RECURSIONS ASSOCIATED TO TRAPEZOID, SYMMETRIC AND ROTATION SYMMETRIC FUNCTIONS OVER GALOIS FIELDS

FRANCIS N. CASTRO, ROBIN CHAPMAN, LUIS A. MEDINA, AND L. BREHSNER SEPÚLVEDA

Abstract. Rotation symmetric Boolean functions are invariant under circular translation of indices. These functions have very rich cryptographic properties and have been used in different cryptosystems. Recently, Thomas Cusick proved that exponential sums of rotation symmetric Boolean functions satisfy homogeneous linear recurrences with integer coefficients. In this work, a generalization of this result is proved over any Galois field. That is, exponential sums over Galois fields of rotation symmetric polynomials satisfy linear recurrences with integer coefficients. In the particular case of $\mathbb{F}_2$, an elementary method is used to obtain explicit recurrences for exponential sums of some of these functions. The concept of trapezoid Boolean function is also introduced and it is showed that the linear recurrences that exponential sums of trapezoid Boolean functions satisfy are the same as the ones satisfied by exponential sums of the corresponding rotations symmetric Boolean functions. Finally, it is proved that exponential sums of trapezoid and symmetric polynomials also satisfy linear recurrences with integer coefficients over any Galois field $\mathbb{F}_q$. Moreover, the Discrete Fourier Transform matrix and some Complex Hadamard matrices appear as examples in some of our explicit formulas of these recurrences.

1. Introduction

A Boolean function is a function from the vector space $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Boolean functions are part of a beautiful branch of combinatorics with applications to many scientific areas. Some particular examples are the areas of theory of error-correcting codes and cryptography. Efficient cryptographic implementations of Boolean functions with many variables is a challenging problem due to memory restrictions of current technology. Because of this, symmetric Boolean functions are good candidates for efficient implementations. However, symmetry is a too special property and may imply that these implementations are vulnerable to attacks.

In [19], Pieprzyk and Qu introduced rotation symmetric Boolean functions. A *rotation symmetric Boolean function* in n variables is a function which is invariant under the action of the cyclic group C_n on the set $\mathbb{F}_2^n$. For example, let $X_i \in \mathbb{F}_2$ for $1 \leq i \leq n$. Define, for $1 \leq k \leq n$, the shift function

$$E_n^k(X_i) = \begin{cases} X_{i+k} & \text{if } i+k \leq n, \\ X_{i+k-n} & \text{if } i+k > n. \end{cases} \tag{1.1}$$

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

$$E_n^k(X_1, X_2, \cdots, X_n) = (E_n^k(X_1), E_n^k(X_2), \cdots, E_n^k(X_n)). \tag{1.2}$$

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

$$E_n^k(X_{i_1}X_{i_2}\cdots X_{i_t}) = E_n^k(X_{i_1})E_n^k(X_{i_2}), \cdots E_n^k(X_{i_t}). \tag{1.3}$$

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

$$F(E_n^k(X_1\cdots, X_n)) = F(X_1\cdots, X_n) \tag{1.4}$$

for every $1 \leq k \leq n$. Pieprzyk and Qu showed that these functions are useful in the design of fast hashing algorithms with strong cryptographic properties. This work sparked interest in these functions and today their study is an active area of research [3, 10, 12, 13, 14, 16, 21, 22].

Every Boolean function in n variables can be identified with a multi-variable Boolean polynomial. This polynomial is known as the algebraic normal form (ANF for short) of the Boolean function. The degree of a Boolean function $F(\mathbf{X})$ is the degree of its ANF. The ANF of a rotation symmetric Boolean function is

Date: September 11, 2018.

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

Key words and phrases. rotation functions, trapezoid functions, symmetric polynomials, exponential sums, recurrences.

very well-structured. For example, suppose we have a rotation symmetric Boolean function in 5 variables. Suppose that $X_1X_2X_3$ is part of the ANF of the function. Then, the terms

$$\begin{aligned} E_5^1(X_1X_2X_3) &= X_2X_3X_4 \\ E_5^2(X_1X_2X_3) &= X_3X_4X_5 \\ E_5^3(X_1X_2X_3) &= X_4X_5X_1 \\ E_5^4(X_1X_2X_3) &= X_5X_1X_2 \end{aligned} \tag{1.5}$$

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

$$X_2X_4, X_3X_5, X_4X_1, X_5X_2$$

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

$$\begin{aligned} R(\mathbf{X}) &= X_1X_2X_3 + X_2X_3X_4 + X_3X_4X_5 + X_4X_5X_1 + X_5X_1X_2 + \\ &\quad X_1X_3 + X_2X_4 + X_3X_5 + X_4X_1 + X_5X_2. \end{aligned} \tag{1.6}$$

Therefore, once a monomial $X_{i_1}\cdots X_{i_t}$ is part of the ANF of a rotation symmetric Boolean function, so is $E_n^k(X_{i_1}\cdots X_{i_t})$ for all $1 \leq k \leq n$. This implies that the information encoded in the ANF of a rotation symmetric Boolean function can be obtained with minimal information. Define the set

$$RSet_n(X_{i_1}\cdots X_{i_t}) = \{E_n^k(X_{i_1}\cdots X_{i_t}) \,|\, 1 \leq k \leq n\}. \tag{1.7}$$

For example,

$$RSet_5(X_1X_2X_3) = \{X_2X_3X_4, X_3X_4X_5, X_4X_5X_1, X_5X_1X_2, X_1X_2X_3\}. \tag{1.8}$$

Select as a representative for the set $RSet_n(X_{i_1}\cdots X_{i_t})$ the first element in the lexicographic order. For example, the representative for

$$\{X_2X_3X_4, X_3X_4X_5, X_4X_5X_1, X_5X_1X_2, X_1X_2X_3\}$$

is $X_1X_2X_3$. Observe that if the rotation symmetric Boolean function is not constant, then X_1 always appears in the lexicographically first element of $RSet_n(X_{i_1}\cdots X_{i_t})$. The *short algebraic normal form* (or SANF) of a rotation symmetric Boolean function is a function of the form

$$a_0 + a_1X_1 + \sum a_{1,j}X_1X_j + \cdots + a_{1,2,\cdots,n}X_1X_2\cdots X_n, \tag{1.9}$$

where $a_0, a_1, a_{1,j}, \cdots, a_{1,2,\cdots,n} \in \mathbb{F}_2$ and the existence of the term $X_1X_{i_2}\cdots X_{i_t}$ implies the existence of every term in

$$RSet_n(X_1X_{i_2}\cdots X_{i_t})$$

in the ANF. For example, the SANF of the rotation symmetric Boolean function (1.6) is given by

$$X_1X_3 + X_1X_2X_3. \tag{1.10}$$

Let $1 < j_1 < \cdots < j_s$ be integers. A rotation symmetric Boolean function of the form

$$R_{j_1,\cdots,j_s}(n) = X_1X_{j_1}\cdots X_{j_s} + X_2X_{j_1+1}\cdots X_{j_s+1} + \cdots + X_nX_{j_1-1}\cdots X_{j_s-1}, \tag{1.11}$$

where the indices are taken modulo n and the complete system of residues is $\{1, 2, \cdots, n\}$, is called a *monomial rotation symmetric* Boolean function. For example, the rotation symmetric Boolean function (1.6) is given by

$$R(\mathbf{X}) = R_{2,3}(5) + R_3(5). \tag{1.12}$$

Sometimes the notation $(1, j_1, \cdots, j_s)_n$ is used to represent the monomial rotation Boolean function (1.11), see [9].

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. Balancedness of Boolean functions can be studied from the point of view of exponential sums. The *exponential sum* of an n-variable Boolean function $F(\mathbf{X})$ is defined as

$$S(F) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{F(\mathbf{x})}. \tag{1.13}$$

Observe that a Boolean function $F(\mathbf{X})$ is balanced if and only if $S(F) = 0$. This gives importance to the study of exponential sums. This point of view is also a very active area of research. For some examples, please refer to [1, 2, 5, 6, 7, 8, 15, 17, 18, 20].

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* or F. The *Hamming weight* of F, denoted by $\mathrm{wt}(F)$, is the number of 1's in the truth table of F. Observe that a Boolean function in n variables is balanced if and only if its Hamming weight is 2^{n-1}. The Hamming weight of a Boolean function F and its exponential sums are related by the equation

$$\mathrm{wt}(F) = \frac{2^n - S(F)}{2}. \tag{1.14}$$

The study of weights of rotations symmetric Boolean functions has received some attention lately [3, 10, 12, 21]. In particular, it has been observed that weights of cubic rotation symmetric Boolean functions are linear recursive with constant coefficients [3, 10]. Recently, Cusick [9] showed that weights of any rotation symmetric Boolean function satisfy linear recurrences with integer coefficients. Since the exponential sum and the weight function of a Boolean function are related by (1.14), then it is also true that exponential sums of rotation symmetric Boolean functions satisfy linear recurrences with integer coefficients.

One of the most important results in this work is a generalization of Cusick's Theorem over any Galois field. To be specific, let $q = p^r$ with p prime and $r \geq 1$. Exponential sums over $\mathbb{F}_q$ of monomial rotation symmetric polynomials (and linear combinations of them) satisfy homogeneous linear recurrences with integer coefficients. Remarkably, this can be proved by elementary means. Another important result included in this work is that exponential sums over $\mathbb{F}_q$ of elementary symmetric polynomials and linear combinations of them also satisfy linear recurrences with integer coefficients. Surprisingly, the Discrete Fourier Transform matrix, some Complex Hadamard matrices and the quadratic Gauss sum mod p appear in the study of the recurrences considered in this work.

