcal{H}_{T_{n,[2,\cdots,k]},\mathbb{F}_p}(\mathbf{0})=\sum_{j=1}^{k}c_j(\mathbf{0})\beta_j^j$$

where each $c_j(\mathbf{0})\neq 0$. Let β_1 be the unique positive root of $Q_{k,p}(X)$ of Ostrovsky's Theorem. Then $|\beta_j|<\beta_1$ for $j=2,\cdots,k$ and so

$$\lim_{n\to\infty}\frac{1}{\beta_1^n}\left|\mathcal{H}_{T_{n,[2,\cdots,k]},\mathbb{F}_p}(\mathbf{0})\right|=|c_1(\mathbf{0})|\neq 0. \tag{3.7}$$

Now observe that

$$Q_{k,p}(\sqrt{p}) = \frac{(p-1)p^{k/2} - p(p-1)^{k-1}}{p - \sqrt{p} - 1}.$$

Our hypothesis on p and k imply that this value is a negative number. Also observe that

$$Q_{k,p}(p) = p(p-1)^{k-1}$$

is a positive number. Therefore, the unique positive root β_1 satisfies $\beta_1 > \sqrt{p}$. But then,

$$\left|\mathcal{H}_{T_{n,[2,\cdots,k]},\mathbb{F}_p}(\mathbf{0})\right| \neq p^{\frac{n}{2}},$$

for all n sufficiently large because otherwise it would imply

$$\lim_{n\to\infty} \frac{1}{\beta_1^n} \left|\mathcal{H}_{T_{n,[2,\cdots,k]},\mathbb{F}_p}(\mathbf{0})\right| = \lim_{n\to\infty} \frac{p^{n/2}}{\beta_1^n} = \lim_{n\to\infty} \left(\frac{\sqrt{p}}{\beta_1}\right)^n = 0,$$

which contradicts (3.7). But a p-ary function $f_n \in \mathcal{B}_{n,p}$ is bent if and only if

$$\left|\mathcal{H}_{f_n,\mathbb{F}_p}(\boldsymbol{a})\right| = p^{\frac{n}{2}}$$

for all $\boldsymbol{a} \in \mathbb{F}_p^n$. Therefore, we conclude that $T_{n,[2,\cdots,k]}$ is not bent over $\mathbb{F}_p$. □

Computer experiments suggest that the polynomial $Q_{k,p}(X)$ appears as a factor of the characteristic polynomial of the minimal linear recurrence with integer coefficients that $\{W_{R_{n,[2,3,\cdots,k]}}(\boldsymbol{a})\}$ satisfy. We have been unable to prove this, but if true, the argument provided in this work can be used to show that $R_{n,[2,3,\cdots,k]}$ is not bent over $\mathbb{F}_p$.

4. Concluding remarks

In this work we showed that Walsh transformations of generalized p-ary functions whose components are symmetric, rotation symmetric or a linear combination or concatenation of them are C-finite sequences. This generalizes the results presented in [8, 9] for regular p-ary functions to generalized ones. It would be nice to see if some of these results work carry over to generalized q-ary functions when q is a power of a prime p. This is part of future work.

We also showed that roots of characteristic polynomials associated to linear recurrences satisfied by Walsh transformations of families of p-ary functions are bounded in absolute value by p. That results combined with some analysis of these roots can be used to obtain information about the balancedness and non-linearity of the p-ary functions. We hope and expect the expert reader to find applications of our results.

Acknowledgments. The research of the first 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 third author was also supported as a student by the same grant.

