HADAMARD MATRICES AND THE SPECTRUM OF QUADRATIC SYMMETRIC POLYNOMIALS OVER FINITE FIELDS

FRANCIS N. CASTRO AND LUIS A. MEDINA

Abstract. In this article, we present a beautiful connection between Hadamard matrices and exponential sums of quadratic symmetric polynomials over Galois fields. This connection appears when the recursive nature of these sequences is analyzed. We calculate the spectrum for the Hadamard matrices that dominate these recurrences. The eigenvalues depend on the Legendre symbol and the quadratic Gauss sum over finite field extensions. In particular, these formulas allow us to calculate closed formulas for the exponential sums over Galois field of quadratic symmetric polynomials. Finally, in the particular case of finite extensions of the binary field, we show that the corresponding Hadamard matrix is a permutation away from a classical construction of these matrices.

1. Introduction

Boolean functions are functions from the vector space $\mathbb{F}_2^n$ to $\mathbb{F}_2$ where $\mathbb{F}_2$ represents the binary field. Applications of these beautiful combinatorial objects to computer science fields such as coding theory, cryptography and information theory have made them a source of active research. Moreover, due to memory restrictions of current technology efficient implementations of these functions is an area of special interest. Efficient implementations, in the most general sense, is a very hard problem. However, some classes like the class of symmetric Boolean functions and the class of rotation symmetric Boolean functions are excellent candidates for efficient implementations. These functions are part of ongoing research.

In some applications 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. Let $F(\mathbf{X})$ be a Boolean function. List the elements of $\mathbb{F}_2^n$ in lexicographic order and label them as $\mathbf{x}_0 = (0, 0, \cdots, 0)$, $\mathbf{x}_1 = (0, 0, \cdots, 1)$ and so on. The vector $(F(\mathbf{x}_0), F(\mathbf{x}_1), \cdots, F(\mathbf{x}_{2^n-1}))$ is called the *truth table of* F. Balancedness of Boolean functions are usually studied from the point of view of Hamming weights or from the point of view of exponential sums.

The *Hamming weight* of a Boolean function F, usually denoted by $\mathrm{wt}(F)$, is the number of 1's in the truth table of F. Thus, a Boolean function F is balanced if and only if $\mathrm{wt}(F) = 2^{n-1}$. Weights of symmetric Boolean functions are somewhat understood. For instance, it is known since the 90's that weights of symmetric Boolean functions are linear recursive with integer coefficients [4, 5]. On the other hand, the study of weights of rotations symmetric Boolean functions is becoming an active area of research [3, 13, 15, 27, 28]. Similar to the symmetric case, it had been observed that weights of cubic rotation symmetric Boolean functions are linear recursive [3, 13]. This prompted the question if the same holds for any degree. An answer was given by Cusick [12] when he showed that weights of any rotation symmetric Boolean function satisfy linear recurrences with integer coefficients.

The *exponential sum* of an n-variable Boolean function $F(\mathbf{X})$ is defined as

$$S(F) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{F(\mathbf{x})}. \tag{1.1}$$

Observe that a Boolean function $F(\mathbf{X})$ is balanced if and only if $S(F) = 0$. This point of view is also a very active area of research. For some examples, please refer to [5–7, 9, 11, 19, 21, 24]. Moreover, both point of views are equivalent and are linked by the equation

$$\mathrm{wt}(F) = \frac{2^n - S(F)}{2}. \tag{1.2}$$

Date: December 14, 2017.

2010 *Mathematics Subject Classification.* 05B20, 05E05, 11T23.

Key words and phrases. Hadamard matrices, Walsh transform, recurrences, exponential sums.

Cusick's result about the linear recursive behavior of exponential sums of rotation symmetric Boolean functions was generalized in [8] to the general setting of exponential sums over finite fields. Consider the Galois field $\mathbb{F}_q$ where $q = p^r$ with p prime and $r \geq 1$. The *exponential sum over* $\mathbb{F}_q$ of a function $F : \mathbb{F}_q \to \mathbb{F}_q$ is given by

$$S_{\mathbb{F}_q}(F) = \sum_{\mathbf{x} \in \mathbb{F}_q^n} e^{\frac{2\pi i}{p} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(F(\mathbf{x}))}, \tag{1.3}$$

where $i = \sqrt{-1}$ and $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ represents the field trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. In [8] it was proved that exponential sums over Galois fields of rotation symmetric polynomials are also linear recurrent with integer coefficients. Therefore, the recursive nature of these sequences is not special to the binary field.

The authors of [8] also proved that exponential sums over Galois fields of symmetric polynomials are linear recurrent with integer coefficients. Moreover, a beautiful relation between Hadamard matrices and exponential sums of quadratic symmetric polynomials over the prime fields $\mathbb{F}_p$ (p prime) was found. This link is the main focus of this article where we show that the same holds true when quadratic symmetric polynomials are considered over any Galois fields $\mathbb{F}_q$.

The connection to Hadamard matrices emerges when the problem of finding linear recurrences for these exponential sums is considered. This sounds technical, but in reality, once the proper framework is established, it is a very straight forward problem. In fact, the main idea to find such recurrences is to transform the problem into a linear system and to compute an annihilator for the matrix associated to it. An *annihilator* for a matrix A is simply a polynomial $p(X)$ satisfied by A, i.e. a polynomial $p(X)$ for which $p(A) = 0$. The characteristic polynomial of A is such an example. We show that the matrices that dominates the recurrences associated to quadratic symmetric polynomials over any Galois field are all Hadamard matrices. Moreover, previous constructions of Hadamard matrices re-emerge when the equivalent class of the matrix associated to quadratic symmetric polynomials is considered.

As just mentioned, in this article we show that the matrices that dominate the linear recursive nature of exponential sums of quadratic symmetric polynomials over $\mathbb{F}_q$ are all Hadamard (regardless of q). In the particular case when q is odd we compute the eigenvalues and eigenvectors for the corresponding Hadamard matrices. These formulas depend on the Legendre symbol and quadratic Gauss sum over $\mathbb{F}_q$. Moreover, these formulas for the eigenvalues allow us to compute closed formulas for the corresponding exponential sums.

This paper is divided as follows. Next section is a short survey of Hadamard matrices. This survey is included for completeness purposes. The expert reader may skip it. Some preliminaries and examples that expose the relation between Hadamard matrices and exponential sums of quadratic symmetric polynomials are the subject of Section 3. In the fourth and final section we showed that the matrices related to the recursions considered in this article are indeed Hadamard. We also compute the spectrum for these matrices when q is odd and provide closed formulas for their corresponding exponential sums. These closed formulas depend on the Legendre symbol and the quadratic Gauss sum. These behavior is in line with the classical results in number theory where Gauss sums appear (naturally) in the general theory of exponential sums. However, as far we know, this is a new result. Finally, in the particular case of finite extensions of the binary field, we show that the corresponding Hadamard matrix is a permutation away from a classical construction of these matrices.

2. Hadamard matrices: a short survey

Hadamard matrices, named after the great mathematician Jacques Hadamard, are fascinating combinatorial objects with applications to many scientific areas. Some examples include statistics, modern communications systems, error-correcting codes and cryptography. In the particular case of error-correcting codes, they are an important ingredient in the famous Reed-Muller code and Walsh-Hadamard code.

One of the most appealing aspects of Hadamard matrices is the simplicity of its formal definition: a square matrix H of order n is a *Hadamard matrix* if all its entries are either 1 or -1 and it satisfies

$$HH^T = nI_n, \tag{2.1}$$

where I_n is the $n \times n$ identity matrix. Some simple examples of Hadamard matrices are

$$\begin{pmatrix} 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{2.2}$$

Up to equivalence, these are the three smallest examples. Two Hadamard matrices H and H' are said to be *equivalent* if H' can be obtained from H by interchanging rows or columns, or by multiplying rows or columns by -1. Up to equivalence, there is a unique Hadamard matrix of orders 1, 2, 4, 8, and 12. There are 5 inequivalent matrices of order 16. In contrast, there are millions (13,710,027 to be exact) of inequivalent matrices of order 32 [18]. See sequence `A007299` in [25].