This article is divided as follows. The next section is an introduction of the elementary method used to obtain the recurrences. This introduction is done over $\mathbb{F}_2$ in order to solidify the intuition. The reader interested in the generalization is invited to skip this section, however, the reader is encouraged to read the definition of trapezoid functions, as they are used through out the article. In section 3 linear recurrences with integer coefficients are obtained for exponential sums trapezoid functions over Galois fields. Moreover, it is in this section where it is proved that exponential sums over $\mathbb{F}_q$ of monomial rotation symmetric polynomials and linear combinations of them satisfy linear recurrences with integer coefficients. The same technique is used in the section 4 to prove that exponential sums over $\mathbb{F}_q$ of elementary symmetric polynomials and linear combinations of them also satisfy linear recurrences with integer coefficients. Finally, in the last section, some conjectures about the initial conditions of some of the sequences considered in this work are presented.

2. Linear recurrences over $\mathbb{F}_2$

As mentioned in the introduction, Cusick [9] recently showed that exponential sums of rotation symmetric Boolean functions satisfy homogeneous linear recurrences with integer coefficients. This fact was suggested by some previous works on the subject. For example, in [12], Cusick and Stănică provided a linear recursion for the sequence of weights for the monomial rotation function $(1, 2, 3)_n$. This recursion, however, was not homogeneous, but it could be transformed into a homogeneous one, see [3]. Later, Cusick and Johns [10] provided recursions for weights of cubic rotation symmetric Boolean functions.

In this section we use elementary machinery to provide explicit homogeneous linear recurrences with integer coefficients for exponential sums of some rotation symmetric Boolean functions. The idea is to show that exponential sums of rotation symmetric Boolean functions satisfy the same linear recurrences of exponential sums of trapezoid Boolean functions (see definition below). We prove this fact using elementary machinery and, at this early stage, without the use linear algebra. In the next section we show that exponential sums of rotation symmetric functions over any Galois field satisfy linear recurrences. The reader interested in this generalization may skip this section, but not before reading the definition of trapezoid functions.

Define the *trapezoid* Boolean function in n variables of degree k as

$$\tau_{n,k} = \sum_{j=1}^{n-k+1} X_j X_{j+1} \cdots X_{j+k-1}. \tag{2.1}$$

For example,

$$\begin{aligned}\tau_{7,3} &= X_1X_2X_3 + X_2X_3X_4 + X_3X_4X_5 + X_4X_5X_6 + X_5X_6X_7\\ \tau_{6,4} &= X_1X_2X_3X_4 + X_2X_3X_4X_5 + X_3X_4X_5X_6.\end{aligned}$$

The name trapezoid comes from counting the number of times each variable appears in the function $\tau_{n,k}$. For example, consider $\tau_{7,3}$. Observe that X_1 appears 1 time in $\tau_{7,3}$, X_2 appears 2 times, X_3, X_4 and X_5 appears 3 times each, X_6 appears twice, and X_7 appears once. Plotting the these values and connecting the dots produces the shape of an isosceles trapezoid. Figure 1 is a graphical representation of this. The Boolean variable X_i is represented by i in the x-axis. The y-axis corresponds to the number of times the variable appears in $\tau_{7,3}$.

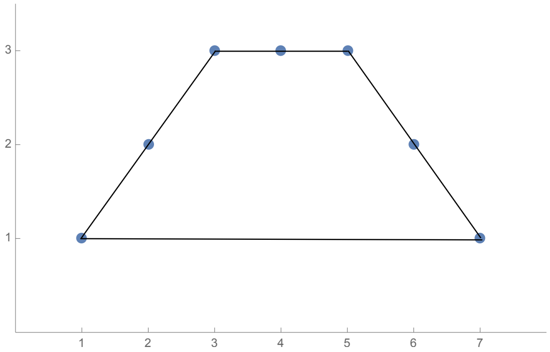

FIGURE 1. Trapezoid associated to the Boolean function $\tau_{7,3}$

The opposite is also true, that is, for every isosceles trapezoid that can be constructed by steps of length at most 1, one can construct a trapezoid Boolean function.

It turns out that sequences of exponential sums of trapezoid Boolean functions of fixed degree satisfy homogeneous linear recurrences with integer coefficients. These linear recurrences are the same satisfied by sequences of exponential sums of $(1, 2, \cdots, k)$-rotation symmetric Boolean functions. Remarkably, this fact can be proved by elementary means by "playing" a simple game of turning *ON* and *OFF* some of the variables. Given a Boolean variable X_i, we say that it is turned *OFF* if X_i assumes the value 0 and turned *ON* if the variable assumes the value 1. In other words, each Boolean variable represents a "switch" with two options: 0 (*OFF*) and 1 (*ON*).

We start the discussion with the recurrence for exponential sums of trapezoid Boolean functions.

Theorem 2.1. *The sequence $\{S(\tau_{n,k})\}_{n=k}^{\infty}$ satisfies a homogeneous linear recurrence with integer coefficients whose characteristic polynomial is given by*

$$p_k(X) = X^k - 2(X^{k-2} + X^{k-3} + \cdots + X + 1). \tag{2.2}$$

Proof. For the sake of simplicity, we present, in detail, the proof for the cases $k = 3$ and $k = 4$. The general case becomes clear after that. Moreover, the complete proof of a generalization of this theorem over any Galois field is presented in section 3.

Start with the case $k = 3$. Observe that by turning X_n *OFF* and *ON* we get the identity

$$S(\tau_{n,3}) = S(\tau_{n-1,3}) + S(\tau_{n-1,3} + X_{n-2}X_{n-1}). \tag{2.3}$$

Consider now $S(\tau_{n-1,3} + X_{n-2}X_{n-1})$. Turn X_{n-1} *OFF* and *ON* to get

$$S(\tau_{n-1,3} + X_{n-2}X_{n-1}) = S(\tau_{n-2,3}) + S(\tau_{n-2,3} + X_{n-2} + X_{n-3}X_{n-2}). \tag{2.4}$$

Finally, turn X_{n-2} *OFF* and *ON* to get

$$S(\tau_{n-2,3}+X_{n-2}+X_{n-3}X_{n-2})=S(\tau_{n-3,3})-S(\tau_{n-3,3}+X_{n-3}+X_{n-4}X_{n-3}). \tag{2.5}$$

The last equation is equivalent (after relabeling) to

$$S(\tau_{n,3})=S(\tau_{n+1,3}+X_{n+1}+X_nX_{n+1})+S(\tau_{n,3}+X_n+X_{n-1}X_n). \tag{2.6}$$

Observe that equations (2.3) and (2.4) can be combined to obtain

$$S(\tau_{n,3})=S(\tau_{n-1,3})+S(\tau_{n-2,3})+S(\tau_{n-2,3}+X_{n-2}+X_{n-3}X_{n-2}). \tag{2.7}$$

Let $a_{n,3}=S(\tau_{n,3}+X_n+X_{n-1}X_n)$. Note that (2.6) implies that $S(\tau_{n,3})=a_{n+1,3}+a_{n,3}$. Therefore, (2.7) can be re-written as

$$(a_{n+1,3}+a_{n,3})=(a_{n,3}+a_{n-1,3})+(a_{n-1,3}+a_{n-2,3})+a_{n-2,3}, \tag{2.8}$$

which is equivalent to

$$a_{n+1,3}=2a_{n-1,3}+2a_{n-2,3}. \tag{2.9}$$

This implies that $\{a_{n,3}\}$ satisfies the linear recurrence whose characteristic polynomial is given by $p_3(X)$. Since $S(\tau_{n,3})=a_{n+1,3}+a_{n,3}$, then $\{S(\tau_{n,3})\}$ also satisfies such recurrence and the result holds for $k=3$.

Consider now the case when $k=4$. As it was done in the case when $k=3$, turning *OFF* and *ON* several variables leads to

$$\begin{aligned} S(\tau_{n,4}) &= S(\tau_{n-1,4})+S(\tau_{n-2,4})+S(\tau_{n-3,4}) \\ &\quad +S(\tau_{n-3,4}+X_{n-3}+X_{n-4}X_{n-3}+X_{n-5}X_{n-4}X_{n-3}) \end{aligned} \tag{2.10}$$

and

$$\begin{aligned} S(\tau_{n,4}) &= S(\tau_{n+1,4}+X_{n+1}+X_nX_{n+1}+X_{n-1}X_nX_{n+1}) \\ &\quad +S(\tau_{n,4}+X_n+X_{n-1}X_n+X_{n-2}X_{n-1}X_n). \end{aligned} \tag{2.11}$$

Now let $a_{n,4}=S(\tau_{n,4}+X_n+X_{n-1}X_n+X_{n-2}X_{n-1}X_n)$ and observe that (2.10) can be re-written as

$$(a_{n+1,4}+a_{n,4})=(a_{n,4}+a_{n-1,4})+(a_{n-1,4}+a_{n-2,4})+(a_{n-2,4}+a_{n-3,4})+a_{n-3,4}, \tag{2.12}$$

which is equivalent to

$$a_{n+1,4}=2a_{n-1,4}+2a_{n-2,4}+2a_{n-3,4}. \tag{2.13}$$

Therefore, $\{a_{n,4}\}$ satisfies the linear recurrence whose characteristic polynomial is given by $p_4(X)$. Since $S(\tau_{n,4})=a_{n+1,4}+a_{n,4}$, then $\{S(\tau_{n,4})\}$ also satisfies such recurrence and the result also holds for $k=4$.