References

[1] L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer-Verlag, 2014.
[2] J. Cai, F. Green, and T. Thierauf. On the correlation of symmetric functions. *Math. Systems Theory* 29 (1996) 245–258.
[3] C. Carlet. Boolean functions for cryptography and error correcting codes, in: Boolean Methods and Models. *Cambridge University Press*, Cambridge (2010),257–397.
[4] F. Castro and L. A. Medina. Linear Recurrences and Asymptotic Behavior of Exponential Sums of Symmetric Boolean Functions. *Elec. J. Combin.* 18 (2011), #P8.
[5] F. Castro and L. A. Medina. Asymptotic Behavior of Perturbations of Symmetric Functions. *Annals of Combin.* 18 (2014) 397–417.
[6] F. Castro, O. E. González and L. A. Medina. Diophantine equations with binomial coefficients and perturbations of symmetric Boolean functions. *IEEE Trans. Inform. Theory* 64(2) (2018) 1347–1360.
[7] F. Castro, L.A. Medina, P. P. Stănică. Generalized Walsh transforms of symmetric and rotation symmetric Boolean functions are linear recurrent. *Applicable Algebra in Engineering, Communication and Computing* (2018) 1–21.
[8] F. Castro, R. Chapman, L.A. Medina, L. B. Sepúlveda Recursions associated to traprezoid, symmetric and rotation symmetric functions over Galois fields. *Discrete Mathematics* **341**(2018)1915–1931.
[9] F. Castro, L.A. Medina, L. B. Sepúlveda Closed formulas for exponential sums of symmetric polynomials over Galois fields. *J. Algebr. Comb.* (2018) DOI 10.1007/s10801-018-0840-4.
[10] K. Conrad. Roots on a circle. Expository note available at `http://www.math.uconn.edu/ kconrad/blurbs/`.
[11] T. W. Cusick. Weight recursions for any rotation symmetric Boolean functions. *IEEE Trans. Inf. Theory* 64(4) (2018) 2962–2968.

[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 Y. Li. k-th order symmetric SAC Boolean functions and bisecting binomial coefficients. *Discrete Appl. Math.* 149 (2005) 73–86.
[14] T. W. Cusick, Y. Li, and P. Stănică. Balanced Symmetric Functions over $GF(p)$. *IEEE Trans. Inf. Theory* 5 (2008) 1304–1307.
[15] T. W. Cusick and P. Stănică. Fast evaluation, weights and nonlinearity of rotation symmetric functions. *Discr. Math.* 258 (2002) 289–301.
[16] T. W. Cusick, P. Stănică. Cryptographic Boolean Functions and Applications *Academic Press*,(Ed. 2), San Diego, CA, 2017.
[17] 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.
[18] 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.
[19] 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.
[20] S. Hodžić and E. Pasalic. Generalized bent functions: Some general construction methods and related necessary and sufficient conditions. *Cryptograph. Commun.*,**7**4 (2015) 469–483.
[21] P. V. Kumar, R. A. Scholtz and L. R. Welch. Generalized bent functions and their properties. *J. Combin Theory -Ser. A* **40** (1985) 90–107.
[22] Y. Li and T.W. Cusick. Linear Structures of Symmetric Functions over Finite Fields. Inf. Processing Letters **97** (2006) 124–127.
[23] Y. Li and T. W. Cusick. Strict Avalanche Criterion Over Finite Fields. *J. Math. Cryptology* **1(1)** (2007) 65–78.
[24] M. Liu, P. Lu and G.L. Mullen. Correlation-Immune Functions over Finite Fields. *IEEE Trans. Inf. Theory* **44** (1998), 1273–1276.
[25] T. Martinsen, W. Meidl, S. Mesnager, P. Stănică. Decomposing generalized bent and hyperbent functions. *IEEE Trans. Inf. Theory* 63 (2017) 7804–7812.
[26] L. A. Medina, L. B. Sepúlveda and C. Serna-Rapello. Value distribution of elementary symmetric polynomials and its perturbations over finite fields. *Finite Fields Th. App.* 63 (2020) 1–21.
[27] M. G. Parker and A. Pott. On Boolean functions which are bent and negabent. *Proc. Int. Conf. Sequences, Subsequences, Consequences*, LNCS-4893 (2007) 9–23.
[28] J. Pieprzyk and C.X. Qu. Fast hashing and rotation-symmetric functions. *J. Universal Comput. Sci.* 5(1) (1999) 20–31.
[29] C. Riera, M. G. Parker. Generalized bent criteria for Boolean functions. *IEEE Trans. Inf. Theory* 52(9) (2006), 4142–4159.
[30] O. S. Rothaus. On bent functions. *J. Combin. Theory Ser. A* 20 (1976) 300–305.
[31] P. Stănică. Weak and strong 2^k-bent functions. *IEEE Trans. Inform. Theory* **62** 2827–2835 (2016)
[32] P. Stănică, S. Gangopadhyay, B. K. Singh. "Some Results Concerning Generalized Bent Functions. ". Available at http://eprint.iacr.org/2011/290.pdf
[33] P. Stănică, T. Martinsen, S. Gangopadhyay, B. K. Singh. Bent and generalized bent Boolean functions. *Des. Codes Cryptogr.*, **69**(2013) 77–94.

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

Department of Mathematics, University of Puerto Rico, San Juan, PR 00925
Email address: leonid.sepulveda1@upr.edu

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