CHAPTER 1

Introduction

The experimental and discrete mathematics play a very important role in the development of this thesis. It's precisely in these two branches of research that the family of symmetric functions defined over Galois fields has reached a special interest. Moreover, it could be said that in the last decades the family of symmetrical Boolean functions has acquired a greater importance in the area of applicable mathematics. Thus, over time, the study of these functions have helped to obtain great advances in applications, for example, today they are active areas of research as the experimental mathematical, combinatorial theory, coding theory, cryptography, the theory of error-correcting codes, game theory and electrical engineering (see [**4, 6, 10, 12, 20, 21, 24, 39, 40**]).

Below we present some of the main components of this thesis in a brief conceptual framework taking as an example, the Boolean space. That is, all the mathematical objects mentioned in this first part of the introduction are defined in a similar way for other Galois fields ($\mathbb{F}_q$ with q a power of a prime p). similar all the results of the research. To begin with, one of the firsts mathematical objects used and highlighted in this section is that of a Boolean function. A Boolean function is

defined as

$$F^* : \mathbb{F}_2^n \to \mathbb{F}_2. \tag{1.0.1}$$

For the purpose of this investigation, we frequently use the polynomial representation of F^* known as algebraic normal form (ANF) of F^* and we identify it as a function F in n variables over $\mathbb{F}_2$ [**7, 28**]. In addition it should be noted that, within the family of Boolean functions, there are functions that fulfill an important property, that of being symmetric. It is said that a Boolean function F is symmetric if it is verified that

$$F(x_1, \cdots, x_n) = F\left(x_{\sigma(1)}, \cdots, x_{\sigma(n)}\right), \tag{1.0.2}$$

where σ is any permutation of the symmetric group S_n. In other words, for simplicity it is said that F is symmetric if the subindices of $(x_1, \cdots, x_n)$ can be permuted so that the resulting function is invariant. Within the family of the symmetric Boolean functions, two important functions that will be studied in this investigation are highlighted: the elementary symmetric Boolean polynomial and the rotation symmetric Boolean function. The symmetric Boolean function can be associated with an exponential sum and define as a second main mathematical object. The exponential sum of symmetric Boolean function is defined as

$$S(F) = \sum_{X \in \mathbb{F}_2^n} (-1)^{F(X)}. \tag{1.0.3}$$

To continue complementing the mathematical objects used in this thesis, especially in Chapter 2, knowledge of the properties of homogeneous linear recurrence sequences with integer coefficients is required (see next section). The sequences of exponential sums, such as the sequences of exponential sums of elementary symmetric functions and rotation symmetric functions are well studied throughout this workt. In particular, for research on the sequences of exponential sums of symmetric Boolean functions, it is very important to highlight the following relation

$$wt(F) = \frac{2^n - S(F)}{2}, \tag{1.0.4}$$

where wt(F) is the weight of Hamming (wt(F) counts the number of non-zero components of the $W_F = (F(X_1), \ldots, F(X_{2^n}))$) **[15, 16, 17, 20]**. More precisely, the equation (1.0.4) postulates that, any sequence of exponential sums of symmetric Boolean functions satisfying a homogeneous linear recurrence with integer coefficients, would lead to the respective Hamming weights sequence of these functions, also would satisfy one of these homogeneous linear recurrence (see Chapter 2). In other investigations where equation (1.0.4) **[10, 16]** is studied, known that this relationship involves two important properties over Boolean functions, such properties are the weight of Hamming and the exponential sum. In the area of cryptography, in particular, the criterion of the balanced of a Boolean function is investigated; in this case, equation (1.0.4) us allows to relate the balancing of an elementary symmetric Boolean polynomial $\mathcal{F}$ ($W_{\mathcal{F}}$ has the same number of zero and one's

components) through its exponential sum [**12, 18**]. For example, a Boolean function F is balanced if and only if $S(F) = 0$.

An important aspect in this research and presented in Chapter 3, is the efficiency in the computation of the implementations of the closed formulas established in the results of this chapter, that is, in this thesis we present closed formulas of efficient calculations. For example, the closed formula of exponential sums that generalize the result of Cai, Green, and Thierauf [**6**]. From the definition itself, several of the properties on the mathematical objects mentioned previously would be quite expensive to verify them, for example, the verification of the balanced of a Boolean function using the Hamming weight of a symmetric Boolean function is not very efficient. Moreover, the closed formulas of Chapter 3 corroborate or support the verification of the Stanica-Li-Cusick conjecture asymptotically for Galois fields [**10**].

Already on Galois fields, we present an important relationship that opens a new approach for future research. In Chapter 3 we present closed formulas that link the exponential sums of symmetric polynomials over any Galois field with one related to the problem of the bisecting binomial coefficients. A solution $(\delta_0, \delta_1, \cdots, \delta_n)$ to the equation

$$\sum_{j=0}^{n} \delta_j \binom{n}{j} = 0, \quad \delta_j \in \{-1, 1\}, \tag{1.0.5}$$

is said to give a *bisection of the binomial coefficients* $\binom{n}{j}$, $0 \leq j \leq n$. To end this part of the chapter, we define next the exponential sum of

a symmetric polynomial P defined over $\mathbb{F}_q$ as

$$S_{\mathbb{F}_q}(P) = \sum_{x \in \mathbb{F}_q^n} \zeta_p^{Tr_{\mathbb{F}_q/\mathbb{F}_p}(P(x))} \tag{1.0.6}$$

where $\zeta_p = e^{\frac{2\pi i}{p}}$ and $Tr_{\mathbb{F}_q/\mathbb{F}_p}$ is the trace function defined from $\mathbb{F}_q$ to $\mathbb{F}_p$. The symmetric polynomial P and its trace (defined over Galois fields), is in active research, for example, in the case of balanced of P are directly related to the study of the trace function [**2**]. In the following sections, we introduce a summary on the theme of linear recurrences of symmetric functions, associated recursions of special functions and closed formulas of symmetric polynomial over Galois fields (Chapters 2 and 3 respectively).