In general, $S(\tau_{n,k})$ can be expressed as

$$S(\tau_{n,k})=\sum_{i=1}^{k-1}S(\tau_{n-i,k})+S\left(\tau_{n-k+1,k}+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n-k+1-i}\right) \tag{2.14}$$

and as

$$S(\tau_{n,k})=S\left(\tau_{n+1,k}+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n+1-i}\right)+S\left(\tau_{n,k}+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n-i}\right). \tag{2.15}$$

Combine these equations and proceed as before to obtain the result. This concludes the proof. □

It turns out that the sequence of exponential sums of $(1,2,\cdots,k)$-rotation symmetric Boolean functions, that is, of $R_{2,3,\cdots,k}(n)$, also satisfies the linear recurrence whose characteristic polynomial is given $p_k(X)$. This is a well-known result for the case when $k=3$ ([3, 10]), but, to the knowledge of the authors, the closed formula for the general case is new. Before proving that $\{S(R_{2,3,\cdots,k}(n))\}$ satisfies the linear recurrence with characteristic polynomial $p_k(X)$, we show an auxiliary result which can be proved using the same arguments as in the proof of Theorem 2.1.

Lemma 2.2. *Let $\tau_{n,k}$ be the trapezoid Boolean function of degree k in n variables. Suppose that $F(\mathbf{X})$ is a Boolean polynomial in the first j variables with $j < k$. Then, the sequences*

$$\{S(\tau_{n,k} + F(\mathbf{X}))\}$$

and

$$\{S(\tau_{n,k} + F(\mathbf{X}) + X_n + X_nX_{n-1} + X_nX_{n-1}X_{n-2} + \cdots + X_nX_{n-1}\cdots X_{n-k+2})\}$$

satisfies the linear recurrence whose characteristic polynomial is given by $p_k(X)$.

Proof. The proof of this result follows the same argument of the proof of Theorem 2.1. □

Theorem 2.1 and Lemma 2.2 is all that is needed to show that the sequence of exponential sums of $(1, 2, \cdots, k)$-rotation symmetric Boolean functions satisfies the linear recurrence with characteristic polynomial $p_k(X)$.

Theorem 2.3. *The sequence $\{S(R_{2,3,\cdots,k}(n))\}$ satisfies the homogeneous linear recurrence whose characteristic polynomial is given by $p_k(X)$.*

Proof. This result can also be proved by turning *OFF* and *ON* several variables. As before, we provide the proof for the case when $k = 4$. The general case follows the same argument.

To start the argument, turn *OFF* and *ON* the variable X_n to get

$$S(R_{2,3,4}(n)) = S(\tau_{n-1,4}) + S(\tau_{n-1,4} + X_1X_2X_3 + X_1X_2X_{n-1} + X_1X_{n-2}X_{n-1}). \tag{2.16}$$

Consider the second term of the right hand side of this equation. Turn X_{n-1} *OFF* and *ON* to get

$$\begin{aligned} &S(\tau_{n-1,4} + X_1X_2X_3 + X_1X_2X_{n-1} + X_1X_{n-2}X_{n-1}) \\ &\quad = S(\tau_{n-2,4} + X_1X_2X_3) \\ &\quad\quad + S(\tau_{n-2,4} + X_1X_2 + X_1X_2X_3 + X_1X_{n-2} + X_{n-3}X_{n-2} + X_{n-4}X_{n-3}X_{n-2}). \end{aligned} \tag{2.17}$$

Again, consider the second term of the right hand side of equation (2.17). Turn X_{n-2} *OFF* and *ON* to get

$$\begin{aligned} &S(\tau_{n-2,4} + X_1X_2 + X_1X_2X_3 + X_1X_{n-2} + X_{n-3}X_{n-2} + X_{n-4}X_{n-3}X_{n-2}) \\ &\quad = S(\tau_{n-3,4} + X_1X_2 + X_1X_2X_3) \\ &\quad\quad + S(\tau_{n-3,4} + X_1 + X_1X_2 + X_1X_2X_3 + X_{n-3} + X_{n-4}X_{n-3} + X_{n-5}X_{n-4}X_{n-3}). \end{aligned} \tag{2.18}$$

Equations (2.16), (2.17) and (2.18) lead to the equation

$$\begin{aligned} S(R_{2,3,4}(n)) &= S(\tau_{n-1,4}) + S(\tau_{n-2,4} + X_1X_2X_3) + S(\tau_{n-3,4} + X_1X_2 + X_1X_2X_3) \\ &\quad + S(\tau_{n-3,4} + X_1 + X_1X_2 + X_1X_2X_3 + X_{n-3} + X_{n-4}X_{n-3} + X_{n-5}X_{n-4}X_{n-3}). \end{aligned} \tag{2.19}$$

Theorem 2.1 and Lemma 2.2 imply that $\{S(\tau_{n-1,4})\}$, $\{S(\tau_{n-2,4}+X_1X_2X_3)\}$, $\{S(\tau_{n-3,4}+X_1X_2+X_1X_2X_3)\}$ and

$$\{S(\tau_{n-3,4} + X_1 + X_1X_2 + X_1X_2X_3 + X_{n-3} + X_{n-4}X_{n-3} + X_{n-5}X_{n-4}X_{n-3})\}$$

satisfy the linear recurrence whose characteristic polynomial $p_4(X)$. Since $\{S(R_{2,3,4}(n))\}$ is a linear combination of them, then the result holds when $k = 4$.

In general, $S(R_{2,3,\cdots,k}(n))$ can be expressed as

$$\begin{aligned} S(R_{2,3,\cdots,k}(n)) &= S(\tau_{n-1,k}) + \sum_{m=0}^{k-3} S\left(\tau_{n-2-m,k} + \sum_{j=0}^{m} \prod_{i=1}^{k-1-j} X_i\right) \\ &\quad + S\left(\tau_{n-k+1,k} + \sum_{j=1}^{k-1}\left(\prod_{i=1}^{j} X_i + \prod_{i=0}^{j-1} X_{n-k+1-i}\right)\right) \end{aligned} \tag{2.20}$$

Invoke Theorem 2.1 and Lemma 2.2 to get the result. This concludes the proof. □

The same technique can be applied to find linear recurrences of exponential sums other rotations. Recall that

$$R_{j_1,\cdots,j_s}(n) = X_1X_{j_1}\cdots X_{j_s} + X_2X_{j_1+1}\cdots X_{j_s+1} + \cdots + X_nX_{j_1-1}\cdots X_{j_s-1}, \tag{2.21}$$

where the indices are taken modulo n and the complete system of residues is $\{1, 2, \cdots, n\}$. We define the equivalent of the trapezoid Boolean function for $R_{j_1,\cdots,j_s}(n)$ as

$$T_{j_1,\cdots,j_s}(n) = X_1X_{j_1}\cdots X_{j_s} + X_2X_{j_1+1}\cdots X_{j_s+1} + \cdots + X_{n+1-j_s}X_{j_1+n-j_s}\cdots X_{j_{s-1}+n-j_s}X_n. \tag{2.22}$$

For instance, under this notation one has

$$\tau_{n,k} = T_{2,3,\cdots,k}(n). \tag{2.23}$$

It turns out that for $k \geq 4$, the sequences $\{S(R_{2,3,\cdots,k-2,k}(n))\}$ and $\{S(R_{2,3,\cdots,k-2,k+1}(n))\}$ both satisfy the linear recurrence whose characteristic polynomial is

$$q_k(X) = X^{k+1} - 2X^{k-1} - 2X^{k-2} - \cdots - 2X^3 - 4. \tag{2.24}$$

As just mentioned, this can be proved by playing a game of turning *ON* and *OFF* some variables. However, the process becomes somewhat tedious at a very early stage.

For example, recall that Theorem 2.1 is an auxiliary result that was used to show that $\{S(R_{2,3,\cdots,k}(n))\}$ satisfies the linear recurrence with characteristic polynomial $p_k(X)$. Let us show the equivalent of Theorem 2.1 for $\{S(R_{2,4}(n))\}$. The idea is to show the reader how tedious the process can get. Recall that the equivalent of the trapezoid Boolean function for this problem is

$$T_{2,4}(n) = X_1X_2X_4 + X_2X_3X_5 + \cdots + X_{n-3}X_{n-2}X_n. \tag{2.25}$$

Start with the equation

$$\begin{aligned} S(T_{2,4}(n) + X_{n-1}X_n) \quad &= \quad S(T_{2,4}(n+1) + X_{n-1}X_n + X_{n+1} + X_nX_{n+1}) + \\ &\quad\;\; S(T_{2,4}(n) + X_{n-2}X_{n-1} + X_n + X_{n-1}X_n), \end{aligned} \tag{2.26}$$

which is a consequence of turning *OFF* and *ON* the variable X_{n+1}. On the other hand, by turning X_n *OFF* and *ON* one gets

$$S(T_{2,4}(n) + X_{n-1}X_n) \quad = \quad S(T_{2,4}(n-1) + S(T_{2,4}(n-1) + X_{n-1} + X_{n-2}X_{n-3}). \tag{2.27}$$

This gave us two equations for $S(T_{2,4}(n) + X_{n-1}X_n)$.