There exist no $n \times n$ Hadamard matrices for $n \notin \{1, 2, 4k \,|\, k \in \mathbb{N}\}$. In fact, it has been conjectured that a Hadamard matrix of order n exists if and only if $n = 1, 2, 4k$ for k a natural number. This is known as *Hadamard's Conjecture*. It remains an open question, but it is widely believed to be true.

One of the earliest champions of Hadamard matrices (and perhaps, the first one) was James Joseph Sylvester. In [29] (1867), Sylvester provided a construction of a Hadamard matrix of order 2^r for every non-negative integer r. Let H be a Hadamard matrix of order n. He noticed that the partition matrix

$$\begin{pmatrix} H & H \\ -H & H \end{pmatrix} \tag{2.3}$$

is also Hadamard. Therefore, defining $H_1 = (1)$ and applying (2.3) repeatedly lead to the construction of the Hadamard matrix

$$H_{2^r} = \begin{pmatrix} H_{2^{r-1}} & H_{2^{r-1}} \\ -H_{2^{r-1}} & H_{2^{r-1}} \end{pmatrix}. \tag{2.4}$$

In fact, the three examples in (2.2) are just H_1, H_2 and H_4.

Sylvester's construction can be written in terms of Kronecker products. If A and B are matrices, their *Kronecker product* $A \otimes B$ is the matrix M constructed by replacing each entry $A_{i,j}$ in A by $A_{i,j}B$. Therefore, in terms of Kronecker products, Sylvester's construction is

$$H_{2^r} = H_2 \otimes H_{2^{r-1}}. \tag{2.5}$$

Sylvester's construction has been generalized. Specifically, if H_n, H_m are Hadamard matrices of orders n and m (resp.), then their Kronecker product $H_n \otimes H_m$ is an Hadamard matrix of order nm. See [26] for more information.

The existence of Hadamard matrices for orders different than a power of two was established by Hadamard [16] when he constructed Hadamard matrices of order 12 and 20. Other constructions of Hadamard matrices include the famous Paley Construction [23] and Williamson Construction [31]. In fact, the literature of Hadamard matrices and their constructions is quite extensive. Some examples are [2, 10, 17, 20, 30]. The smallest order of the form $4k$ for which a Hadamard matrix cannot be constructed by a combination of known methods and for which no Hadamard matrix is known is 668.

There are various ways to generalize the concept of Hadamard matrices. The one that we use in this article is the concept of complex Hadamard Matrices. An $n \times n$ matrix H is called a *complex Hadamard matrix* if all its entries H_{ij} are complex numbers with $|H_{ij}| = 1$ (unimodularity) and

$$H\overline{H}^T = nI_n, \tag{2.6}$$

where $\overline{H}$ represents the matrix obtained by complex conjugation of all entries of H.

One of the most notable differences between complex Hadamard matrices and real Hadamard matrices is their existence. While the order n of a real Hadamard matrix is necessarily $1, 2$ or $4m$, with m a natural number, complex Hadamard matrices exist for any natural n. The classical example is the $n \times n$ *Discrete*

Fourier Transform matrix W_n (DFT), which is defined by

$$W_n = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(n-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \omega^{3(n-1)} & \cdots & \omega^{(n-1)(n-1)} \end{pmatrix}, \tag{2.7}$$

where $\omega = e^{2\pi i/n}$ is a primitive nth root of unity. Observe that if $F_n = \sqrt{n}W_n$, then

$$F_n \overline{F_n}^T = nI_n. \tag{2.8}$$

Thus, F_n is a complex Hadamard matrix of order n.

Two complex Hadamard matrices H and H' are called *equivalent* if there exist diagonal unitary matrices D_1 and D_2 and permutation matrices P_1 and P_2 such that

$$H' = D_1 P_1 H P_2 D_2. \tag{2.9}$$

An $n \times n$ complex Hadamard matrix is called *dephased* when its first column and first row are $\mathbf{1}$ and $\mathbf{1}^T$ (resp.) where $\mathbf{1}$ is the column vector of dimension n whose entries are all 1's. For example, the rescaled Discrete Fourier Transform matrix F_n is dephased. Every complex Hadamard matrix is equivalent to a dephased one. This is actually very simple to see if the Hadamard matrix H has first row equal to $\mathbf{1}^T$. Given an $n \times n$ complex Hadamard matrix $H = (H_{jk})$ whose first row is equal to $\mathbf{1}^T$, define $Deph(H)$ as

$$Deph(H) = D_H \cdot H, \tag{2.10}$$

where

$$D_H = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & H_{2,1}^{-1} & 0 & \cdots & 0 \\ 0 & 0 & H_{3,1}^{-1} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & H_{n,1}^{-1} \end{pmatrix}. \tag{2.11}$$

Observe that the result of this matrix multiplication is equal to the matrix obtained from H by multiplying each row of H by the inverse of its first entry. Clearly, $Deph(H)$ is dephased and

$$\begin{aligned} Deph(H) \cdot \overline{Deph(H)}^T &= D_H \cdot H \cdot \overline{H}^T \cdot \overline{D_H}^T \\ &= D_H \cdot nI_n \cdot \overline{D_H}^T = nI_n. \end{aligned} \tag{2.12}$$

Thus, $Deph(H)$ is complex Hadamard and, according to definition (2.9), equivalent to H.

***Remark* 2.1.** Following what is now a "not so good" habit in the culture of mathematicians, we abuse notation $Deph(H)$. For now on we use $Deph(H)$ to represent a dephased Hadamard matrix for which H is equivalent to, even though we defined $Deph(H)$ for Hadamard matrices with first row equal to $\mathbf{1}^T$.

In the next section we expose a connection between Hadamard matrices and exponential sums of quadratic symmetric polynomials over Galois fields. This relationship flourishes when the recursive nature of this sequences is explored.

3. A connection to Hadamard matrices

As mentioned in the introduction, we present a beautiful relation between Hadamard matrices and exponential sums of quadratic symmetric polynomials over Galois fields. Let $\boldsymbol{e}_{n,k}$ denotes the *elementary symmetric polynomial* in n variables of degree k. This polynomial is formed by adding together all distinct products of k distinct variables. For example,

$$\boldsymbol{e}_{4,3} = X_1X_2X_3 + X_1X_4X_3 + X_2X_4X_3 + X_1X_2X_4. \tag{3.1}$$

Consider the Galois field $\mathbb{F}_q$ where $q = p^r$ with p prime and $r \geq 1$. Recall that the *exponential sum* of a function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ is defined by

$$S_{\mathbb{F}_q}(F) = \sum_{\mathbf{x} \in \mathbb{F}_q^n} e^{\frac{2\pi i}{p} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(F(\mathbf{x}))}, \tag{3.2}$$

where $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ represents the field trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. The *field trace function* can be explicitly defined as

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \sum_{i=0}^{r-1} \alpha^{p^i}, \tag{3.3}$$

with arithmetic done in $\mathbb{F}_q$.

Similar to the Boolean case, a function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ is balanced if its values are uniformly distributed. That is, if F takes each value of $\mathbb{F}_q$ exactly q^{n-1} times. As in the case of Boolean functions, if a function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ is balanced, then $S_{\mathbb{F}_q}(F)$ is 0. The converse is not necessarily true, however it holds if $q = p$. In [8], Castro, Chapman, Medina and Sepúlveda showed that exponential sums of elementary symmetric polynomials and linear combinations of them are linear recurrent with integer coefficients. In principle, this implies that exponential sums of this type of functions can be computed rapidly.

The argument presented in [8] is actually quite simple: find a recursive generating set for $S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})$. That is, find a set of sequences

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

such that for some integer l,

$$S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k}) = \sum_{j=1}^{s} c_j \cdot a_j(n-l)$$

where c_j's are constants, and, for each $1 \leq j_0 \leq s$ and every n, one has

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

where $d_{j_0,j}$'s are constant. Once this is done, then to find a linear recurrence satisfied by $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})\}$, it is enough to find an annihilating polynomial $Q(X)$ for the matrix $A = (d_{ij})$. A polynomial $Q(X)$ is said to be an *annihilating polynomial* for a $n \times n$ matrix A if $Q(A) = O$, where O represents the $n \times n$ matrix whose entries are all 0. Note that the sequence $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})\}$ will satisfy the linear recurrence with characteristic polynomial $Q(X)$ because it is a linear combination of the $\{a_j(n)\}$.