1.1. Sequence of linear recurrences

A *sequence of linear recurrences* s is as infinite sequence $s_0, s_1, \cdots$ of elements in $\mathbb{Z}[\zeta_p]$ where $\zeta_p = e^{\frac{2\pi i}{p}}$, having the following property: there are constant $a_0, a_1, \cdots, a_{k-1}$ (con $a_0 \neq 0$) such that, for all $n \geq 0$,

$$s_{n+k} = a_{k-1}s_{n+(k-1)} + \cdots + a_1 s_{n+1} + a_0 s_n + a \tag{1.1.1}$$

If initial values $s_0, s_1, \cdots, s_{k-1}$ of the sequence are provided, the recurrence relation defines the rest of the seuqence uniquely. Such a sequence es said to order k. Also we say that the recurrrence (1.1.1) is homogeneous, if $a = 0$. For example, the exponential sums of the Boolean function

$$F_n(\mathbf{X}) = X_1X_2X_4 + X_2X_3X_5 + \cdots + X_{n-3}X_{n-2}X_n + X_{n-2}X_{n-1}X_1 + X_{n-1}X_nX_2 + X_nX_1X_3$$

satisfies homogeneous linear recurrence with integer coefficients of order 6 , that is, let $X \in \mathbb{F}_2^n$, the sequence $\{S(F_n(\mathbf{X}))\}_{n\geq 4}$ satisfies

$$a_n = 2a_{n-1} + 2a_{n-2} - 4a_{n-3} + 4a_{n-5} - 8a_{n-6}$$

where the first integers of recurrence are

$$8, 20, 16, 56, 32, 144, 144, 352, 512, 832, 1600, \cdots,$$

also satisfies homogeneous linear recurrence its weight sequences $\{wt(F_n(\mathbf{X}))\}$ (see more in the Chapter 2) . Other example, the next symmetric function of order 3

$$e_{n,3} = X_1X_2X_3 + X_1X_2X_4 + \cdots + X_{n-3}X_{n-2}X_n$$

also generates the sequence $\{S_{\mathbb{F}_4}(e_{n,3})\}_{n\geq 3}$ that satisfies homogeneous linear recurrence with integer coefficients of order 3 and by theorem (15) of Chapter 3, you have the formula closed

$$S_{\mathbb{F}_4}(\boldsymbol{e}_{n,3}) \;=\; 4^{n-1} + 3\cdot 2^{n-1} - 3\cdot 2^{n-1}\cos\left(\frac{n\pi}{2}\right).$$

The homogeneous sequence that satisfies(1.1.1) can be associated with the following polynomial,

$$P_k(X) = X^k - a_{k-1}X^{k-1} - \cdots - a_1X - a_0$$

known as the *polynomial characteristic of s* or to the linear recurrence sequence$\{s_n\}_{n\in\mathbb{N}}$. In practice, when all the roots λ_i of the polynomial

$P_k(X)$ are different, then the expression $\sum_{i=1}^{k} a_i\lambda_i^n$ satisfies linear recurrence sequence of the form (1.1.1). Moreover, if we denote s_n by $\sum_{i=1}^{k} a_i\lambda_i^n$, we can say that the sequence $s_0, s_1, \cdots$ satisfies a homogeneous linear recurrence of the form (1.1.1) such that

$$P_k(X) = \prod_{i=1}^{k} (X - \lambda_i)$$

is its characterist polynomial.

EXAMPLE 1. If we apply a result of Cai, Green, and Thierauf , the theorem 3.2 [**6**] or the theorem 3.1 [**10**], the sequence $\left\{S(\boldsymbol{e}_{n,2^l})\right\}$ satisfies a homogeneous linear recurrence whose characteristic polynomial is

$$P_{2^r-1}(X) = \prod_{i=0}^{2^r-1} (X - \lambda_i) \tag{1.1.2}$$

where $\lambda_j = 1 + \zeta_j$ and $\lambda_0 = 2^n$ are the roots of the polynomial (all different). In other words, we can for a fixed integer l, then for all $n \geq 2^l$

$$S(\boldsymbol{e}_{n,2^l}) = c_0(2^l)2^n + \sum_{j=1}^{2^{l+1}-1} c_j(2^l)(1+\zeta_j)^n, \tag{1.1.3}$$

otras where $\zeta_j = e^{\frac{\pi i j}{2^l}}, i = \sqrt{-1}$ and

$$c_j(2^l) = \frac{1}{2^{l+1}} \sum_{t=0}^{2^{l+1}-1} (-1)^{\binom{t}{2^l}} \zeta_j^{-t}.$$

by the theorem (15) the sequence $\left\{S(\boldsymbol{e}_{n,2^l})\right\}$ and its exponential sum $S(\boldsymbol{e}_{n,2^l})$ expressed as a closed formula (see equation 1.1.3) satisfies homogeneous linear recurrence with integer coefficients