Consider now the right hand side of (2.27). Turn X_{n-1} *OFF* and *ON* to get

$$\begin{aligned} S(T_{2,4}(n-1) + X_{n-1} + X_{n-2}X_{n-3}) \quad &= \quad S(T_{2,4}(n-2) + X_{n-2}X_{n-3}) - \\ &\quad\;\; S(T_{2,4}(n-2) + X_{n-4}X_{n-3} + X_{n-3}X_{n-2}) \end{aligned} \tag{2.28}$$

Now turn X_{n-2} *OFF* and *ON* to get the equation

$$\begin{aligned} S(T_{2,4}(n-2) + X_{n-4}X_{n-3} + X_{n-3}X_{n-2}) \quad &= \quad S(T_{2,4}(n-3) + X_{n-4}X_{n-3}) + \\ &\quad\;\; S(T_{2,4}(n-3) + X_{n-5}X_{n-4} + X_{n-3} + X_{n-4}X_{n-3}). \end{aligned} \tag{2.29}$$

Combine equations (2.26), (2.27), (2.28), and (2.29) to get

$$\begin{aligned} S(T_{2,4}(n) \quad &= \quad S(T_{2,4}(n+1) + X_nX_{n+1}) - S(T_{2,4}(n-1) + X_{n-2}X_{n-1}) + S(T_{2,4}(n-2) + X_{n-3}X_{n-2}) \\ &\quad\;\; +S(T_{2,4}(n-2) + X_{n-4}X_{n-3} + X_{n-2} + X_{n-3}X_{n-2}). \end{aligned} \tag{2.30}$$

Now let $a_n = S(T_{2,4}(n) + X_{n-2}X_{n-1} + X_n + X_{n-1}X_n)$. Observe that equation (2.26) can be re-written as

$$S(T_{2,4}(n) + X_{n-1}X_n) = a_{n+1} + a_n. \tag{2.31}$$

This and equation (2.30) imply

$$\begin{aligned} S(T_{2,4}(n)) \quad &= \quad (a_{n+2} + a_{n+1}) - (a_n + a_{n-1}) + (a_{n-1} + a_{n-2}) + a_{n-2} \\ &= \quad a_{n+2} + a_{n+1} - a_n + 2a_{n-2}. \end{aligned} \tag{2.32}$$

On the other hand, by switching *OFF* and *ON* several variables one obtains

$$\begin{aligned} S(T_{2,4}(n)) \quad &= \quad S(T_{2,4}(n-1)) + S(T_{2,4}(n-2) + X_{n-3}X_{n-2}) + S(T_{2,4}(n-3) + X_{n-4}X_{n-3}) \\ &\quad\;\; +S(T_{2,4}(n-3) + X_{n-5}X_{n-4} + X_{n-3} + X_{n-4}X_{n-3}). \end{aligned} \tag{2.33}$$

Writing this last equation in terms of a_n one gets

$$\begin{aligned} (a_{n+2} + a_{n+1} - a_n + 2a_{n-2}) \quad &= \quad (a_{n+1} + a_n - a_{n-1} + 2a_{n-3}) \\ &\quad\;\; +(a_{n-1} + a_{n-2}) + (a_{n-2} + a_{n-3}) + a_{n-3}, \end{aligned} \tag{2.34}$$

which simplifies to

$$a_{n+2} = 2a_n + 4a_{n-3}. \tag{2.35}$$

The characteristic polynomial for this recurrence is $q_3(X)$.

Other examples on which this elementary method can be used to find explicit formulas for linear recurrences include the sequence

$$\{S(R_{2,3,\cdots,k}(n) + R_{2,3,\cdots,k-1}(n))\}, \tag{2.36}$$

which satisfies the linear recurrence with characteristic polynomial

$$x^k - 2x^{k-1} + 2, \tag{2.37}$$

the sequence

$$\{S(R_{2,3,\cdots,k-1,k}(n) + R_{2,3,\cdots,k-2,k}(n))\}, \tag{2.38}$$

which satisfies the linear recurrence with characteristic polynomial

$$x^k - 2x^{k-1} + 2x - 2, \tag{2.39}$$

and the sequence

$$\{S(R_{2,3,\cdots,k-2,k}(n) + R_{2,3,\cdots,k-1}(n) + R_{2,3,\cdots,k}(n))\}, \tag{2.40}$$

which satisfies the linear recurrence with characteristic polynomial

$$x^k - 2(x^{k-2} + x^{k-3} + \cdots + x^2 + 1). \tag{2.41}$$

However, the process is somewhat tedious to be done by hand. Automatization seems to be the way to go. The reader is invited to read Cusick's work [9], which includes a *Mathematica* code that calculates a linear recurrences for the weights of a given rotation.

3. Linear recurrences over $\mathbb{F}_q$

In this section we show that exponential sums of rotation functions over Galois fields satisfy linear recurrence. This is a generalization of Cusick's result.

Consider the Galois field $\mathbb{F}_q = \{0, \alpha_1, \cdots, \alpha_{q-1}\}$ 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 given by

$$S_{\mathbb{F}_q}(F) = \sum_{\mathbf{x} \in \mathbb{F}_q^n} e^{\frac{2\pi i}{p} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(F(\mathbf{x}))}, \tag{3.1}$$

where $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ represents the field trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. The same technique used for exponential sums of Boolean functions can be used in general. However, instead of having two options for the "switch", we now have q of them. Let X be a variable which takes values on $\mathbb{F}_q$. As before, we say that the variable X can be turned *OFF* or *ON*, however, this time the term "turn *OFF*" means that X assumes the value 0, while the term "turn *ON*" means that X assumes all values in $\mathbb{F}_q$ that are different from zero. Think of this situation as a light switch on which you have the option to turn *OFF* the light and the option to turn it *ON* to one of $q - 1$ colors.

We consider first sequences exponential sums of trapezoid functions. As in the case over $\mathbb{F}_2$, they satisfy linear recurrences with integer coefficients over any Galois field $\mathbb{F}_q$. We start with the following lemma, which is interesting in its own right.

Lemma 3.1. *Let k, n and j be integers with $k > 2$, $1 \leq j < k$ and $n \geq k$. Then,*

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{n-l}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j} \prod_{l=0}^{k-s-1} X_{n-l}\right) \tag{3.2}$$

for any choice of $\beta_s \in \mathbb{F}_q^{\times}$.

Proof. The proof is by induction on n. Suppose first that $n = k$. Observe that

$$\begin{aligned} T_{2,3,\cdots,k}(k) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{k-l} &= X_1 X_2 \cdots X_k + \beta_j X_{j+1} X_{j+2} \cdots X_k + \beta_{j-1} X_j X_{j+1} \cdots X_k \\ &\quad + \cdots + \beta_2 X_3 X_4 \cdots X_k + \beta_1 X_2 X_3 \cdots X_k. \end{aligned} \tag{3.3}$$

Consider the right hand side of (3.3). If $1 \leq j \leq k-2$, then make the changes of variables

$$\begin{aligned} X_t &= Y_t, \quad \text{for } j+2 \leq t \leq k \\ X_{j+1} &= \beta_j^{-1} Y_{j+1} \\ X_t &= \beta_{t-1}^{-1} \beta_t Y_t, \quad \text{for } 2 \leq t \leq j \\ X_1 &= \beta_1 Y_1. \end{aligned}$$

On the other hand, if $j = k-1$, then make the change of variables

$$\begin{aligned} X_k &= \beta_{k-1}^{-1} Y_k \\ X_t &= \beta_{t-1}^{-1} \beta_t Y_t, \quad \text{for } 2 \leq t \leq k-1 \\ X_1 &= \beta_1 Y_1. \end{aligned}$$

This transforms (3.3) into

$$Y_1 Y_2 \cdots Y_k + \sum_{s=1}^{j} \prod_{l=0}^{k-s-1} Y_{k-l}. \tag{3.4}$$

Therefore,

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(k) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{k-l}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(k) + \sum_{s=1}^{j} \prod_{l=0}^{k-s-1} X_{k-l}\right). \tag{3.5}$$

This concludes the base case.

Suppose now that for some $n \geq k$ we have

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{n-l}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j} \prod_{l=0}^{k-s-1} X_{n-l}\right). \tag{3.6}$$

Consider

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n+1) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{n+1-l}\right). \tag{3.7}$$

Suppose first that $1 \leq j \leq k-2$. Letting X_{n+1} run over every element of the field leads to

$$\begin{aligned} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n+1) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{n+1-l}\right) &= S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)\right) \\ &\quad + \sum_{\alpha \in \mathbb{F}_q^{\times}} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j+1} \gamma_s(\alpha) \prod_{l=0}^{k-s-1} X_{n-l}\right), \end{aligned} \tag{3.8}$$

where $\gamma_1(\alpha) = \alpha$ and $\gamma_s(\alpha) = \alpha\beta_{s-1}$. By induction

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j+1} \gamma_s(\alpha) \prod_{l=0}^{k-s-1} X_{n-l}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j+1} \prod_{l=0}^{k-s-1} X_{n-l}\right). \tag{3.9}$$

Therefore,

$$\begin{aligned} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n+1)+\sum_{s=1}^{j}\beta_s\prod_{l=0}^{k-s-1}X_{n+1-l}\right) &= S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)\right) \\ &+\sum_{\alpha\in\mathbb{F}_q^\times}S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{s=1}^{j+1}\prod_{l=0}^{k-s-1}X_{n-l}\right). \end{aligned} \tag{3.10}$$

However, (3.10) does not depend on the choice of the β_t's. It follows that

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n+1)+\sum_{s=1}^{j}\beta_s\prod_{l=0}^{k-s-1}X_{n+1-l}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n+1)+\sum_{s=1}^{j}\prod_{l=0}^{k-s-1}X_{n+1-l}\right)$$

is true for $1\leq j\leq k-2$.

Consider now the case $j=k-1$. Again, letting X_{n+1} run over every element of the field leads to

$$\begin{aligned} S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n+1)+\sum_{s=1}^{k-1}\beta_s\prod_{l=0}^{k-s-1}X_{n+1-l}) &= S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)\right) \\ &+\sum_{\alpha\in\mathbb{F}_q^\times}e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha\beta_{k-1})}S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{s=1}^{k-1}\gamma_s(\alpha)\prod_{l=0}^{k-s-1}X_{n-l}\right), \end{aligned} \tag{3.11}$$

where $\gamma_1(\alpha)=\alpha$ and $\gamma_s(\alpha)=\alpha\beta_{s-1}$. However, by induction

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{s=1}^{k-1}\gamma_s(\alpha)\prod_{l=0}^{k-s-1}X_{n-l}\right)=S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{s=1}^{j+1}\prod_{l=0}^{k-s-1}X_{n-l}\right). \tag{3.12}$$

Since

$$\sum_{\alpha\in\mathbb{F}_q^\times}e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha\beta_{k-1})}=-1, \tag{3.13}$$

then it follows that

$$\begin{aligned} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n+1)+\sum_{s=1}^{k-1}\beta_s\prod_{l=0}^{k-s-1}X_{n+1-l}\right) &= S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)\right) \\ &-\sum_{\alpha\in\mathbb{F}_q^\times}S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{s=1}^{k-1}\prod_{l=0}^{k-s-1}X_{n-l}\right). \end{aligned} \tag{3.14}$$

Since (3.10) does not depend on the choice of the β_t's, then it follows that

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n+1)+\sum_{s=1}^{k-1}\beta_s\prod_{l=0}^{k-s-1}X_{n+1-l}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n+1)+\sum_{s=1}^{k-1}\prod_{l=0}^{k-s-1}X_{n+1-l}\right)$$

is true. This completes the induction and the proof. □

Next is the recurrence for exponential sums of trapezoid functions over any Galois field.