Let us illustrate the problem with a detailed example.

Example 3.1. Consider the irreducible polynomial $f(X) = X^3 + X + 1$ in $\mathbb{F}_2[X]$. Make the identification

$$\mathbb{F}_8 = \mathbb{F}_2[X]/(f(X)), \tag{3.4}$$

and let $\alpha = [X]$, i.e. α is the equivalence class of X. This implies that $\alpha^3 = \alpha + 1$. Now order $\mathbb{F}_8$ using the lexicographic order, that is,

$$\begin{aligned} \mathbb{F}_8 &= \left\{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\right\} \\ &= \{\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7\}. \end{aligned} \tag{3.5}$$

Consider the sequence $\{S_{\mathbb{F}_8}(\boldsymbol{e}_{n,2})\}$. Observe that if we let X_n assume the value β_j, then $\boldsymbol{e}_{n,2}$ gets transformed to

$$\boldsymbol{e}_{n-1,2} + \beta_j \boldsymbol{e}_{n-1,1}. \tag{3.6}$$

Thus, letting X_n assume all values in the field leads to

$$
\begin{aligned}
S_{\mathbb{F}_8}(\boldsymbol{e}_{n,2}) &= \sum_{\mathbf{x}\in\mathbb{F}_8^n} (-1)^{\mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\boldsymbol{e}_{n,2}(\mathbf{x}))} \\
&= \sum_{j=0}^{7} \sum_{(x_1,\cdots,x_{n-1})\in\mathbb{F}_8^{n-1}} (-1)^{\mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\boldsymbol{e}_{n,2}(x_1,\cdots,x_{n-1},\beta_j))} \\
&= \sum_{j=0}^{7} \sum_{\mathbf{x}\in\mathbb{F}_8^{n-1}} (-1)^{\mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\boldsymbol{e}_{n-1,2}(\mathbf{x})+\beta_j\boldsymbol{e}_{n-1,1}(\mathbf{x}))} \\
&= \sum_{j=0}^{7} S_{\mathbb{F}_8}(\boldsymbol{e}_{n-1,2}+\beta_j\boldsymbol{e}_{n-1,1}).
\end{aligned} \tag{3.7}
$$

Define $a_{\beta_j}(n) = S_{\mathbb{F}_8}(\boldsymbol{e}_{n,2}+\beta_j\boldsymbol{e}_{n,1})$. Observe that if we show that every $\{a_{\beta_j}(n)\}$ satisfies a common linear recurrence, then $\{S_{\mathbb{F}_8}(\boldsymbol{e}_{n,2})\}$ will satisfy such recurrence.

Consider the polynomial $\boldsymbol{e}_{n,2}+\beta_l\boldsymbol{e}_{n,1}$. As before, letting X_n assume the value β_j transforms $\boldsymbol{e}_{n,2}+\beta_l\boldsymbol{e}_{n,1}$ into

$$\boldsymbol{e}_{n-1,2} + (\beta_l+\beta_j)\boldsymbol{e}_{n-1,1} + \beta_l\beta_j. \tag{3.8}$$

Therefore, letting X_n assume all values in the field leads to

$$a_{\beta_l}(n) = \sum_{j=0}^{7} (-1)^{\mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\beta_l\beta_j)} a_{\beta_l+\beta_j}(n-1). \tag{3.9}$$

Using the values

$$
\begin{aligned}
&\mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\beta_j) = 0, \text{ for } j = 0,2,4,6 \\
&\mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\beta_j) = 1, \text{ for } j = 1,3,5,7,
\end{aligned} \tag{3.10}
$$

equation (3.9) can be written in matrix form as

$$
\begin{pmatrix} a_{\beta_0}(n) \\ a_{\beta_1}(n) \\ a_{\beta_2}(n) \\ a_{\beta_3}(n) \\ a_{\beta_4}(n) \\ a_{\beta_5}(n) \\ a_{\beta_6}(n) \\ a_{\beta_7}(n) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} a_{\beta_0}(n-1) \\ a_{\beta_1}(n-1) \\ a_{\beta_2}(n-1) \\ a_{\beta_3}(n-1) \\ a_{\beta_4}(n-1) \\ a_{\beta_5}(n-1) \\ a_{\beta_6}(n-1) \\ a_{\beta_7}(n-1) \end{pmatrix}. \tag{3.11}
$$

Denote by M_8 the matrix in (3.11). If we wish to find a linear recurrence with constant coefficients satisfied by $\{S_{\mathbb{F}_8}(\boldsymbol{e}_{n,2})\}$, then it is enough to find an annihilating polynomial for M_8. That is because every $\{a_{\beta_j}(n)\}$ will satisfy the linear recurrence whose characteristic polynomial is given by this annihilating polynomial.

A simple, but perhaps tedious, calculation shows that the minimal polynomial of M_8 is $q_8(X) = X^4+64$. Thus, $\{S_{\mathbb{F}_8}(\boldsymbol{e}_{n,2})\}$ satisfies the linear recurrence whose characteristic polynomial is $q_8(X)$. Explicitly, if we define

$$
\begin{aligned}
x_2 &= S_{\mathbb{F}_8}(\boldsymbol{e}_{2,2}) = 8 \\
x_3 &= S_{\mathbb{F}_8}(\boldsymbol{e}_{3,2}) = 0 \\
x_4 &= S_{\mathbb{F}_8}(\boldsymbol{e}_{4,2}) = -64 \\
x_5 &= S_{\mathbb{F}_8}(\boldsymbol{e}_{5,2}) = -512 \\
x_n &= -64x_{n-4}, \quad \text{for } n \geq 6,
\end{aligned} \tag{3.12}
$$

then $S_{\mathbb{F}_8}(\boldsymbol{e}_{n,2}) = x_n$. In fact, using this recurrence we know that the first few values of $\{S_{\mathbb{F}_8}(\boldsymbol{e}_{n,2})\}_{n\geq 2}$ are

$$8, 0, -64, -512, -512, 0, 4096, 32768, 32768, 0, -262144, \cdots.$$

This calculation is done almost instantly. For example, using an old computer (whose features are not top of the art) from one of the authors, it took 0.116 seconds to calculate $S_{\mathbb{F}_8}(\boldsymbol{e}_{50000,2})$ which is a number with

$22,578$ digits. Also, this recurrence implies that $\boldsymbol{e}_{n,2}$ is balanced over $\mathbb{F}_8$ if and only if $n = 4m-1$ for m a positive integer. This coincides with a conjecture given in [1]. This concludes the example.

In [8], the sequence $\{S_{\mathbb{F}_p}(\boldsymbol{e}_{n,2})\}$, for p prime, was studied in some details. In particular, it was observed that this sequence is linear recurrent and that its recursive nature is dominated by the matrix

$$M_p = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ e^{\frac{2(p-1)\pi i}{p}} & 1 & e^{\frac{2\pi i}{p}} & e^{\frac{4\pi i}{p}} & \cdots & e^{\frac{2(p-2)\pi i}{p}} \\ e^{\frac{2\times 2(p-2)\pi i}{p}} & e^{\frac{2\times 2(p-1)\pi i}{p}} & 1 & e^{\frac{4\pi i}{p}} & \cdots & e^{\frac{2\times 2(p-3)\pi i}{p}} \\ e^{\frac{2\times 3(p-3)\pi i}{p}} & e^{\frac{2\times 3(p-2)\pi i}{p}} & e^{\frac{2\times 3(p-1)\pi i}{p}} & 1 & \cdots & e^{\frac{2\times 2(p-3)\pi i}{p}} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ e^{\frac{2(p-1)\pi i}{p}} & e^{\frac{2\times 2(p-1)\pi i}{p}} & e^{\frac{2\times 3(p-1)\pi i}{p}} & e^{\frac{2\times 4(p-1)\pi i}{p}} & \cdots & 1 \end{pmatrix}. \tag{3.13}$$

The matrix M_p turns out to be a very interesting mathematical object. First, it can be obtained from the $p \times p$ Fourier Discrete Transform Matrix by replacing its j-row $\boldsymbol{r}_j$ by $RTC^{j-1}(\boldsymbol{r}_j)$, where RTC is the *rotate through carry* function

$$RTC(a_1, a_2, \cdots, a_n) = (a_n, a_1, a_2, \cdots, a_{n-1}) \tag{3.14}$$

and RTC^m represents m iterations of RTC. Second, its eigenvalues are given by

$$\lambda = \left(\frac{-2}{p}\right) g(1;p)\zeta^{-sa^2},$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol, $g(a;p)$ is the quadratic Gauss sum mod p, $s = (p-1)/2$, and $\zeta = e^{2\pi i/p}$. And third, the matrix M_p is complex Hadamard.