1.2. Recursion associated to some special functions

In the theorem (15) of the Chapter 2, establishes that for $n \geq k$, the elementary symmetric polynomial $e_{n,k}$ associated with the exponential sum $S(\boldsymbol{e}_{n,k})$ generates a homogeneous recurrent sequence of linear origin and with integer coefficients. Similarly by the theorem L of chapter 2 it is established in the same way that other two important functions satisfy homogeneous linear recurrence, we enumerate them, the first is the function initially defined by Pieprzyk an Qu in [**36**] called the rotation symmetric Boolean function. Some examples of rotation symmetric functions are given by

$$R_{2,3,4}(\mathbf{5}) = X_1X_2X_3 + X_2X_3X_4 + X_3X_4X_1 + X_4X_1X_2 \tag{1.2.1}$$

and

$$R_2(n) = X_1X_2 + X_2X_3 + \cdots + X_{n-1}X_n + X_nX_1, \tag{1.2.2}$$

where the indices are taken modulo n or are variant under circular translation of indices (see formal definition chapter 2), and the second function is the trapezoidal function. An example of a trapezoidal function is given by

$$\tau_{7,3} = X_1X_2X_3 + X_2X_3X_4 + X_3X_4X_5 + X_4X_5X_6 + X_5X_6X_7$$

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 $\tau_{7,3}$. . Both

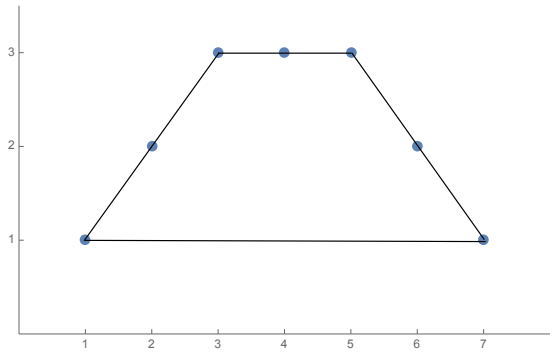

FIGURE 1. Trapezoid associated to the Boolean function $\tau_{7,3}$

$\{\tau_{n,3}\}_{n\geq 3}$ and $\{R_{2,3,4}(n)\}_{n\geq 4}$ can be shown to satisfy a linear recurrence (see theorems 2 and 5) using the following elementary method , the ON or OFF method that we define below:

Method Boolean case (ON or OFF): This technique consists of the simple game of assigning the numeric value to the Boolean variable X_i a "0" or a "1", that is, it is defined $ON:=$ *turn on,* if the variable $X_i = 1$ and $OFF:=$ *turn off,* if the variable $X_i = 0$.

Using the assertion that the sequence $\{\tau_{n,3}\}_{n\geq 3}$ satisfy a linear recurrence with integer coefficients homogeneous with $\tau_{n,3}$ defined over $\mathbb{F}_3$

and whose polynomial associated with the homogeneous linear sequence of $\{\tau_{n,3}\}_{n\geq 3}$ (theorem (7)) is given by

$$P_3(X) = X^3 - 3X - 6,$$

Now by the equation (2.3.4) of the Chapter 2, the sequence$\{\tau_{n,3}\}_{n\geq 3}$ satisfies the following linear recurrence

$$\tau_{n,3} = 3\tau_{n-1,3} + 6\tau_{n-2,3}.$$

Also by Theorem (10) the sequence $\{R_2(n)\}_{n\geq 2}$ also satisfies a homogeneous linear recurrence with integer coefficients whose characteristic polynomial is

$$P_4(X) = X^4 - 9 = \left(x - 3^{\frac{1}{2}}\right)\left(x + 3^{\frac{1}{2}}\right)\left(x - 3^{\frac{1}{2}}i\right)\left(x + 3^{\frac{1}{2}}i\right),$$

where $i = \sqrt{-1}$. For properties of homogeneous linear recurrences, there are constants a_1, a_2, a_3, a_4 such that

$$R_2(n) = a_1 3^{\frac{n}{2}} + a_2(-3)^{\frac{n}{2}} + a_3\left(3^{\frac{1}{2}}i\right)^n + a_4\left(-3^{\frac{1}{2}}i\right)^n$$

To conclude this section with this brief introduction a new concept called the recursive generated set for $\{s_n\}$ (see definition (12)) which is based the argument of the demonstrations that the sequence

(1.2.3) $$\{S_{\mathbb{F}_q}(R_{2,3,\cdots,k}(n))\}_{n\geq k} \text{ and } \{S_{\mathbb{F}_q}(e_{n,k})\}_{n\geq k}$$

satisfy homogeneous linear recurrences with integer coefficients. Some well-known examples of exponential sums are special cases of definition (2.1.3).

1.3. Closed formulas for some special exponential sum

The closed formulas of exponential sums associated with the elementary symmetric polynomial defined over field of galois are the central axis in the research presented in chapter 3. It is well known in many areas of the mathematics that the tool of discrete fourier transform is a mathematical object used for fast and efficient calculations. In this thesis, chapter 3, presents how to obtain a characteristic polynomial of a linear recurrence homogeneous of exponential sums of symmetric polynomials defined over Galois field. In the same way as shown, in the equation (1.1.3), Boolean case. For example, the theorem 3.1 in [**10**] is a general Boolean version of result of Cai, Green, and Thierauf. Similar to equation (1.1.3), let $1 \leq k_1 < \cdots < k_s$ be fixed integers and $r = \lfloor \log_2(k_s) \rfloor + 1$. The value of the exponential sum

$$S(\boldsymbol{e}_{n,[k_1,\cdots,k_s]}) = S(\boldsymbol{e}_{n,k_1}) + \cdots + S(\boldsymbol{e}_{n,k_s})$$

is given by

$$S(\boldsymbol{e}_{n,[k_1,\cdots,k_s]}) = c_0 2^n + \sum_{j=1}^{2^r-1} c_j \lambda_j^n, \tag{1.3.1}$$

where $\lambda_j = 1 + \zeta_j$, $\zeta_j = e^{\frac{\pi i\, j}{2^{r-1}}}$, $i = \sqrt{-1}$ and c_j are constant elements. The formula 1.3.1 is a closed formula for exponential sum $S(\boldsymbol{e}_{n,[k_1,\cdots,k_s]})$.