Theorem 3.2. *Let $k\geq 2$ be an integer and $q=p^r$ with p prime. The sequence $\{S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n))\}_{n=k}^{\infty}$ satisfies a homogeneous linear recurrence with integer coefficients whose characteristic polynomial is given by*

$$Q_{T,k,\mathbb{F}_q}(X)=X^k-q\sum_{l=0}^{k-2}(q-1)^lX^{k-2-l}. \tag{3.15}$$

In particular, when $q=2$ we recover Theorem 2.1.

Proof. We present the proof for $k > 2$. The case $k = 2$ can be proved using similar techniques. Start by turning X_n *OFF* and *ON*, that is, by letting X_n assume all its possible values. This produces the identity

$$S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) = S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n-1)) + \sum_{\beta\in\mathbb{F}_q^{\times}} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-1) + \beta\prod_{j=1}^{k-1} X_{n-j}\right) \tag{3.16}$$

However, Lemma 3.1 implies

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-1) + \beta\prod_{j=1}^{k-1} X_{n-j}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-1) + \prod_{j=1}^{k-1} X_{n-j}\right) \tag{3.17}$$

for every $\beta \in \mathbb{F}_q^{\times}$. Therefore, (3.16) reduces to

$$S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) = S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n-1)) + (q-1)S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-1) + \prod_{j=1}^{k-1} X_{n-j}\right) \tag{3.18}$$

Consider now $S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-1) + \prod_{j=1}^{k-1} X_{n-j}\right)$. Let X_{n-1} assume all its possible values and use the same argument as before to get

$$\begin{aligned} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-1) + \prod_{j=1}^{k-1} X_{n-j}\right) &= S_{\mathbb{F}_p}\left(T_{2,3,\cdots,k}(n-2)\right) \\ &\quad +(q-1)S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-2) + \prod_{j=1}^{k-2} X_{n-1-j} + \prod_{j=1}^{k-1} X_{n-1-j}\right) \end{aligned} \tag{3.19}$$

Thus, (3.18) reduces to

$$\begin{aligned} S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) &= S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n-1)) + (q-1)S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-2)\right) \\ &\quad +(q-1)^2 S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-2) + \prod_{j=1}^{k-2} X_{n-1-j} + \prod_{j=1}^{k-1} X_{n-1-j}\right). \end{aligned} \tag{3.20}$$

Continue in this manner to get the following equation

$$\begin{aligned} S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) &= \sum_{l=1}^{k-1}(q-1)^{l-1} S_{\mathbb{F}_q} T_{2,3,\cdots,k}(n-l)) \\ &\quad +(q-1)^{k-1} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-k+1) + \sum_{j=0}^{k-2}\prod_{l=0}^{j} X_{n-k+1-l}\right). \end{aligned} \tag{3.21}$$

On the other hand, let X_{n+1} assume all its possible values and use Lemma 3.1 to get the equation

$$\begin{aligned} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n+1)+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n+1-l}\right) &= S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) \\ &+e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(1)}S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n-l}\right) \\ &+e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(2)}S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n-l}\right) \\ &+e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(3)}S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n-l}\right) \\ &\vdots \\ &+e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha_{p-1})}S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n-l}\right). \end{aligned} \tag{3.22}$$

Use the well-known formula

$$\sum_{\beta\in\mathbb{F}_q^{\times}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta)} = -1. \tag{3.23}$$

to reduce (3.22) to

$$\begin{aligned} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n+1)+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n+1-l}\right) &= S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) \\ &= -S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n-l}\right). \end{aligned} \tag{3.24}$$

This last equation is equivalent to

$$\begin{aligned} S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) &= S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n+1)+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n+1-l}\right) \\ &+S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n-l}\right). \end{aligned} \tag{3.25}$$

Let $a_n = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{j=0}^{k-2}\prod_{i=0}^{j}X_{n-l}\right)$. Then,

$$S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) = a_{n+1}+a_n \tag{3.26}$$

and equation (3.21) is now

$$(a_{n+1}+a_n) = \sum_{l=1}^{k-1}(q-1)^{l-1}(a_{n+1-l}+a_{n-l})+(q-1)^{k-1}a_{n-k+1}. \tag{3.27}$$

The last equation reduces to

$$a_{n+1} = \sum_{l=0}^{k-2} q(q-1)^l a_{n-1-l} \tag{3.28}$$

This concludes the proof. □

The polynomial $Q_{T,k,\mathbb{F}_q}(X)$ is quite interesting. In particular, it seems to be irreducible for $k > 2$ and every $q = p^r$ with p prime. The irreducibility of $Q_{T,k,\mathbb{F}_q}(X)$ when $\gcd(k, r) = 1$ is a consequence of Eisenstein-Dumas criterion.

Theorem 3.3 (Eisenstein-Dumas criterion)**.** *Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ be a polynomial. Let p be a prime. Denote the p-adic valuation of an integer m by $\nu_p(m)$ (with $\nu_p(0) = +\infty$). Suppose that*

(1) $\nu_p(a_n) = 0$,
(2) $\nu_p(a_{n-i})/i > \nu_p(a_0)/n$ *for* $1 \leq i \leq n-1$, *and*
(3) $\gcd(\nu_p(a_0), n) = 1$.

Then, $f(x)$ is irreducible over $\mathbb{Q}$.

Proposition 3.4. *Let $q = p^r$ with p prime. Suppose that* $\gcd(k, r) = 1$. *Then, the polynomial*

$$Q_{T,k,\mathbb{F}_q}(X) = X^k - q\sum_{l=0}^{k-2}(q-1)^l X^{k-2-l} \tag{3.29}$$

is irreducible over $\mathbb{Q}$.

Proof. This is a direct consequence of Eisenstein-Dumas criterion. □

Exponential sums over $\mathbb{F}_q$ of rotation functions also satisfy homogeneous linear recurrences. However, in general, these linear recurrences have higher order than the homogeneous linear recurrences satisfied by exponential sums of trapezoid functions. In other words, the identity observed over $\mathbb{F}_2$ between the linear recurrences of exponential sums of trapezoid Boolean functions and rotation symmetric Boolean functions is lost over $\mathbb{F}_q$. For example, if we consider the monomial rotation

$$R_2(n) = X_1X_2 + X_2X_3 + \cdots + X_{n-1}X_n + X_nX_1, \tag{3.30}$$

then we have the following result. This is the first result that relies on linear algebra.

Theorem 3.5. *Suppose that $p > 2$ is prime. Then, $\{S_{\mathbb{F}_p}(R_2(n))\}$ satisfy the homogeneous linear recurrence with characteristic polynomial*

$$Q_{R,2,\mathbb{F}_p}(X) = X^4 - p^2. \tag{3.31}$$

Proof. Turn X_n and X_{n-1} *OFF* and *ON*, that is, let them assume all values in $\mathbb{F}_p$, and use the identity

$$S_{\mathbb{F}_p}(T_2(n) + \beta X_n) = S_{\mathbb{F}_p}(T_2(n) + X_n), \text{ for } \beta \in \mathbb{F}_p^{\times} \tag{3.32}$$

to get the equation

$$\begin{aligned} S_{\mathbb{F}_p}(R_2(n)) &= S_{\mathbb{F}_p}(T_2(n-2)) + (p-1)S_{\mathbb{F}_p}(T_2(n-2) + X_{n-2}) \\ &\quad + \sum_{\alpha\in\mathbb{F}_p^{\times}}\sum_{\beta\in\mathbb{F}_p} e^{\frac{2\pi i}{p}\alpha\beta} S_{\mathbb{F}_p}(T_2(n-2) + \alpha X_1 + \beta X_{n-2}), \end{aligned} \tag{3.33}$$

Let

$$\begin{aligned} a_0(n) &= S_{\mathbb{F}_p}(T_2(n)) \\ a_1(n) &= S_{\mathbb{F}_p}(T_2(n) + X_n) \\ b_{\alpha,\beta}(n) &= S_{\mathbb{F}_p}(T_2(n) + \alpha X_1 + \beta X_n) \text{ for } \alpha \in \mathbb{F}_p^{\times}, \beta \in \mathbb{F}_p. \end{aligned} \tag{3.34}$$

Then,

$$S_{\mathbb{F}_p}(R_2(n)) = a_0(n-2) + (p-1)a_1(n-2) + \sum_{\alpha\in\mathbb{F}_p^{\times}}\sum_{\beta\in\mathbb{F}_p} e^{\frac{2\pi i}{p}\alpha\beta} b_{\alpha,\beta}(n-2). \tag{3.35}$$