The fact that all the matrices associated to $\{S_{\mathbb{F}_p}(\boldsymbol{e}_{n,2})\}$ for p prime are Hadamard leads to question if this holds for matrices associated to $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,2})\}$ when q is a power of a prime. In order to try to answer this, let us revisit M_8, the matrix in Example 3.1. The reader can check using her favorite computer algebra system that this matrix is indeed real Hadamard. Of course, there is, up to equivalence, only one Hadamard matrix of order 8. This means that the Sylvester matrix H_8 and M_8 are equivalent. Indeed, $Deph(M_8)$ can be constructed from H_8 by applying the permutation $\sigma = (1\,8)(2\,7)(3\,4)(5\,6)$ to the columns of H_8.

***Notation* 3.2.** Let A be an $n \times n$ matrix and let $\sigma \in S_n$, where S_n represents the symmetric group of n symbols. The expression $\sigma(A)$ represents the matrix that can be constructed from A by applying the permutation σ to its columns.

Let us do another example to see if the pattern continues.

Example 3.3. Construct $\mathbb{F}_{16}$ by identifying

$$\mathbb{F}_{16} = \mathbb{F}_2[X]/(f(X)), \tag{3.15}$$

where $f(X) = X^4 + X + 1$ in $\mathbb{F}_2[X]$ is irreducible. Let $\alpha = [X]$, then $\alpha^4 = \alpha + 1$. Order $\mathbb{F}_{16}$ using the lexicographic order, that is,

$$\begin{aligned} \mathbb{F}_{16} &= \left\{0, 1, \alpha, \alpha+1, \alpha^2, \cdots, \alpha^3+\alpha^2+\alpha+1\right\} \\ &= \{\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \cdots, \beta_{15}\}. \end{aligned} \tag{3.16}$$

Consider the sequence $\{S_{\mathbb{F}_{16}}(\boldsymbol{e}_{n,2})\}$ and proceed as in Example 3.1. This process produces a matrix M_{16} of order 16 with entries ± 1. As in the previous example, the matrix M_{16} turns out to be (real) Hadamard. It was mentioned in the previous section that there are 5 inequivalent Hadamard matrices of order 16, one of them being the Sylvester matrix H_{16}. It is natural to ask to which of these 5 matrices our Hadamard matrix is equivalent to. The answer is to the Sylvester matrix H_{16}! Indeed, $Deph(M_{16})$ can be constructed from H_{16} by applying the permutation

$$\sigma = (1\ 15\ 10\ 7\ 9\ 16)(2\ 8)(3\ 11\ 12)(5\ 13\ 14).$$

to the columns of H_{16}. In other words, $Deph(M_{16}) = \sigma(H_{16})$.

Another example, but with q odd.

Example 3.4. Similar to Example 3.1, the identification $\mathbb{F}_9 = \mathbb{F}_3[X]/(f(X))$, where $f(X) = X^2 + 1$ is irreducible in $\mathbb{F}_3[X]$ produces the matrix

$$M_9 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ e^{\frac{2i\pi}{3}} & 1 & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & 1 & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & 1 & e^{-\frac{2i\pi}{3}} \\ e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & 1 & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & 1 & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & 1 \\ e^{-\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & 1 & 1 & 1 & e^{\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} \\ 1 & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & 1 & e^{-\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & 1 \\ 1 & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & 1 & e^{-\frac{2i\pi}{3}} & 1 & e^{\frac{2i\pi}{3}} \\ e^{-\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & 1 & 1 & 1 \\ 1 & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & 1 & e^{\frac{2i\pi}{3}} & 1 & e^{-\frac{2i\pi}{3}} \\ 1 & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & 1 & e^{\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & 1 \end{pmatrix}.$$

It can be verified that this matrix is indeed complex Hadamard. Moreover, its eigenvalues are all of the form $-g(1;3)^2\zeta_3^b$ where $b \in \mathbb{F}_3$, $g(a;p)$ is the quadratic Gauss sum mod p and $\zeta_3 = e^{2\pi i/3}$. Thus, a behavior similar to the one for $S_{\mathbb{F}_p}(\boldsymbol{e}_{n,2})$ seems to hold for $q = p^r$. This is explored in the next section where a formula for the eigenvalues of M_q when q is odd is provided.

The reader is encouraged to experiment and convince herself that all matrices M_q's associated to $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,2})\}$, for $q = p^r$, appear to be complex Hadamard. Moreover, in the case when $q = 2^r$ is a power of 2, the matrix seems to be real Hadamard and its dephased form is a permutation of the columns of the Sylvester matrix H_{2^r}. Think of this as if the dephased form of our matrix is a "permutation away" from the Sylvester matrix. In the next section we prove these facts.

4. The recursive nature of quadratic symmetric polynomials and Hadamard matrices

In this section we prove the assertions presented in the previous section. That is, all matrices M_q's associated to $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,2})\}$ are complex Hadamard and in the case when $q = 2^r$, the produced matrix is equivalent to H_{2^r} because its $Deph(M_{2^r})$ is a permutation away from it. We also find explicit formulas for the eigenvalues of our matrices, which in turns allows us to provide closed formulas for $S_{\mathbb{F}_q}(\boldsymbol{e}_{n,2})$.

Let $\alpha \in \mathbb{F}_q$ be a primitive element, that is, $\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{q-2}\}$. Similar to Example 3.1, one has

$$S_{\mathbb{F}_q}(\boldsymbol{e}_{n,2}) = S_{\mathbb{F}_q}(\boldsymbol{e}_{n-1,2}) + \sum_{j=0}^{q-2} S_{\mathbb{F}_q}(\boldsymbol{e}_{n-1,2} + \alpha^j \boldsymbol{e}_{n-1,1}). \tag{4.1}$$

Therefore, if we define

$$a_\beta(n) = S_{\mathbb{F}_q}(\boldsymbol{e}_{n,2} + \beta \boldsymbol{e}_{n,1}), \text{ for } \beta \in \mathbb{F}_q, \tag{4.2}$$

then

$$S_{\mathbb{F}_q}(\boldsymbol{e}_{n,2}) = \sum_{\beta \in \mathbb{F}_q} a_\beta(n-1). \tag{4.3}$$

Thus, the recursive nature of $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,2})\}$ is dominated by the sequences $\{a_\beta(n)\}$. Again, similar to Example 3.1, one has

$$a_\gamma(n) = \sum_{\beta \in \mathbb{F}_q} e^{\frac{2\pi i}{p} \cdot \mathrm{Tr}(\gamma\beta)} a_{\gamma+\beta}(n-1), \tag{4.4}$$

where $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ is the field trace. Therefore, if we let

$$\boldsymbol{a}(n) = \begin{pmatrix} a_0(n) \\ a_1(n) \\ a_\alpha(n) \\ a_{\alpha^2}(n) \\ \vdots \\ a_{\alpha^{q-2}}(n) \end{pmatrix}, \tag{4.5}$$

then (4.4) can be written as $\boldsymbol{a}(n) = M_q \cdot \boldsymbol{a}(n-1)$ for a suitable matrix M_q.