The formula in equation (1.3.1) implicitly depends on the discrete fourier transform to reach it (see [**6, 10**]). The implementation of these formulas in any mathematics program allows the calculation of the value of the exponential sum $S(\boldsymbol{e}_{n,[k_1,\cdots,k_s]})$ to be efficient in any computer. Once again, the discrete fourier transform and mathematical object of circulat matrices are the basis for obtaining the closed formulas of $S(\boldsymbol{e}_{n,k})$ for any Gaois field (see chapter 3). The closed formula of $S(\boldsymbol{e}_{n,k})$ allows us to show that the sequence $\{S(\boldsymbol{e}_{n,k})\}$ satisfies homogeneous linear recurrences with integer coefficients (see [**14**]). Also in chapter 3, the Theorem (20) whose implementation in an old computer (whose features are not top of the art) of the research, it took *Mathematica* 0.008seconds to calculate

$$S_{\mathbb{F}_3}(\boldsymbol{e}_{12,5}) = 346113 + 92664e^{\frac{2i\pi}{3}} + 92664e^{-\frac{2i\pi}{3}} = 253449. \tag{1.3.2}$$

In comparison, it took 26.6 minutes when using the definition of the exponential sum. The same implementation can be used to obtain values of exponential sums for n relatively big. For instance, it took *Mathematica* 1.28 seconds to calculate

(1.3.3)

$$S_{\mathbb{F}_3}(\boldsymbol{e}_{100,7}) = 113935090835950800739864834563949291416514642941,$$

and 41.28 seconds to calculate

$$S_{\mathbb{F}_4}(\boldsymbol{e}_{50,5}) = 158735097466874432874732322816. \tag{1.3.4}$$

It took about two minutes and a half to calculate $S_{\mathbb{F}_3}(\boldsymbol{e}_{500,11})$, which is an integer with 239 digits. For the Boolean case, the study of the equation (1.3.1) leads us to the demonstration of the cusick conjecture, Li and Stanica asymptotically (see **[10]**). It is clear that the computation of the values of $S_{\mathbb{F}_q}(F)$ is an exponentially hard problem, moreover, still the study of the closed formula for $S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})$ remains as an open research problem: the verification of the Cusick, Li, Stanica conjecture asymptotically for fields Galois (see **[2]**). On the other hand, the closed formula (see theorem 20) shows a link between exponential sums of symmetric polynomials over Galois fields and a problem for multinomial coefficients which is similar to the problem of bisecting binomial coefficients. The elementary symmetric Boolean polynomial $\boldsymbol{e}_{n,k}$ can be represented as $\binom{i}{k}$ where $wt(X) = j$ is the Hamming weight of X, then

$$S(\boldsymbol{e}_{n,k}) = \sum_{j=0}^{n} (-1)^{\binom{j}{k}} \binom{n}{j}. \tag{1.3.5}$$

This last equation is related to two Boolean mathematical problems of interest in cryptography: the balanced of a Boolean function and the problem of bisection of the binomial coefficients (see **[18, 19, 32]**). A solution $(\delta_0, \delta_1, \cdots, \delta_n)$ to the equation

$$\sum_{j=0}^{n} \delta_j \binom{n}{j} = 0, \;\; \delta_j \in \{-1, 1\}, \tag{1.3.6}$$

is said to give a bisection of the binomial coefficients $\binom{n}{j}$, $0 \leq j \leq n$.

To finish this introduction the formula closed for $S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})$ is not only to computational improvement over the formal definition of $S_{\mathbb{F}_q}(F)$,

but also provide a link to a similar problem to the problem of bisecting binomial coefficients (for multinomial coefficients). For example. suppose that $\mathbb{F}_3 = \mathbb{Z}_3$ is the Galois field of 3 elements. Then a explicit formula for $S_{\mathbb{F}_3}(\boldsymbol{e}_{4,2})$ is given by

$$S_{\mathbb{F}_3}(\boldsymbol{e}_{4,2}) = \sum_{m_1=0}^{4} \sum_{m_2=0}^{4-m_1} \binom{4}{m_0^*, m_1, m_2} e^{\left(\frac{2\pi i}{3}\right)(\Lambda_{1,-1}(2,m_1,m_2))}$$

where $\Lambda_{1,-1}(2, m_1, m_2) = \sum_{j=0}^{m_2} \binom{m_2}{j}\binom{m_1}{2-j}(-1)^j$ and $m_0^* = 4 - (m_1 + m_2)$. Moreover, the fact that exponential sums of symmetric polynomials over finite fields can be expressed as multinomial sums is later used in the proof of closed formulas for them. The proof of the closed formulas also depends on a classical result in number theory known as Lucas' Theorem.

CHAPTER 2

Recursion

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 too special a property and may imply that these implementations are vulnerable to attacks.

2.1. Preliminaries

As mentioned in the introduction, Pieprzyk and Qu ([**36**]) 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 $\mathbb{F}_2^n$. Let us explain this definition in a more concrete way. Our explanation is similar to the one presented in [**39**].

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

(2.1.1)

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

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

$$R(\mathbf{X}) = R_{2,3}(5) + R_3(5). \tag{2.1.2}$$

Sometimes the notation $(1, j_1, \cdots, j_s)_n$ is used to represent the monomial rotation Boolean function (2.1.1), see [**16**].

As mentioned in the introduction, in this work we present a method that could be used to generalize Cusick's result over any Galois field. In particular, we show that exponential sums over finite fields of some rotation symmetric polynomials are linear recurrent with integer coefficients. The *exponential sum* of a function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ is given by

$$S_{\mathbb{F}_q}(F) = \sum_{\mathbf{x}\in\mathbb{F}_q^n} e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(F(\mathbf{x}))}. \tag{2.1.3}$$

Here, $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ represents the *field trace function* from $\mathbb{F}_q$ to $\mathbb{F}_p$.