Observe that

$$\begin{aligned} a_0(n) &= a_0(n-1) + (p-1)a_1(n-1) \\ a_1(n) &= a_0(n-1) - a_1(n-1) \\ b_{\alpha,\beta}(n) &= \sum_{\gamma\in\mathbb{F}_p} e^{\frac{2\pi i}{p}(\beta\gamma)} b_{\alpha,\gamma}(n-1), \end{aligned} \tag{3.36}$$

which can be written in matrix form as

$$\begin{pmatrix} a_0(n) \\ a_1(n) \\ b_{1,0}(n) \\ b_{1,1}(n) \\ \vdots \\ b_{p-1,p-1}(n) \end{pmatrix} = A(p) \begin{pmatrix} a_0(n-1) \\ a_1(n-1) \\ b_{1,0}(n-1) \\ b_{1,1}(n-1) \\ \vdots \\ b_{p-1,p-1}(n-1) \end{pmatrix} \tag{3.37}$$

where

$$A(p) \quad = \left(\begin{array}{c|c|c|c|c} A_0(p) & O & O & \cdots & O \\ \hline O & A_1(p) & O & \cdots & O \\ \hline O & O & A_2(p) & \cdots & O \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline O & O & O & \cdots & A_{p-1}(p) \end{array}\right), \tag{3.38}$$

and

$$A_0(p) = \begin{pmatrix} 1 & p-1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad A_j(p) = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & e^{\frac{2\pi i}{p}} & e^{\frac{4\pi i}{p}} & \cdots & e^{\frac{2(p-1)\pi i}{p}} \\ 1 & e^{\frac{4\pi i}{p}} & e^{\frac{8\pi i}{p}} & \cdots & e^{\frac{2\times 2(p-1)\pi i}{p}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & e^{\frac{2(p-1)\pi i}{p}} & e^{\frac{4(p-1)\pi i}{p}} & \cdots & e^{\frac{2\times(p-1)^2\pi i}{p}} \end{pmatrix}, \tag{3.39}$$

for $1 \leq j \leq p-1$. It is clear that the first block $A_0(p)$ satisfies $X^2 - p$. All other blocks $A_j(p)$'s, for $1 \leq j \leq p-1$, are $\sqrt{p} \cdot W_p$, where W_p is the $p \times p$ square Discrete Fourier Transform matrix. Observe that

$$A_j(p)^2 = \begin{pmatrix} p & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & p \\ 0 & 0 & \cdots & p & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & p & \cdots & 0 & 0 \end{pmatrix}. \tag{3.40}$$

Therefore,

$$A_j(p)^4 = \begin{pmatrix} p^2 & 0 & 0 & \cdots & 0 \\ 0 & p^2 & 0 & \cdots & 0 \\ 0 & 0 & p^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & p^2 \end{pmatrix}. \tag{3.41}$$

In other words, the big blocks $A_j(p)$'s satisfiy $X^4 - p^2$. Since $X^2 - p \mid X^4 - p^2$, then we conclude that the matrix $A(p)$ satisfies the polynomial

$$Q_{R,2,\mathbb{F}_p}(X) = X^4 - p^2. \tag{3.42}$$

This means that the sequences $\{a_0(n)\}$, $\{a_1(n)\}$ and $\{b_{\alpha,\beta}(n)\}$, for $\alpha \in \mathbb{F}_p^\times, \beta \in \mathbb{F}_p$, all satisfy the linear recurrence with characteristic polynomial given by $Q_{R,2,\mathbb{F}_p}(X)$. Since $\{S_{\mathbb{F}_p}(R_2(n))\}$ is a combination of these sequences, then it also satisfies such recurrence. This concludes the proof. □

We are now ready to prove one of the main results of this article. That is, exponential sums of rotation polynomials satisfiy linear recurrences with integer coefficients.

Theorem 3.6. *Let $k \geq 2$ be an integer and $q = p^r$ with p prime and $r \geq 1$. The sequence $\{S_{\mathbb{F}_q}(R_{2,3,\cdots,k}(n))\}_{n \geq k}$ satisfies a linear recurrence with integer coefficients.*

Proof. Let $\zeta_p = e^{2\pi i/p}$. Consider the expression $S_{\mathbb{F}_q}(R_{2,3,\cdots,k}(n+k))$. Let $X_{n+k}, X_{n+k-1}, \cdots, X_n$ assume all values in $\mathbb{F}_q$ and observe that $S_{\mathbb{F}_q}(R_{2,3,\cdots,k}(n+k))$ can be written as a linear combination of expressions of the form

$$a_{\boldsymbol{\alpha};\boldsymbol{\beta}}(n) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{j=1}^{k-1}\left(\alpha_j \prod_{l=1}^{j} X_{n+1-l} + \beta_j \prod_{l=1}^{j} X_l\right)\right), \tag{3.43}$$

where $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_k) \in \mathbb{F}_q^{k-1}$ and $\boldsymbol{\beta} = (\beta_1, \cdots, \beta_k) \in \mathbb{F}_q^{k-1}$. However, note that for each $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{F}_q^{k-1}$, we have

$$a_{\boldsymbol{\alpha};\boldsymbol{\beta}}(n) = \sum_{\boldsymbol{\gamma},\boldsymbol{\lambda} \in \mathbb{F}_q^{k-1}} c_{\boldsymbol{\gamma},\boldsymbol{\lambda}} \cdot a_{\boldsymbol{\gamma},\boldsymbol{\lambda}}(n-1), \tag{3.44}$$

where $c_{\boldsymbol{\gamma},\boldsymbol{\lambda}} \in \mathbb{Z}[\zeta_p]$ is a cyclotomic integer. Let $A_{2,3,\cdots,k}(q)$ be the corresponding matrix for the linear equations in (3.44) and $F(X)$ be any annihilating polynomial for $A_{2,3,\cdots,k}(q)$. We can assume that $F(X)$ has integer coefficients. This is because the minimal polynomial of $A_{2,3,\cdots,k}(q)$ is monic, has algebraic integers coefficients and integrality is transitive. Then each $\{a_{\boldsymbol{\alpha};\boldsymbol{\beta}}(n)\}_n$ satisfies the linear recurrence with characteristic polynomial given by $F(X)$. Since $\{S_{\mathbb{F}_q}(R_{2,3,\cdots,k}(n+k))\}$ is a linear combination of these sequences, then $\{S_{\mathbb{F}_q}(R_{2,3,\cdots,k}(n+k))\}$ also satisfies such recurrence. This concludes the proof. □

We know that the identity between linear recurrences of exponential sums of trapezoid Boolean functions and rotation symmetric Boolean functions is lost over $\mathbb{F}_q$. However, the proof of Theorem 3.6 suggests that a relation can be recovered.

Corollary 3.7. *Let $q = p^r$ with p prime and $r \geq 1$. Let $\mu_{T,k,\mathbb{F}_q}(X)$ and $\mu_{R,k,\mathbb{F}_q}(X)$ be the characteristic polynomials associated to the minimal homogeneous linear recurrences with integer coefficients satisfied by $\{S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n))\}$ and $\{S_{\mathbb{F}_q}(R_{2,3,\cdots,k}(n))\}$ (resp.). Then,*

$$\mu_{T,k,\mathbb{F}_q}(X) \mid \mu_{R,k,\mathbb{F}_q}(X). \tag{3.45}$$

In particular, if $\gcd(k,r) = 1$*, then* $Q_{T,k,\mathbb{F}_q}(X) \mid \mu_{R,k,\mathbb{F}_q}(X)$

Proof. In the proof of Theorem 3.6. Observe that $\{a_{\mathbf{0};\mathbf{0}}(n)\} = \{S_q(T_{2,3,\cdots,k}(n))\}$, this implies (3.45). Now, if $\gcd(k,r) = 1$, then $Q_{T,k,\mathbb{F}_q}(X)$ is irreducible and therefore $\mu_{T,k,\mathbb{F}_q}(X) = Q_{T,k,\mathbb{F}_q}(X)$. This concludes the proof. □

Definition 3.8. Let $\{b(n)\}$ be a sequence on an integral domain D. A set of sequences

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

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

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

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

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

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

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

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

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

***Remark* 3.9.** It is a well-known result in the theory of recursive sequences that a sequence that has a recursive generating set satisfies a linear recurrence with constant coefficients. In fact, this technique has been used in Theorems 3.5 and 3.6.

Theorem 3.6 generalizes to monomial rotation functions and linear combinations of them, that is, exponential sums over any Galois field of linear combinations of monomial rotation polynomials satisfy linear recurrences. Of course, in general, we might need to turn *OFF* and *ON* more than k variables, even if the rotation is of degree k. Also, even though the sequences (3.43) always exist, their number might be too big to be handled by hand. For example, consider the sequence of exponential sums $\{S_{\mathbb{F}_3}(R_{2,3}(n))\}$. After some identifications, the authors needed 24 different recursive generating sequences (not claiming that this is optimal) of the form (3.43) and their corresponding 24×24 matrix in order to find that $\{S_{\mathbb{F}_3}(R_{2,3}(n))\}$ satisfy the linear recurrence whose characteristic polynomial is given by

$$\begin{aligned} X^6 - 3X^4 - 9X^3 + 9X + 18 &= \left(X^3 - 3\right)\left(X^3 - 3X - 6\right) \\ &= \left(X^3 - 3\right) Q_{T,3,\mathbb{F}_3}(X). \end{aligned} \tag{3.46}$$

Also, in general, finding the minimal polynomial of a matrix is not an easy task, therefore explicit formulas like the ones in Theorem 3.2 and Theorem 3.5 are much harder to get.

In the next section, this technique is used to prove that exponential sums over Galois fields of elementary symmetric polynomials (and linear combinations of them) satisfy homogeneous linear recurrences with integer coefficients.

4. Linear recurrences over $\mathbb{F}_q$: Symmetric polynomials case

It is a well-established result that exponential sums of symmetric Boolean functions are linear recurrent. This was first established by Cai, Green and Thierauf [4]. In [5], Castro and Medina use this result to show that a conjecture of Cusick, Li, Stănică [11] is true asymptotically. In [6], some of the results of [5] where extended to some perturbations of symmetric Boolean functions. This recursivity was also used in [7, 8] to study the periodicity mod p (p prime) of exponential sums of symmetric Boolean functions.