Theorem 4.1. *Let $q = p^r$ with p prime. The matrix M_q is a $q \times q$ complex Hadamard matrix.*

Proof. Define $\lambda_\beta(x) = x + \beta$. Then the matrix M_q is given by

$$M_q = \begin{pmatrix} R_0(q) \\ R_1(q) \\ R_\alpha(q) \\ \vdots \\ R_{\alpha^{q-2}}(q) \end{pmatrix} \tag{4.6}$$

where $R_\beta(q)$, for $\beta \in \mathbb{F}_q$, is the row vector

$$R_\beta(r) = \begin{pmatrix} e^{\frac{2\pi i}{p}\mathrm{Tr}(\beta\lambda_{-\beta}(0))} & e^{\frac{2\pi i}{p}\mathrm{Tr}(\beta\lambda_{-\beta}(1))} & e^{\frac{2\pi i}{p}\mathrm{Tr}(\beta\lambda_{-\beta}(\alpha))} & \cdots & e^{\frac{2\pi i}{p}\mathrm{Tr}(\beta\lambda_{-\beta}(\alpha^{q-2}))} \end{pmatrix}. \tag{4.7}$$

The row $R_0(q)$ is simply the row vector whose entries are all 1 because $\mathrm{Tr}(0) = 0$. Now, for any $a \in \mathbb{F}_p$, we have

$$|\{\alpha \in \mathbb{F}_q \,:\, \mathrm{Tr}(\alpha) = a\}| = q^{r-1}. \tag{4.8}$$

This, together with the fact that the function $\alpha^j\lambda_{-\alpha^j}(X)$ is a permutation of $\mathbb{F}_q$, implies that in row $R_{\alpha^j}(q)$ with $j \geq 0$, each number in the set

$$\left\{1, e^{\frac{2\pi i}{p}}, e^{\frac{4\pi i}{p}}, \cdots, e^{\frac{2(p-1)\pi i}{p}}\right\}$$

appears the same amount of times. It is clear that

$$\begin{aligned} R_0(q)\cdot\overline{R_0(q)} &= q \\ R_{\alpha^j}(q)\cdot\overline{R_{\alpha^j}(q)} &= q, \quad \text{for } j \geq 0. \end{aligned} \tag{4.9}$$

Also, if $j \geq 0$, then

$$R_0(q)\cdot\overline{R_{\alpha^j}(q)} = 0, \tag{4.10}$$

because, as mentioned before, all entries of $R_0(q)$ are 1's and each number in the set

$$\left\{1, e^{\frac{2\pi i}{p}}, e^{\frac{4\pi i}{p}}, \cdots, e^{\frac{2(p-1)\pi i}{p}}\right\}$$

appears the same amount of times in $R_{\alpha^j}(q)$.

Suppose now that $0 \leq l, j \leq q-2$ and $l \neq j$. The linearity of the field trace function implies

$$\begin{aligned} R_{\alpha^l}(q)\cdot\overline{R_{\alpha^j}(q)} &= \sum_{\beta\in\mathbb{F}_q} e^{\frac{2\pi i}{p}(\mathrm{Tr}(\alpha^l\lambda_{-\alpha^l}(\beta))-\mathrm{Tr}(\alpha^j\lambda_{-\alpha^j}(\beta)))} \\ &= \sum_{\beta\in\mathbb{F}_q} e^{\frac{2\pi i}{p}\mathrm{Tr}(\alpha^l\lambda_{-\alpha^l}(\beta)-\alpha^j\lambda_{-\alpha^j}(\beta))} \end{aligned} \tag{4.11}$$

However, note that if $f : \mathbb{F}_q \to \mathbb{F}_q$ is defined as

$$f(X) = \alpha^l\lambda_{-\alpha^l}(X) - \alpha^j\lambda_{-\alpha^j}(X), \tag{4.12}$$

then

$$\begin{aligned} f(X) &= \alpha^l\lambda_{-\alpha^l}(X) - \alpha^j\lambda_{-\alpha^j}(X) \\ &= \alpha^l(X-\alpha^l) - \alpha^j(X-\alpha^j) \\ &= (\alpha^l-\alpha^j)X + \alpha^{2l} - \alpha^{2j}. \end{aligned} \tag{4.13}$$

But α is a primitive element of $\mathbb{F}_q$ and $l \neq j$, therefore $f(X)$ is injective. This implies that

$$\begin{aligned} R_{\alpha^l}(q)\cdot\overline{R_{\alpha^j}(q)} &= \sum_{\beta\in\mathbb{F}_q} e^{\frac{2\pi i}{p}\mathrm{Tr}(\alpha^l\lambda_{-\alpha^l}(\beta)-\alpha^j\lambda_{-\alpha^j}(\beta))} \\ &= \sum_{\gamma\in\mathbb{F}_q} e^{\frac{2\pi i}{p}\mathrm{Tr}(\gamma)}. \end{aligned} \tag{4.14}$$

However, as mentioned before, for any $a \in \mathbb{F}_p$ one has

$$|\{\alpha \in \mathbb{F}_q \,:\, \mathrm{Tr}(\alpha) = a\}| = q^{r-1}. \tag{4.15}$$

Thus,

$$R_{\alpha^l}(q)\cdot\overline{R_{\alpha^j}(q)} = \sum_{\gamma\in\mathbb{F}_q} e^{\frac{2\pi i}{p}\mathrm{Tr}(\gamma)} = q^{r-1}\sum_{j=0}^{p-1} e^{\frac{2\pi ij}{p}} = 0, \tag{4.16}$$

because $e^{2\pi i/p}$ is a root of $1+X+X^2+\cdots+X^{p-1}$. Equations (4.9), (4.10) and (4.16) imply

$$M_q\overline{M_q}^T = qI_q \tag{4.17}$$

where I_q is the $q\times q$ identity matrix. Thus, M_q is Hadamard. This concludes the proof. □

In [8], a beautiful formula for the eigenvalues of M_p was established. Their formula included the number-theoretical quadratic Gauss sum mod p and the Legendre symbol. In particular, they show the following theorem.

Theorem 4.2. *[8, Th. 5.4] Let $C(p)$ be set of eigenvalues of M_p were p is an odd prime. Let $\zeta_p = e^{2\pi i/p}$. Then $\lambda\in C(p)$ if and only if*

$$\lambda = \left(\frac{-2}{p}\right) g(1;p)\zeta_p^{-sa^2}, \tag{4.18}$$

where $g(a;p)$ is the quadratic Gauss sum mod p and $s=(p-1)/2$. In particular, $|C(p)| = (p+1)/2$.

Moreover, in the proof of Theorem 4.2, the authors of [8] showed that M_p is diagonalizable. A consequence of this, and which was not stated in [8], is the following result.

Theorem 4.3. *Let p be an odd prime. Let*

$$\lambda_j(p) = \left(\frac{-2}{p}\right) g(1;p)\zeta_p^{-sa_j^2}, \tag{4.19}$$

for $1\le j\le (p+1)/2$ be all the different eigenvalues in $C(p)$. Then,

$$S_{\mathbb{F}_p}(\boldsymbol{e}_{n,2}) = \sum_{j=1}^{(p+1)/2} c_j(p)\lambda_j(p)^n = \sum_{j=1}^{(p+1)/2} c_j(p)\left(\frac{-2}{p}\right)^n g(1;p)^n\zeta_p^{-sna_j^2} \tag{4.20}$$

for some suitable constants $c_j(p)$.

Proof. Since the matrix M_p is diagonalizable, then the polynomial

$$\mu_p(X) = \prod_{j=1}^{(p+1)/2}(X-\lambda_j(p))$$

is the minimal polynomial for M_p. But then the sequence $\{S_{\mathbb{F}_p}(\boldsymbol{e}_{n,2})\}$ satisfies the linear recurrence whose characteristic polynomial is $\mu_p(X)$. The result now follows from the theory of linear recurrences. □

It is natural to ask if something similar happens for the matrices M_q. As mentioned in the previous section (see Example 3.4), the eigenvalues of M_9 are all of the form $-g(1;3)^2\zeta_3^b$ where $b\in\mathbb{F}_3$, $g(a;p)$ is the quadratic Gauss sum mod p and $\zeta_3 = e^{2\pi i/3}$. A similar calculation implies that the eigenvalues of M_{25} are all of the form $-g(1;5)^2\zeta_5^b$ and the ones for M_{27} and M_{125} are of the form

$$\left(\frac{-2}{3}\right) g(1;3)^3\zeta_3^b \quad\text{and}\quad \left(\frac{-2}{5}\right) g(1;5)^3\zeta_5^b,$$

respectively. In fact, we have the following result.