Exponential sums are very rich objects in the area of analytic number theory.

In the next section we provide an introduction to the elementary method used in this article to obtain linear recurrences for this type of exponential sums. As mentioned before, this introduction is done over $\mathbb{F}_2$. The reader interested in the generalization is invited to skip this section and go directly to section **??**.

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

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

THEOREM 2. *The sequence $\{S(\tau_{n,k})\}_{n=k}^{\infty}$ satisfies a homogeneous linear recurrence with integer coefficients whose characteristic polynomial is given by*

$$p_k(X) = X^k - 2(X^{k-2} + X^{k-3} + \cdots + X + 1). \tag{2.2.1}$$

REMARK 3. We point out that a more general version of Theorem 2 for cubic functions appears in [**5**].

the same arguments as in the proof of Theorem 2.

LEMMA 4. *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 $p_k(X)$.

Theorem 2 and Lemma 4 are all that is needed to show that the sequence of exponential sums of $R_{2,3,\cdots,k}(n)$ satisfies the linear recurrence with characteristic polynomial $p_k(X)$.

THEOREM 5. *The sequence* $\{S(R_{2,3,\cdots,k}(n))\}$ *satisfies the homogeneous linear recurrence whose characteristic polynomial is given by* $p_k(X)$.

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

In this section we show that Cuscik's result is not unique to the Boolean case. In fact, exponential sums over finite fields of rotation polynomials $R_{j_1,\cdots,j_s}(n)$ (and linear combination of them) satisfy linear recurrences with constant coefficients. 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 $r \geq 1$. The recall that the exponential sum of a function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ is given by

$$S_{\mathbb{F}_q}(F) = \sum_{\mathbf{x} \in \mathbb{F}_q^n} e^{\frac{2\pi i}{p} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(F(\mathbf{x}))}, \tag{2.3.1}$$

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 $q-1$ different colors.

We consider first sequences of exponential sums of trapezoid functions. As in the Boolean case, 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 6. *Let k, n and j be integers with $k > 2$, $1 \leq j < k$ and $n \geq k$. Then,*

(2.3.2)
$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{n-l}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j} \prod_{l=0}^{k-s-1} X_{n-l}\right)$$

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

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

THEOREM 7. *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*

$$Q_{T,k,\mathbb{F}_q}(X) = X^k - q\sum_{l=0}^{k-2}(q-1)^l X^{k-2-l}. \tag{2.3.3}$$

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

PROOF. M

$$a_{n+1} = \sum_{l=0}^{k-2} q(q-1)^l a_{n-1-l} \tag{2.3.4}$$

□

m

THEOREM 8. *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ 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 9. *Let $q = p^r$ with p prime. Suppose that* $\gcd(k, r) = 1$. *Then, the polynomial*

$$Q_{T,k,\mathbb{F}_q}(X) = X^k - q\sum_{l=0}^{k-2}(q-1)^l X^{k-2-l} \tag{2.3.5}$$

is irreducible over $\mathbb{Q}$.

THEOREM 10. *Suppose that $p > 2$ is prime. Then, $\{S_{\mathbb{F}_p}(R_2(n)\}$ satisfy the homogeneous linear recurrence with characteristic polynomial*

$$Q_{R,2,\mathbb{F}_p}(X) = X^4 - p^2. \tag{2.3.6}$$

M

THEOREM 11. *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.*

DEFINITION 12. 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 13. 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 10 and 11.

THEOREM 14. *Let p be prime and $q = p^r$. Consider the function*

$$F_n = \sum_{t=1}^{N} \beta_t R_{j_{t,1},\cdots,j_{t,s_t}}(n),$$

where $\beta_t \in \mathbb{F}_q$ and $1 < j_{t,1} < \cdots < j_{t,s_t}$ are integers. The sequence $\{S_{\mathbb{F}_q}(F_n)\}$ satisfies a linear recurrence with integer coefficients.

M

THEOREM 15. *Let $k \geq 2$ be an integer and $q = p^r$ with p prime and $r \geq 1$. The sequence*

$$\left\{ S_{\mathbb{F}_q}\left(\sum_{j=0}^{k-1} \beta_j \sigma_{n,k-j} \right) \right\} \tag{2.3.7}$$

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

M

THEOREM 16. *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 In particular, $|C(p)| = (p+1)/2$.*

2.4. Concluding remarks

This article is divided as follows. The next section contains some preliminaries. In Section 3.2 we provide multinomial sum expressions

for exponential sums of symmetric polynomials over Galois fields. We also include some representations that depend on integer partitions. These multinomial sums representations are a computational improvement over the formal definition of exponential sums. Moreover, as just mentioned, they provide a connection to a problem similar to the problem of bisecting binomial coefficients. Section 3.3 is the core and final section of this article. It is also the section where the main results are presented. In particular, we find closed formulas for some multinomial sums. This, together with multinomial sum representations for our exponential sums, allow us to prove closed formulas for exponential sums of linear combinations of elementary symmetric polynomials over finite fields. We also provide explicit linear recurrences for such exponential sums, showing that the recursive nature of these sequences is not special to the binary case. Moreover, every multi-variable function over a finite field extension of $\mathbb{F}_2$ can be identified with a Boolean function. Thus, these results also provide new families of Boolean functions that might be useful for efficient implementations.