In this section we show that exponential sums of some symmetric polynomials are linear recurrent over any Galois field. Remarkably, the proof uses the same argument as in the proof of Theorem 3.6. We decided to include the proof for completeness of the writing. However, the reader is welcome to skip the proof.

Let $\sigma_{n,k}$ be the elementary symmetric polynomial in n variables of degree k. For example,

$$\sigma_{4,3} = X_1X_2X_3 + X_1X_4X_3 + X_2X_4X_3 + X_1X_2X_4. \tag{4.1}$$

We have the following result.

Theorem 4.1. *Let $k \geq 2$ be an integer and $q = p^r$ with p prime and $r \geq 1$. The sequence $\{S_{\mathbb{F}_q}(\sigma_{n,k})\}$ satisfies a linear recurrence with constant coefficients.*

Proof. Consider the expression $S_{\mathbb{F}_q}(\sigma_{n+k,k})$. Define

$$a_{\boldsymbol{\beta}}(n) = S_{\mathbb{F}_q}\left(\sigma_{n,k} + \sum_{j=1}^{k-1} \beta_j \sigma_{n,k-j}\right), \tag{4.2}$$

The set $\{a_{\boldsymbol{\beta}}(n)\}_{\boldsymbol{\beta}\in\mathbb{F}_q^{k-1}}$ is a recursive generating set for $S_{\mathbb{F}_q}(\sigma_{n+k,k})$. Therefore, the sequence $\{S_{\mathbb{F}_q}(\sigma_{n+k,k})\}_{n\geq 0}$ satisfies a linear recurrence with constant coefficients. As in the proof of Theorem 3.6, it can be argued that a linear recurrence with integer coefficients is guaranteed to exist. This concludes the proof. □

This result can be generalized to any polynomial of the form

$$\sum_{j=0}^{k-1} \beta_j \sigma_{n,k-j}, \tag{4.3}$$

with $\beta_j \in \mathbb{F}_q$. We present the result without proof, as it follows almost verbatim as the one from Theorem 4.1.

Theorem 4.2. *Let $k \geq 2$ be an integer and $q = p^r$ with p prime and $r \geq 1$. The sequence*

$$S_{\mathbb{F}_q}\left(\sum_{j=0}^{k-1} \beta_j \sigma_{n,k-j}\right) \tag{4.4}$$

satisfies a linear recurrence with constant coefficients, regardless of the choice of the β_j's.

Example 4.3. Consider the sequence $\{S_{\mathbb{F}_3}(\sigma_{n,3})\}$. Recall that in this case the generating sequences are given by

$$a_{(s,t)}(n) = \{S_{\mathbb{F}_3}(\sigma_{n,3} + s\sigma_{n,2} + t\sigma_{n,1})\}, \tag{4.5}$$

where $s, t \in \mathbb{F}_3$. Establish the order

$$(0,0), (1,0), (2,0), (0,1), (1,1), (2,1), (0,2), (1,2), (2,2).$$

Then,

$$\begin{pmatrix} a_{(0,0)}(n) \\ a_{(1,0)}(n) \\ \vdots \\ a_{(2,2)}(n) \end{pmatrix} = A \begin{pmatrix} a_{(0,0)}(n-1) \\ a_{(1,0)}(n-1) \\ \vdots \\ a_{(2,2)}(n-1) \end{pmatrix}, \tag{4.6}$$

where the matrix A is given by

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & 0 & 0 & 0 \\ e^{-\frac{2i\pi}{3}} & 0 & 0 & 0 & 1 & 0 & 0 & 0 & e^{\frac{2i\pi}{3}} \\ e^{\frac{2i\pi}{3}} & 0 & 0 & 0 & 0 & 1 & 0 & e^{-\frac{2i\pi}{3}} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} \\ 0 & 0 & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & 0 & 0 & 0 & 1 & 0 \\ 0 & e^{\frac{2i\pi}{3}} & 0 & e^{-\frac{2i\pi}{3}} & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.7}$$

The minimal polynomial of A is given by

$$\begin{aligned} \mu_A(X) &= X^9 - 9X^8 + 36X^7 - 81X^6 + 108X^5 - 81X^4 + 81X^2 - 81X + 27 \\ &= \left(X^3 - 3X^2 + 3\right)\left(X^6 - 6X^5 + 18X^4 - 30X^3 + 36X^2 - 27X + 9\right). \end{aligned} \tag{4.8}$$

Therefore, $\{S_{\mathbb{F}_3}(\sigma_{n,3})\}$ satisfies the linear recurrence with characteristic polynomial given by $\mu_A(X)$.

4.1. **Quadratic case.**

The case of the elementary symmetric polynomial of degree 2 is fascinating. Observe that

$$a_s(n) = S_{\mathbb{F}_p}(\sigma_{n,2} + s\sigma_{n,1}), \tag{4.9}$$

where $s \in \mathbb{F}_p$, are the generating sequences of $\{S_{\mathbb{F}_p}(\sigma_{n,2})\}$. Also,

$$\begin{pmatrix} a_0(n) \\ a_1(n) \\ \vdots \\ a_{p-1}(n) \end{pmatrix} = M(p) \begin{pmatrix} a_0(n-1) \\ a_1(n-1) \\ \vdots \\ a_{p-1}(n-1) \end{pmatrix}, \tag{4.10}$$

where the matrix $M(p)$ is given by

$$M(p) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ e^{\frac{2(p-1)\pi i}{p}} & 1 & e^{\frac{2\pi i}{p}} & e^{\frac{4\pi i}{p}} & e^{\frac{6\pi i}{p}} & \cdots & e^{\frac{2(p-2)\pi i}{p}} \\ e^{\frac{2\times 2(p-2)\pi i}{p}} & e^{\frac{2\times 2(p-1)\pi i}{p}} & 1 & e^{\frac{4\pi i}{p}} & e^{\frac{8\pi i}{p}} & \cdots & e^{\frac{2\times 2(p-3)\pi i}{p}} \\ e^{\frac{2\times 3(p-3)\pi i}{p}} & e^{\frac{2\times 3(p-2)\pi i}{p}} & e^{\frac{2\times 3(p-1)\pi i}{p}} & 1 & e^{\frac{6\pi i}{p}} & \cdots & e^{\frac{2\times 2(p-3)\pi i}{p}} \\ e^{\frac{2\times 4(p-4)\pi i}{p}} & e^{\frac{2\times 4(p-3)\pi i}{p}} & e^{\frac{2\times 4(p-2)\pi i}{p}} & e^{\frac{2\times 4(p-2)\pi i}{p}} & 1 & \cdots & e^{\frac{2\times 2(p-3)\pi i}{p}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ e^{\frac{2(p-1)\pi i}{p}} & e^{\frac{2\times 2(p-1)\pi i}{p}} & e^{\frac{2\times 3(p-1)\pi i}{p}} & e^{\frac{2\times 4(p-1)\pi i}{p}} & e^{\frac{2\times 5(p-1)\pi i}{p}} & \cdots & 1 \end{pmatrix}. \tag{4.11}$$

The matrix $M(p)$ can be obtained from the $p \times p$ Fourier Discrete Transform Matrix by replacing its j-row $\mathbf{r}_j$ by $RTC^{j-1}(\mathbf{r}_j)$, where RTC is the *rotate through carry* function

$$RTC(a_1, a_2, a_3, \cdots, a_n) = (a_n, a_1, a_2, \cdots, a_{n-1}) \tag{4.12}$$

and RTC^m represents m iterations of RTC.

It is not hard to prove that $M(p)$ is a Complex Hadamard Matrix. In particular,

$$M(p)\overline{M(p)}^T = \overline{M(p)}^T M(p) = \begin{pmatrix} p & 0 & 0 & \cdots & 0 \\ 0 & p & 0 & \cdots & 0 \\ 0 & 0 & p & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & p \end{pmatrix}. \tag{4.13}$$

This implies that $M(p)$ is diagonalizable and that all its eigenvalues satisfy $|\lambda| = \sqrt{p}$. Moreover, its eigenvalues are related to the number-theoretical quadratic Gauss sum mod p. The *quadratic Gauss sum mod p* is defined by

$$g(a;p) = \sum_{k=0}^{p-1} e^{2\pi i a k^2/p} \tag{4.14}$$

It is well-established that

$$g(a;p) = \left(\frac{a}{p}\right) g(1;p), \tag{4.15}$$

where (a/p) denotes the Legendre's symbol, and that

$$g(1;p) = \begin{cases} \sqrt{p} & p \equiv 1 \mod 4 \\ i\sqrt{p} & p \equiv 3 \mod 4. \end{cases} \tag{4.16}$$

Theorem 4.4. *Let $C(p)$ be the set of eigenvalues of $M(p)$. Let $\zeta_p = e^{2\pi i/p}$. Then, $\lambda \in C(p)$ if and only if*

$$\lambda = \left(\frac{-2}{p}\right) g(1;p)\zeta^{-sa^2}. \tag{4.17}$$

In particular, $|C(p)| = (p+1)/2$.

Proof. Let p be an odd prime number and $\zeta = \exp(2\pi i/p)$. The matrix $M(p)$ has (j,k)-entry $\zeta^{j(k-j)}$ where j and k run from 0 to $p-1$ inclusive. We compute the eigenvalues of $M(p)$ simply by writing down its eigenvectors.