Theorem 4.4. *Suppose that $q = p^r$ with p odd prime and $r > 1$. Let $C(q)$ be the eigenvalues of M_q. Let $\zeta_p = e^{2\pi i/p}$. Then $\lambda \in C(q)$ if and only if*

$$\begin{aligned} \lambda_j(q) &= \left(\frac{-2}{\mathbb{F}_q}\right) g(1;\mathbb{F}_q)\zeta_p^j \\ &= (-1)^{r-1}\left(\frac{-2}{p}\right)^r g(1;p)^r\zeta_p^j, \end{aligned} \tag{4.21}$$

where $j \in \mathbb{F}_p$, $g(a;\mathbb{F}_q)$ and $g(a;p)$ are the quadratic Gauss sum in $\mathbb{F}_q$ and $\mathbb{F}_p$ (resp.), and $(-2/\mathbb{F}_q)$ and $(-2/p)$ are the Legendre's symbol in $\mathbb{F}_q$ and $\mathbb{F}_p$ (resp.). In particular, $|C(q)| = p$.

Proof. Let $\mathbb{F}_q = \{\alpha_0, \alpha_1, \cdots, \alpha_{q-1}\}$ with $\alpha_0 = 0$. Let $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$. We will prove that the $\lambda_j(q)$'s are all the eigenvalues of M_q by finding their corresponding eigenvectors.

Define $v_{\alpha_a}(q)$ as the column vector whose k entry, for $0 \le k \le q-1$, is

$$\zeta_p^{s\mathrm{Tr}\left((\alpha_k-\alpha_a)^2\right)}.$$

The j entry of $M_q v_{\alpha_a}(q)$ is

$$\sum_{k=0}^{q-1} \zeta_p^{\mathrm{Tr}(\alpha_j(\alpha_k-\alpha_j))+s\mathrm{Tr}\left((\alpha_k-\alpha_a)^2\right)}.$$

However, observe that

$$\begin{aligned} \mathrm{Tr}\left(\alpha_j(\alpha_k-\alpha_j)\right) + s\mathrm{Tr}\left((\alpha_k-\alpha_a)^2\right) &= \mathrm{Tr}\left(\alpha_j(\alpha_k-\alpha_j) + s(\alpha_k-\alpha_a)^2\right) \\ &= \mathrm{Tr}\left(\alpha_j\alpha_k - \alpha_j^2 + s\alpha_k^2 - 2s\alpha_a\alpha_k + s\alpha_a^2\right) \\ &= \mathrm{Tr}\left(-2s\alpha_j\alpha_k + 2s\alpha_j^2 + s\alpha_k^2 - 2s\alpha_a\alpha_k + s\alpha_a^2\right) \\ &= \mathrm{Tr}\left(s(\alpha_k-\alpha_a-\alpha_j)^2 + s\alpha_j^2 - 2s\alpha_a\alpha_j\right). \end{aligned} \tag{4.22}$$

This implies that the j entry of $M_q v_{\alpha_a}(q)$ is

$$\sum_{k=0}^{q-1} \zeta_p^{\mathrm{Tr}\left(s(\alpha_k-\alpha_a-\alpha_j)^2+s\alpha_j^2-2s\alpha_a\alpha_j\right)} = g(s;\mathbb{F}_q)\zeta_p^{\mathrm{Tr}\left(s(\alpha_j-\alpha_a)^2-s\alpha_a^2\right)}$$

Observe that this is $g(s;\mathbb{F}_q)\zeta_p^{\mathrm{Tr}\left(-s\alpha_a^2\right)}$ times the j entry in $v_{\alpha_a}(q)$. Therefore, $v_{\alpha_a}(q)$ is an eigenvector with eigenvalue

$$g(s;\mathbb{F}_q)\zeta_p^{\mathrm{Tr}\left(-s\alpha_a^2\right)} = \left(\frac{s}{\mathbb{F}_q}\right) g(1;\mathbb{F}_q)\zeta_p^{\mathrm{Tr}\left(-s\alpha_a^2\right)} = \left(\frac{-2}{\mathbb{F}_q}\right) g(1;\mathbb{F}_q)\zeta_p^{-s\mathrm{Tr}\left(\alpha_a^2\right)}.$$

The claim that the eigenvalues of M_q are all of the form

$$\left(\frac{-2}{\mathbb{F}_q}\right) g(1;\mathbb{F}_q)\zeta_p^b = (-1)^{r-1}\left(\frac{-2}{p}\right)^r g(1;p)^r\zeta_p^b, \quad \text{for } b \in \mathbb{F}_p$$

follows from the fact that the function $f : \mathbb{F}_q \to \mathbb{F}_p$ given by $f(\alpha_a) = -s\mathrm{Tr}(\alpha_a)$ is surjective and the classical formulas

$$\left(\frac{a}{\mathbb{F}_q}\right) = \left(\frac{a}{p}\right)^r \quad \text{and} \quad g(1;\mathbb{F}_q) = (-1)^{r-1}g(1;p)^r. \tag{4.23}$$

The linear independence of the vectors $v_{\alpha_a}(q)$, for $0 \le a \le q-1$ (see next proposition) completes the proof. □

In order for the proof of Theorem 4.4 to be complete, we need to show that the vectors $v_{\alpha_a}(q)$, for $0 \le a \le q-1$, are linearly independent. However, this is a consequence of the following (beautiful) result.

Proposition 4.5. *The matrix A_q, whose a-th row is given by $v_{\alpha_a}(q)^T$, is complex Hadamard, i.e. $A_q \cdot \overline{A_q}^T = qI_q$ where I_q is the $q \times q$ identity matrix. In particular, the vectors $v_{\alpha_a}(q)$, for $0 \le a \le q-1$, are linearly independent.*

Proof. Let $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$. By definition,

$$v_{\alpha_j}(q)^T = \left(\zeta_p^{-s\mathrm{Tr}\left((\alpha_0-\alpha_j)^2\right)}, \zeta_p^{-s\mathrm{Tr}\left((\alpha_1-\alpha_j)^2\right)}, \cdots, \zeta_p^{-s\mathrm{Tr}\left((\alpha_{q-1}-\alpha_j)^2\right)}\right).$$

It is clear that

$$v_{\alpha_j}(q)^T \cdot \overline{v_{\alpha_j}(q)}^T = q.$$

On the other hand, suppose that $0 \leq k, j \leq q-1$ and $k \neq j$. Then,

$$\begin{aligned} v_{\alpha_k}(q)^T \cdot \overline{v_{\alpha_j}(q)}^T &= \sum_{m=0}^{q-1} \zeta_p^{s\mathrm{Tr}\left((\alpha_m-\alpha_k)^2\right)-s\mathrm{Tr}\left((\alpha_m-\alpha_j)^2\right)} \\ &= \sum_{m=0}^{q-1} \zeta_p^{s\mathrm{Tr}\left(2(\alpha_j-\alpha_k)\alpha_m+\alpha_k^2-\alpha_j^2\right).} \end{aligned}$$

However, the function $f(X) = 2s(\alpha_j - \alpha_k)X + \alpha_k^2 - \alpha_j^2$ is a bijection of $\mathbb{F}_q$. Thus,

$$\begin{aligned} v_{\alpha_k}(q)^T \cdot \overline{v_{\alpha_j}(q)}^T &= \sum_{m=0}^{q-1} \zeta_p^{s\mathrm{Tr}\left(2(\alpha_j-\alpha_k)\alpha_m+\alpha_k^2-\alpha_j^2\right)} \\ &= \sum_{\beta\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(\beta)} = 0. \end{aligned}$$

We conclude that A_q is complex Hadamard. □

Observe that Theorem 4.4 and Proposition 4.5 imply that, for $q = p^r$ with p odd prime and $r > 1$, the minimal polynomial for the sequence $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,2})\}$ is

$$\mu_q(X) = \prod_{j=0}^{p-1} \left(X - \lambda_j(q)\right).$$

In particular, we have the following corollary.