CHAPTER 3

Closed formulas for exponential sums of symmetric polynomial

3.1. Preliminaries

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

$$\boldsymbol{e}_{4,3} = X_1X_2X_3 \oplus X_1X_4X_3 \oplus X_2X_4X_3 \oplus X_1X_2X_4,$$

where $\oplus$ represents addition modulo 2. Every symmetric Boolean function $F(\mathbf{X})$ can be identified with an expression of the form where $0 \leq k_1 < k_2 < \cdots < k_s$ are integers. For the sake of simplicity, the notation $\boldsymbol{e}_{n,[k_1,\ldots,k_s]}$ is used to denote (**??**). For example,

THEOREM 17. *Let $1 \leq k_1 < \cdots < k_s$ be fixed integers and $r = \lfloor \log_2(k_s) \rfloor + 1$. The value of the exponential sum $S(\boldsymbol{e}_{n,[k_1,\cdots,k_s]})$ is given by*

$$S(\boldsymbol{e}_{n,[k_1,\cdots,k_s]}) \quad = \quad c_0(k_1,\cdots,k_s)2^n + \sum_{j=1}^{2^r-1} c_j(k_1,\cdots,k_s)(1+\zeta_j)^n,$$

where $\zeta_j = e^{\frac{\pi i j}{2^{r-1}}}, i = \sqrt{-1}$ *and*

$$c_j(k_1, \cdots, k_s) = \frac{1}{2^r} \sum_{t=0}^{2^r-1} (-1)^{\binom{t}{k_1}+\cdots+\binom{t}{k_s}} \zeta_j^{-t}. \tag{3.1.1}$$

Theorem 17 and a closed formula for $c_0(k)$ (proved in [**10**]) were used by Castro and Medina [**10**] to prove asymptotically a conjecture of Cusick, Li and Stănică about the balancedness of elementary symmetric polynomials [**18**]. An adaptation of Theorem 17 to perturbations of symmetric Boolean functions (see [**11**]) was recently used in [**?**] to prove a generalized conjecture of Canteaut and Videau [**7**] about the existence of balanced perturbations when the number of variables grows. The original conjecture, which was stated for symmetric Boolean functions, said that only trivially balanced functions exists when the number of variables grows. The original conjecture was proved by Guo, Gao and Zhao [**23**]. The same behavior holds true for perturbations of symmetric Boolean functions.

One of the goals of this article is to generalize Theorem 17 to the general setting of Galois fields. If $F : \mathbb{F}_q^n \to \mathbb{F}_q$, then its *exponential sum over* $\mathbb{F}_q$ is given by

$$S_{\mathbb{F}_q}(F) = \sum_{\mathbf{x} \in \mathbb{F}_q^n} e^{\frac{2\pi i}{p} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(F(\mathbf{x}))}, \tag{3.1.2}$$

trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. The *field trace function* can be explicitly defined as

$$\mathrm{Tr}_{\mathbb{F}_{p^l}/\mathbb{F}_p}(\alpha) = \sum_{j=0}^{l-1} \alpha^{p^j}, \tag{3.1.3}$$

with arithmetic done in $\mathbb{F}_{p^l}$. Recently in [**14**], it was proved that exponential sums over $\mathbb{F}_q$ of linear combinations of elementary symmetric polynomials are linear recurrent with integer coefficients. Thus, the recursive nature of these sequences is not restricted to $\mathbb{F}_2$. The approach presented in [**14**], however,

THEOREM 18. *Suppose that n and k are non-negative integers and let p be a prime. Suppose that*

$$\begin{aligned} n &= n_0 + n_1 p + \cdots + n_l p^l \\ k &= k_0 + k_1 p + \cdots + k_l p^l, \end{aligned}$$

with $0 \leq n_j, k_j < p$ for $j = 1, \cdots, l$. Then,

$$\binom{n}{k} \equiv \prod_{j=0}^{l} \binom{n_j}{k_j} \mod p.$$

Let $D = p^{\lfloor \log_p(k) \rfloor + 1}$. Observe that one consequence of Lucas' Theorem is

$$\binom{n+D}{k} \equiv \binom{n}{k} \mod p. \tag{3.1.4}$$

This will be used throughout the rest of the paper.

3.2. A formula for exponential sums in terms of multinomial sums

In this section we prove a formula for $S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})$ in terms of multinomial coefficients. This formula is a computational improvement over

(3.1.2). We start by finding a formula, in this case, a recursive one, for the value of $\boldsymbol{e}_{n,k}$ at a vector $\mathbf{x}$.

Let n, k and m be positive integers and a_s be a parameter (s a positive integer). Let

$$\Lambda_{a_1}(k,m) = a_1^k \binom{m}{k} \tag{3.2.1}$$

and define $\Lambda_{a_1,\cdots,a_l}$ recursively by

(3.2.2)

$$\Lambda_{a_1,a_2,\cdots,a_{l+1}}(k,m_1,m_2,\cdots,m_{l+1}) = \sum_{j=0}^{m_{l+1}} \binom{m_{l+1}}{j} a_{l+1}^j \Lambda_{a_1,\cdots,a_l}(k-j,m_1,m_2,\cdots,m_l),$$

The value of $\boldsymbol{e}_{n,k}$ is linked to $\Lambda_{a_1,\cdots,a_l}$.

LEMMA 19. *Let n and k be positive integers. Let $A_l = \{0, a_1, \cdots, a_l\}$ and $\mathbf{x} \in A_l^n$. Suppose that a_j appears m_j times in $\mathbf{x}$. Then,*

$$\boldsymbol{e}_{n,k}(\mathbf{x}) = \Lambda_{a_1,\cdots,a_l}(k, m_1, \cdots, m_l). \tag{3.2.3}$$

The above lemma can be used to express exponential sums of symmetric polynomials as a multi-sum of products of multinomial coefficients.

THEOREM 20. *Let n, k be natural numbers such that $k \leq n$, p a prime and $q = p^r$ for some positive integer r. Suppose that $\mathbb{F}_q = \{0, \alpha_1, \cdots, \alpha_{q-1}\}$ is the Galois field of q elements. Then, where $m_0^* = n - (m_1 + \cdots + m_{q-1})$.*

An easy adjustment to the proof of Theorem 20 leads the following corollary.