Set $s = \frac{1}{2}(p-1)$. Then $1 \equiv -2s \pmod p$ For $0 \le a \le p-1$, let v_a be the column vector with k-entry $\zeta^{s(k-a)^2}$ where $0 \le k \le p-1$. Then the v_a are the cyclic shifts of v_0. The entry in row j of $M(p)v_a$ is

$$\begin{aligned} \sum_{k=0}^{p-1} \zeta^{j(k-j)+s(k-a)^2} &= \sum_{k=0}^{p-1} \zeta^{-2sjk+2sj^2+sk^2-2sak+sa^2} \\ &= \sum_{k=0}^{p-1} \zeta^{s(k-a-j)^2+sj^2-2saj} \\ &= g(s;p)\zeta^{s(j-a)^2-sa^2}. \end{aligned}$$

This is $g(s,p)\zeta^{-sa^2}$ times the entry in row j of v_a. Therefore each v_a is an eigenvector with eigenvalue

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

As these eigenvalues are not all distinct, there remains the possibility that some of these eigenvectors v_a are not linearly independent. That can only happen with eigenvectors in the same eigenspace, so for v_a and v_{p-a} where $0 < a < p$. But it is clear that none of the v_a are multiples of any of the others; simply consider the quotients of corresponding entries. So we have a dimension-two eigenspace for each eigenvalue $\left(\frac{-2}{p}\right) g(1,p)\zeta^{-sa^2}$ for $1 \le a \le \frac{1}{2}(p-1)$. This completes the proof. □

Note that if λ is defined as in (4.17), then equation (4.16) implies

$$\lambda^p = (-i)^{\frac{p-1}{2}} \sqrt{p^p} \tag{4.18}$$

for every odd prime p. Therefore, Theorem 4.4 leads to

$$M(p)^p = \begin{pmatrix} (-i)^{\frac{p-1}{2}}\sqrt{p^p} & 0 & 0 & \cdots & 0 \\ 0 & (-i)^{\frac{p-1}{2}}\sqrt{p^p} & 0 & \cdots & 0 \\ 0 & 0 & (-i)^{\frac{p-1}{2}}\sqrt{p^p} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & (-i)^{\frac{p-1}{2}}\sqrt{p^p} \end{pmatrix}, \tag{4.19}$$

and so

$$M(p)^{2p} = \begin{pmatrix} \left(\frac{-1}{p}\right)p^p & 0 & 0 & \cdots & 0 \\ 0 & \left(\frac{-1}{p}\right)p^p & 0 & \cdots & 0 \\ 0 & 0 & \left(\frac{-1}{p}\right)p^p & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \left(\frac{-1}{p}\right)p^p \end{pmatrix}. \tag{4.20}$$

Thus,

$$X^{2p} - \left(\frac{-1}{p}\right)p^p \tag{4.21}$$

is an annihilating polynomial for the matrix $M(p)$, which in turns implies that $\{S_{\mathbb{F}_p}(\sigma_{n,2})\}$ satisfies the linear recurrence with characteristic polynomial (4.21).

5. Some observations and concluding remarks

We had shown that exponential sums over Galois fields of trapezoid polynomials and rotation polynomials satisfy linear recurrences with integer coefficients. This means that they can be calculated efficiently if we know a priori some initial values. We predict the initial conditions for two families of these type of polynomials.

Consider the trapezoid polynomial $T_{2,3,\cdots,k}(n)$. Recall that $\{S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n))\}$ satisfies the linear recurrence with integer coefficients with characteristic polynomial given by $Q_{T,k,\mathbb{F}_q}(X)$, which is of degree k. This implies that we need to know k initial values in order to calculate the whole sequence. Of course, $\{S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n))\}$ makes sense only for values of $n \geq k$, however, since it satisfies a linear recurrence with integer coefficients, it can be extended to values of $n < k$. We conjecture the following.

Conjecture 5.1. *Let $\{t_{k,q}(n)\}$ be defined by*

$$\begin{aligned} t_{k,q}(j) &= q^j, \quad \text{for } 0 \leq j \leq k-1 \\ t_{k,q}(n) &= = q\sum_{l=0}^{k-2}(q-1)^l t_{k,q}(n-(l+2)), \quad \text{for } n \geq k. \end{aligned} \tag{5.1}$$

Then, $S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) = t_{k,q}(n)$ for all values of $n \geq k$.

We were able to prove that this conjecture is true for $k = 2, 3, 4$, but the general statement remains open. We were also able to predict the initial conditions for $\{S(R_{2,3,\cdots,k}(n))\}$ (Boolean case). Recall that this sequence satisfies the linear recurrence whose characteristic polynomial is given by

$$p_k(X) = X^k - 2(X^{k-2} + X^{k-3} + \cdots + X + 1). \tag{5.2}$$

Therefore, as in the case of trapezoid polynomial $T_{2,3,\cdots,k}(n)$, we need to know k initial values in order to calculate the whole sequence.

Conjecture 5.2. *Let*

$$\delta_o(j) = \begin{cases} 0 & \text{if } j \text{ is even} \\ 1 & \text{if } j \text{ is odd.} \end{cases} \tag{5.3}$$

Define $\{r_k(n)\}$ by

$$\begin{aligned} r_k(0) &= k \\ r_k(j) &= 2^j - \delta_o(j)\cdot 2, \quad \textit{for } 1 \leq j \leq k-1 \\ r_k(n) &= 2\sum_{l=0}^{k-2} r_k(n-(l+2)), \quad \textit{for } n \geq k. \end{aligned} \tag{5.4}$$

Then, $S(R_{2,3,\cdots,k}(n)) = r_k(n)$ for all values of $n \geq k$.

The problem of finding suitable initial conditions for this type of sequences is a nice problem, but also an important one. For example, if Conjecture 5.2 is true, then

$$\begin{aligned} \{S(R_{2,3,\cdots,15}(n))\}_{n\geq 15} &= 32766, 65504, 131036, 262036, 524096, 104813, 2096268, 4192412\cdots \\ \{S(R_{2,3,\cdots,30}(n))\}_{n\geq 30} &= 1073086444, 2146129256, 4292171136, 8584167576, 17167985776, \\ & 34335272736, 68669148016, 137335500952, \cdots \\ \{S(R_{2,3,\cdots,100}(n))\}_{n\geq 100} &= 1267650600228229401496703205376, 2535301200456458802993406410548, \\ & 5070602400912917605986812821300, 10141204801825835211973625642388, \\ & 20282409603651670423947251284976, 40564819207303340847894502569720, \\ & \cdots \end{aligned}$$

On the other hand, we know that Conjecture 5.1 is true for $k=3$, which means, for example, that

$$\begin{aligned} \{S_{\mathbb{F}_9}(T_{2,3}(n))\}_{n\geq 3} &= 153, 1377, 7209, 23409, 164025, 729729, 3161673, 18377361, \cdots \\ \{S_{\mathbb{F}_{7^3}}(T_{2,3}(n))\}_{n\geq 3} &= 234955, 80589565, 13881523159, 55203852025, 14215001955427, \\ & 1647320876934229, 11351488736356111, 2232536080171760209, \cdots \\ \{S_{\mathbb{F}_{71^2}}(T_{2,3}(n))\}_{n\geq 3} &= 50818321, 256175156161, 645881606118001, 2582501749259041, \\ & 9764439145967152081, 16422699840579863752321, \\ & 114835229977615135072561, 330868420079857977922668001, \cdots. \end{aligned}$$

Also, if Conjecture 5.1 is true in general, then we have, for example,

$$\begin{aligned} \{S_{\mathbb{F}_5}(T_{2,3,4,5}(n))\}_{n\geq 5} &= 1845, 9225, 39725, 173025, 730725, 2988025, 13244125, 56108625, \cdots \\ \{S_{\mathbb{F}_{11^2}}(T_{2,3,\cdots,7}(n))\}_{n\geq 7} &= 18445769583241, 2231938119572161, 226346720724231481, \\ & 22141818198352009201, 2044333948085969113321, \\ & 170550498912524502711841, 1342127359186464124132761, \cdots \\ \{S_{\mathbb{F}_{7919}}(T_{2,3,\cdots,8}(n))\}_{n\geq 8} &= 13665512318276822315545157633, 108217192048434155916802103295727, \\ & 734609211013142008709051078210604961, \\ & 4848502223556916452901817857822360556623, \\ & 30722822355930196223839440343843855453844801, \\ & 182535766024343164334384388453936618605681619887, \cdots. \end{aligned}$$

All these values where calculated almost instantaneously. Another nice problem is to automatize the process presented in this work.

References

[1] A. Adolphson and S. Sperber. p-adic Estimates for Exponential Sums and the of Chevalley-Warning. *Ann. Sci. Ec. Norm. Super.*, 4^e série, **20**, 545–556, 1987.

[2] J. Ax. Zeros of polynomials over finite fields. *Amer. J. Math.*, **86**, 255–261, 1964.

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

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

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

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

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

[13] 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, 137–156, 2006.

[14] 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.

[15] 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.

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

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

[18] O. Moreno and C. J. Moreno. The MacWilliams-Sloane Conjecture on the Tightness of the Carlitz-Uchiyama Bound and the Weights of Dual of BCH Codes. *IEEE Trans. Inform. Theory*, **40**, 1894–1907, 1994.

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

[20] A. Shpilka and A. Tal. On the Minimal Fourier Degree of Symmetric Boolean Functions. *Combinatorica*, **88**, 359–377, 2014.

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

[22] 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.

Department of Mathematics, University of Puerto Rico, San Juan, PR 00931
E-mail address: franciscastr@gmail.com

Department of Mathematics, University of Exeter, Exeter, EX4 4QF, UK
E-mail address: r.j.chapman@exeter.ac.uk

Department of Mathematics, University of Puerto Rico, San Juan, PR 00931
E-mail address: luis.medina17@upr.edu

Department of Mathematics, University of Puerto Rico, San Juan, PR 00931
E-mail address: leonid.sepulveda1@upr.edu