Corollary 4.6. *Let $q = p^r$ with p odd prime and $r > 1$. Then,*

$$\begin{aligned} S_{\mathbb{F}_q}(\boldsymbol{e}_{n,2}) &= \sum_{j=0}^{p-1} c_j(q)\lambda_j(q)^n \\ &= \sum_{j=0}^{p-1} c_j(q) \left(\frac{-2}{\mathbb{F}_q}\right)^n g(1;\mathbb{F}_q)^n \zeta_p^{jn} \\ &= \left(\frac{-2}{\mathbb{F}_q}\right)^n g(1;\mathbb{F}_q)^n \sum_{j=0}^{p-1} c_j(q)\zeta_p^{jn} \end{aligned} \tag{4.24}$$

for some suitable constants $c_j(q)$. Moreover, the constants $c_j(q)$'s depend on the $\lambda_k(q)$'s and the values $S_{\mathbb{F}_q}(\sigma_{m,2})$ for $m = 2, 3, \cdots, p+1$.

Proof. The first claim is consequence of Theorem 4.4, Proposition 4.5 and the theory of linear recurrences. The second claim follows by solving the linear system

$$\begin{pmatrix} \lambda_0(q)^2 & \lambda_1(q)^2 & \cdots & \lambda_{p-1}(q)^2 \\ \lambda_0(q)^3 & \lambda_1(q)^3 & \cdots & \lambda_{p-1}(q)^3 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_0(q)^{p+1} & \lambda_1(q)^{p+1} & \cdots & \lambda_{p-1}(q)^{p+1} \end{pmatrix} \begin{pmatrix} c_0(q) \\ c_1(q) \\ \vdots \\ c_{p-1}(q) \end{pmatrix} = \begin{pmatrix} S_{\mathbb{F}_q}(\boldsymbol{e}_{2,2}) \\ S_{\mathbb{F}_q}(\boldsymbol{e}_{3,2}) \\ \vdots \\ S_{\mathbb{F}_q}(\boldsymbol{e}_{p+1,2}) \end{pmatrix}.$$

□

In practice, the calculation of the values $S_{\mathbb{F}_q}(\boldsymbol{e}_{m,2})$ for $m = 2, 3, \cdots, p+1$ might not be an easy task.

Example 4.7. Consider $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$. Let $\alpha = [X]$. Observe that

$$\left(\frac{-2}{\mathbb{F}_3}\right) = 1 \quad \text{and} \quad g(1;\mathbb{F}_q) = 3.$$

Therefore,

$$S_{\mathbb{F}_9}(\boldsymbol{e}_{n,2}) = 3^n \left(c_0(9) + c_1(9)e^{\frac{2\pi i n}{3}} + c_2(9)e^{\frac{4\pi i n}{3}}\right).$$

Using the values

$$\begin{aligned} S_{\mathbb{F}_9}(\boldsymbol{e}_{2,2}) &= 9 \\ S_{\mathbb{F}_9}(\boldsymbol{e}_{3,2}) &= 27 \\ S_{\mathbb{F}_9}(\boldsymbol{e}_{4,2}) &= 243, \end{aligned}$$

and solving the corresponding linear system we find

$$c_0(9) = \frac{5}{3}, \quad c_1(9) = \frac{2}{3}e^{\frac{4\pi i}{3}}, \quad c_2(9) = \frac{2}{3}e^{\frac{2\pi i}{3}}.$$

We conclude that

$$S_{\mathbb{F}_9}(\boldsymbol{e}_{n,2}) = 3^{n-1}\left(5 + 2e^{\frac{2i\pi(n+2)}{3}} + 2e^{\frac{2i\pi(2n+1)}{3}}\right) \tag{4.25}$$

$$= \begin{cases} 3^n & n \equiv 0,2 \mod 3 \\ 3^{n+1} & n \equiv 1 \mod 3. \end{cases} \tag{4.26}$$

A similar argument produces the identities

$$\begin{aligned} S_{\mathbb{F}_{25}}(\boldsymbol{e}_{n,2}) &= (-1)^n 5^{n-1}\left(6e^{\frac{(2n+3)i\pi}{5}} + 6e^{\frac{3(2n+3)i\pi}{5}} + 6e^{\frac{(4n+1)i\pi}{5}} + 6e^{\frac{(8n+7)i\pi}{5}} - 1\right) \\ &= \begin{cases} (-5)^n & n \not\equiv 1 \mod 5 \\ (-5)^{n+1} & n \equiv 1 \mod 5. \end{cases} \end{aligned} \tag{4.27}$$

$$\begin{aligned} S_{\mathbb{F}_{27}}(\boldsymbol{e}_{n,2}) &= (-i)^n 3^{\frac{1}{2}(3n-1)}\left(4e^{\frac{1}{6}i\pi(4n-1)} + 2e^{\frac{1}{6}i\pi(8n-5)} + 3i\right) \\ &= \begin{cases} \left(-3i\sqrt{3}\right)^n & n \equiv 0 \mod 3 \\ -\left(-3i\sqrt{3}\right)^{n+1} & n \equiv 1 \mod 3 \\ -\left(-3i\sqrt{3}\right)^n & n \equiv 2 \mod 3. \end{cases} \end{aligned}$$

$$\begin{aligned} S_{\mathbb{F}_{81}}(\boldsymbol{e}_{n,2}) &= (-1)^n 3 \times 9^{n-1}\left(10e^{\frac{\pi}{3}i(2n+1)} + 10e^{\frac{\pi}{3}i(4n-1)} - 7\right) \\ &= \begin{cases} (-9)^n & n \not\equiv 1 \mod 3 \\ (-9)^{n+1} & n \equiv 1 \mod 3. \end{cases} \end{aligned}$$

Note that in all these examples $S_{\mathbb{F}_q}(\boldsymbol{e}_{n,2}) \neq 0$ for every n. This is evidence of a conjecture presented in [1].

Example 4.8. The value of $S_{\mathbb{F}_{3^r}}(\boldsymbol{e}_{n,2})$ is given by

$$S_{\mathbb{F}_{3^r}}(\boldsymbol{e}_{n,2}) = c_0\lambda_0^n + c_1\lambda_1^n + c_2\lambda_2^n, \tag{4.28}$$

where

$$\begin{aligned} \lambda_j = \lambda_j(3^r) &= (-1)^{r-1}(i\sqrt{3})^r e^{\frac{2\pi i j}{3}}, \\ c_j = c_j(3^r) &= \frac{S_{\mathbb{F}_{3^r}}(\boldsymbol{e}_{2,2})\lambda_{[1+j]}\lambda_{[2+j]} - S_{\mathbb{F}_{3^r}}(\boldsymbol{e}_{3,2})\left(\lambda_{[1+j]} + \lambda_{[2+j]}\right) + S_{\mathbb{F}_{3^r}}(\boldsymbol{e}_{4,2})}{{\lambda_{[j]}}^2\left(\lambda_{[j]} - \lambda_{[1+j]}\right)\left(\lambda_{[j]} - \lambda_{[2+j]}\right)}, \end{aligned}$$

and $[a]$ represents the unique integer $l \in \{0,1,2\}$ such that $a \equiv l \mod 3$.

Theorem 4.4 and Corollary 4.6 do not apply when q even. However, not everything is lost for that case. In the previous section we observed that if q is even, then the matrix $Deph(M_q)$ seems to be a permutation away from the Sylvester matrix.

Theorem 4.9. *$Deph(M_{2^r})$ is a permutation away from the Sylvester matrix H_{2^r}.*