COROLLARY 21. *Let $1 \leq k_1 < k_2 < \cdots < k_s$ and n be positive integers, p a prime and $q = p^r$ for some positive integer r. Suppose that $\mathbb{F}_q = \{0, \alpha_1, \cdots, \alpha_{q-1}\}$ is the Galois field of q elements. Consider the symmetric function Then,*

Theorem 20 and its corollary can be written in terms of partitions of n. We say that $\boldsymbol{\lambda} = (\lambda_1, \cdots, \lambda_r)$ is a *partition* of n, and write $\boldsymbol{\lambda} \dashv n$, if the λ_j are integers and

$$\lambda_1 \geq \cdots \geq \lambda_r \geq 1 \text{ and } n = \lambda_1 + \cdots + \lambda_r.$$

We us to denote the set of all rearrangements of $\boldsymbol{\lambda}$. Finally, if $\boldsymbol{\gamma}$ is a non-empty list, then $\boldsymbol{\gamma}^*$ is the list obtained from $\boldsymbol{\gamma}$ by removing the first element. For example, if $\boldsymbol{\gamma} = (2, 2, 1, 1)$, then $\boldsymbol{\gamma}^* = (2, 1, 1)$. Theorem 20 and Corollary 21 can be re-stated as follows.

THEOREM 22. *Let n, k be natural numbers such that $k \leq n$, p a prime and $q = p^r$ for some positive integer r. Suppose that $\mathbb{F}_q = \{0, \alpha_1, \cdots, \alpha_{q-1}\}$ is the Galois field of q elements. Then,*

COROLLARY 23. *Let $1 \leq k_1 < k_2 < \cdots < k_s$ and n be positive integers, p a prime and $q = p^r$ for some positive integer r. Suppose that $\mathbb{F}_q = \{0, \alpha_1, \cdots, \alpha_{q-1}\}$ is the Galois field of q elements. Consider the symmetric function*

$$\sum_{j=1}^{s} \beta_j \boldsymbol{e}_{n,k_j} \quad \text{where } \beta_j \in \mathbb{F}_q^{\times}.$$

Then,

For small q, Theorem 20 and the recursive nature of $\Lambda_{a_1,\cdots,a_l}$ can be used to speed up the computation of $S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})$. For example, using an implementation of Theorem 20 and an old computer (whose features are not top of the art) from one of the authors, it took *Mathematica* 0.008 seconds to calculate where the indices run

$$0 \leq m_0 \leq n, 0 \leq m_1 \leq n-m_0, \cdots, 0 \leq m_{q-2} \leq n-m_0-m_1-\cdots-m_{q-3},$$

into p sublists, $l_j(n;q), 1 \leq j \leq p$, such that the sum on each sublist is the same. This common sum must be q^{n-1}. Observe that every time $S_{\mathbb{F}_q}(\beta_1 \boldsymbol{e}_{n,k_1} + \cdots + \beta_s \boldsymbol{e}_{n,k_s}) = 0$ we obtain a (p,q)-section to of multinomial coefficients. This connection generalizes the one that exists between bisections of binomial coefficients and symmetric Boolean functions.

EXAMPLE 24. The elementary symmetric polynomial $\boldsymbol{e}_{5,3}$ is such that $S_{\mathbb{F}_3}(\boldsymbol{e}_{5,3}) = 0$. Observe that

M

EXAMPLE 25. The symmetric polynomial $\boldsymbol{e}_{6,5} + \boldsymbol{e}_{6,3}$ also satisfies $S_{\mathbb{F}_3}(\boldsymbol{e}_{6,5} + \boldsymbol{e}_{6,3}) = 0$. In this case,

(3.2.4)

$$\mathcal{L}(6;3) = \{1,6,15,20,15,6,1,6,30,60,60,30,6,15,60,90,60,15,20,60,60,20,15,30,15,6,6,1\}.$$

The 3-section that corresponds to $\boldsymbol{e}_{6,5} + \boldsymbol{e}_{6,3}$ over $\mathbb{F}_3$ is

$$
\begin{aligned}
(3.2.5) \qquad l_1(6;3) &= \{1,6,6,15,15,20,30,30,30,90\} \\
l_2(6;3) &= \{1,6,6,15,15,20,60,60,60\} \\
l_3(6;3) &= \{1,6,6,15,15,20,60,60,60\}.
\end{aligned}
$$

As in the Boolean case, we may try to define trivial (p,q)-sections. A possible way to do this is to say that a (p,q)-section is trivial if $l_1(n;k) = l_2(n;k) = \cdots = l_p(n;k)$. Again, following the binary case, we say that a symmetric polynomial $\beta_1 \boldsymbol{e}_{n,k_1} + \cdots + \beta_s \boldsymbol{e}_{n,k_s}$ is trivially balanced over $\mathbb{F}_q$ if its related (p,q)-section is trivial. For example, $\boldsymbol{e}_{5,3}$ is trivially balanced, while $\boldsymbol{e}_{6,5} + \boldsymbol{e}_{6,3}$ is not. It would be interesting to know if some results known for the binary case also apply to this problem.

Exponential sums of linear combinations of elementary symmetric polynomials are also linked, via Theorem we find a solution to (??).

EXAMPLE 26. Consider $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ where $\alpha^2 = \alpha+1$. The symmetric polynomial

$$(1+\alpha)\boldsymbol{e}_{n,3} + (1+\alpha)\boldsymbol{e}_{n,2} + \alpha \boldsymbol{e}_{n,1}$$

is such that

A natural problem to explore is to see how solutions to (??) given by exponential sums of linear combinations of elementary symmetric polynomials look like as n grows. Perhaps something similar to the

study presented in [?] holds true in this case. This is part of future research.