Proof. Let $q = p^r$ with p a prime and r a positive integer. Let $f : \mathbb{F}_q \to \mathbb{C}$ be a function and set $\zeta_p = e^{2\pi i/p}$. The *Walsh transform* of f, denoted by $\hat{f}$, is defined by

$$\hat{f}(\alpha) = \sum_{\beta \in \mathbb{F}_q} f(\beta)\zeta_p^{\mathrm{Tr}(\alpha\beta)}, \tag{4.29}$$

where $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ (see [22] for more details). Let $\alpha \in \mathbb{F}_q$ be a primitive element, that is, $\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{q-2}\}$. The Walsh transform can be written in matrix form as

$$\begin{pmatrix} \hat{f}(0) \\ \hat{f}(1) \\ \hat{f}(\alpha) \\ \vdots \\ \hat{f}(\alpha^{q-2}) \end{pmatrix} = \begin{pmatrix} \zeta_p^{\mathrm{Tr}(0\cdot 0)} & \zeta_p^{\mathrm{Tr}(0\cdot 1)} & \zeta_p^{\mathrm{Tr}(0\cdot \alpha)} & \cdots & \zeta_p^{\mathrm{Tr}(0\cdot \alpha^{q-2})} \\ \zeta_p^{\mathrm{Tr}(1\cdot 0)} & \zeta_p^{\mathrm{Tr}(1\cdot 1)} & \zeta_p^{\mathrm{Tr}(1\cdot \alpha)} & \cdots & \zeta_p^{\mathrm{Tr}(1\cdot \alpha^{q-2})} \\ \zeta_p^{\mathrm{Tr}(\alpha\cdot 0)} & \zeta_p^{\mathrm{Tr}(\alpha\cdot 1)} & \zeta_p^{\mathrm{Tr}(\alpha\cdot \alpha)} & \cdots & \zeta_p^{\mathrm{Tr}(\alpha\cdot \alpha^{q-2})} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \zeta_p^{\mathrm{Tr}(\alpha^{q-2}\cdot 0)} & \zeta_p^{\mathrm{Tr}(\alpha^{q-2}\cdot 1)} & \zeta_p^{\mathrm{Tr}(\alpha^{q-2}\cdot \alpha)} & \cdots & \zeta_p^{\mathrm{Tr}(\alpha^{q-2}\cdot \alpha^{q-2})} \end{pmatrix} \begin{pmatrix} f(0) \\ f(1) \\ f(\alpha) \\ \vdots \\ f(\alpha^{q-2}) \end{pmatrix} \tag{4.30}$$

The matrix in equation (4.30) is known as the *Walsh Transform Matrix* and it is usually denoted by W_q. The careful reader probably noticed that this is the same notation used for the Discrete Fourier Matrix. That is because the Walsh Transform matrix of order q for q prime coincides (upon rescaling) with the Fourier Transform Matrix of the same order.

It is known that when $q = 2^r$, W_q is equal, up to a permutation of columns, to the matrix obtained by letting $W_1 = (1)$,

$$\begin{aligned} W_2 &= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ W_{2^r} &= W_2 \otimes W_{2^{r-1}}. \end{aligned} \tag{4.31}$$

Observe that if $\sigma = (1\,2)$, then $W_2 = \sigma(H_2)$. Moreover,

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \text{ and } W_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{4.32}$$

Thus, if $\sigma = (1\,4)(2\,3)$, then $W_4 = \sigma(H_4)$. In general, if σ is the permutation

$$\sigma = (1\ 2^r)(2\ 2^r - 1)\cdots(2^{r-1}\ 2^{r-1} + 1),$$

then $W_{2^r} = \sigma(H_{2^r})$. Therefore, the Walsh transform matrix W_{2^r} is a permutation away from the Sylvester matrix H_{2^r} (in fact, in other contexts, the Walsh transform matrix W_{2^r} *is* the Sylvester matrix).

Let us revisit our matrix M_q. Observe that if we index our matrix by the elements of $\mathbb{F}_q$, then the (β, γ) entry of M_q is

$$e^{\frac{2\pi i}{p}\mathrm{Tr}(\beta\lambda_{-\beta}(\gamma))} = \zeta_p^{\mathrm{Tr}(\beta\lambda_{-\beta}(\gamma))} = \zeta_p^{\mathrm{Tr}(\beta(\gamma-\beta))}. \tag{4.33}$$

This implies that the (β, γ) entry of $Deph(M_q)$ is

$$\begin{aligned} \zeta_p^{\mathrm{Tr}(\beta\lambda_{-\beta}(\gamma))} \cdot \zeta_p^{-\mathrm{Tr}(\beta\lambda_{-\beta}(0))} &= \zeta_p^{\mathrm{Tr}(\beta\lambda_{-\beta}(\gamma)) - \mathrm{Tr}(\beta\lambda_{-\beta}(0))} \\ &= \zeta_p^{\mathrm{Tr}(\beta\lambda_{-\beta}(\gamma) - \beta\lambda_{-\beta}(0))} \\ &= \zeta_p^{\mathrm{Tr}(\beta(\gamma-\beta) - \beta(0-\beta))} \\ &= \zeta_p^{\mathrm{Tr}(\beta\gamma)}. \end{aligned} \tag{4.34}$$

In other words, $Deph(M_q) = W_q$. This implies that $Deph(M_{2^r})$ is a permutation away from H_{2^r}. This concludes the proof. □

5. Concluding remarks

We show that the recursive behavior of exponential sums of quadratic symmetric polynomials over Galois fields are dominated by Hadamard matrices. We also computed the spectrum of such matrices when working over finite fields extensions of $\mathbb{F}_p$ for p odd prime. This result allowed us to provide closed formulas for the corresponding exponential sums. It would be nice if similar results can be found for the associated matrices of symmetric polynomials of higher degree.

References

[1] R. A. Arce-Nazario, F. N. Castro, O. E. González, L. A. Medina and I. M. Rubio. New families of balanced symmetric functions and a generalization of Cuscik, Li and P. Stănică. *Designs, Codes and Cryptography*, 2017, DOI: 10.1007/s10623-017-0351-7.

[2] L.D. Baumert, M. Hall Jr. Hadamard matrices of the Williamson type. *Math. Comp.*, **19**, 442–447, 1965.

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

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

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

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

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

[8] 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.

[9] F. N. Castro, O. E. González and L. A. Medina. Diophantine equations with binomial coefficients and perturbations of symmetric Boolean functions. *IEEE Trans. Inf. Theory*, 2017, DOI 10.1109/TIT.2017.2750674.

[10] R. Craigen and H. Kharaghani. A combined approach to the construction of Hadamard matrices. *Australas. J. Combin.*, **13**, 89–107, 1996.

[11] T. W. Cusick. Hamming weights of symmetric Boolean functions. *Discrete Appl. Math.* **215**, 14–19, 2016.

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

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

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

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

[16] J. Hadamard. Résolution d'une question relative aux déterminants. *Bulletin des Sciences Mathématiques*, **17**, 240–246, 1893.

[17] H. Kharaghani. A construction for Hadamard matrices. *Discrete Math.*, **120**, 115–120, 1993.

[18] H. Kharaghani and B. Tayfeh-Rezaie. Hadamard matrices of order 32. *J. Combin. Des.*, **21(5)**, 212–221, 2013.

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

[20] M. Miyamoto. A Construction of Hadamard Matrices. *J. Combinatorial Theory, Ser. A.*, **57**, 86–108, 1991.

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

[22] G. L. Mullen and D. Panario. *Handbook of Finite Fields.* Taylor & Francis, 2013

[23] Raymond E.A.C. Paley. On Orthogonal Matrices. *Journal of Mathematics and Physics*, **12**, 311–320, 1933.

[24] A. Shpilka and A. Tal. On the Minimal Fourier Degree of Symmetric Boolean Functions. *Combinatorica*, **88**, 359–377, 2014.
[25] N. J. Sloane. The On-Line Encyclopedia of Integer Sequences. `http://oeis.org/`.
[26] Douglas R. Stinson. *Combinatorial Designs: Constructions and Analysis.* Springer-Verlag, New York, 2004.
[27] P. Stănică and S. Maitra. Rotation Symmetric Boolean Functions – Count and Cryptographic Properties. *Discr. Appl. Math.*, **156**, 1567–1580, 2008
[28] P. Stănică, S. Maitra and J. Clark. Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions. *Fast Software Encryption, FSE 2004*, Lecture Notes in Computer Science, **3017**, 161–177. SpringerVerlag, 2004.
[29] J. J. Sylvester. Thoughts on Orthogonal Matrices, Simultaneous Sign Successions, and Tessellated Pavements in Two or More Colours, with Applications to Newton's Rule, Ornamental Tile-Work, and the Theory of Numbers. *Phil. Mag.*, **34**, 461–475, 1867.
[30] J.S. Wallis. On Hadamard Matrices. *J. Combinatorial Theory, Ser. A.*, **18**, 149–164, 1975.
[31] J. Williamson. Hadamard's Determinant Theorem and the Sum of Four Squares. *Duke Math. J.*, **11**, 65–81, 1944.

Department of Mathematics, University of Puerto Rico, San Juan, PR 00925
E-mail address: `franciscastr@gmail.com`

Department of Mathematics, University of Puerto Rico, San Juan, PR 00925
E-mail address: `luis.medina17@upr.edu`