In the next section, we prove closed formulas for exponential sums of symmetric polynomials over Galois fields. Moreover, we provide explicit linear recurrences with integer coefficients for these exponential sums.

3.3. Closed formulas for exponential sums of symmetric polynomials

In this section we generalize Theorem 17, that is, we provide closed formulas for the exponential sums considered in this article. These formulas, in turn, allow us to find explicit recursions for these sequences. Our formulas depend on circulant matrices and on periodicity. Thus, we start with a short background on these topics.

Let D be a positive integer and $\alpha = (c_0, c_1, \ldots, c_{D-1}) \in \mathbb{C}^D$. The *D-circulant matrix* associated to α, denoted by $\mathrm{circ}(\alpha)$, is defined by

$$\mathrm{circ}(\alpha) := \begin{pmatrix} c_0 & c_1 & \cdots & c_{D-2} & c_{D-1} \\ c_{D-1} & c_0 & \cdots & c_{D-1} & c_{D-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_2 & c_3 & \cdots & c_0 & c_1 \\ c_1 & c_2 & \cdots & c_{D-1} & c_0 \end{pmatrix}. \tag{3.3.1}$$

The polynomial $p_\alpha(X) = c_0 + c_1 X + \cdots + c_{D-1}X^{D-1}$ is called the *associated polynomial* of the circulant matrix. In the literature, this polynomial is also called *representer polynomial*. Observe that if

PROPOSITION 27. *Let $n \in \mathbb{N}$ and $0 \leq t \leq D-1$. Then,*

$$r_t(n;a) = \frac{1}{D}\sum_{m=0}^{D-1} \xi_D^{tm} \lambda_m^n, \tag{3.3.2}$$

where $\xi_D = \exp(2\pi i/D)$ and $\lambda_m = 1 + a\xi_D^{-m}$ are the eigenvalues of

The following results are easy consequences of the above proposition.

COROLLARY 28. *Let F be a periodic function with period D. Suppose that $\xi^D = 1$ (not necessarily primitive). Then,*

$$\sum_{l=0}^{n} \binom{n}{l} a^l \xi^{F(l)} = \frac{1}{D}\sum_{t=0}^{D-1} \xi^{F(t)} \sum_{j=0}^{D-1} \xi_D^{tj} \lambda_j^n, \tag{3.3.3}$$

where $\xi_D = \exp(2\pi i/D)$ and $\lambda_j = 1 + a\xi_D^{-j}$, for $0 \leq j \leq D-1$, are the eigenvalues of

M

COROLLARY 29. *Let F be a periodic function with period D. Suppose that $\xi^D = 1$ (not necessarily primitive). Then,*

$$\sum_{l=0}^{n} \binom{n}{l} \xi^{F(l)} = \frac{1}{D}\sum_{t=0}^{D-1} \xi^{F(t)} \sum_{j=0}^{D-1} \xi_D^{tj} \left(1 + \xi_D^{-j}\right)^n, \tag{3.3.4}$$

where $\xi_D = \exp(2\pi i/D)$.

These results can be extended further to obtain closed formulas for multinomial sums.

THEOREM 30. *Let $F(q_1, \cdots, q_r)$ be a periodic function in each component. Moreover, suppose that D is a period for F in each component and that $\xi^D = 1$ (not necessarily primitive). Define, where $\xi_D = \exp(2\pi i/D)$ and $\lambda_{j_1,\cdots,j_r} = 1 + \xi_D^{-j_1} + \xi_D^{-j_2} + \cdots + \xi_D^{-j_r}$.*

Observe that equation (**??**) can be written as where However, note that $\lambda_{t_1,\cdots,t_r} = \lambda_{t'_1,\cdots,t'_r}$ where $(t'_1, \cdots, t'_r)$ is any rearrangement of $(t_1, \cdots, t_r)$. This means that the coefficient of $\lambda^n_{t_1,\cdots,t_r}$ in (**??**) is the sum of all $d_{t'_1,\cdots,t'_r}(D)$ where $(t'_1, \cdots, t'_r)$ is a rearrangement of $(t_1, \cdots, t_r)$. rearrangements of $(t_1, \cdots, t_r)$. Theorem 30 now can be re-stated as follows.

THEOREM 31. *Let $F(q_1, \cdots, q_r)$ be a periodic function in each component. Moreover, suppose that D is a period for F in each component and that $\xi^D = 1$ (not necessarily primitive). Define, and $\xi_D = \exp(2\pi i/D)$.*

A nice consequence of this result is that sequences of the form $\{S(n)\}$, with $S(n)$ defined as in (**??**), satisfy linear recurrences with integer coefficients. Moreover, we can provide explicit characteristic polynomials for such recurrences.

COROLLARY 32.

The linear recurrence given in Corollary 32 is not necessarily the minimal linear recurrence with integer coefficients satisfied by $\{S(n)\}$. However, the characteristic polynomial of the minimal of such recurrences must be a factor of $P_S(X)$.

EXAMPLE 33. Let F be a n-variable Boolean function. The *nega-Hadamard transform of* F is defined as the complex valued function given by where $\Phi_n(X)$ is the n-th cyclotomic polynomial.

We would like to point out that this is not a new result. It was already established in [**13**]. However, we decided to include it because it is a straightforward application of our results.

EXAMPLE 34. Consider the sum The fact that $\mu_S(X)|P_S(X)$ is now evident.

M

EXAMPLE 35. Other toy examples can be constructed with previous classical results. For example, it is known that $\{f_n \mod m\}$, where f_n represents the n-th Fibonacci number and m is a positive integer, is periodic. The period is known as the Pisano period mod m and it is usually denoted by $\pi(m)$. Let $f_n^{(m)}$ represent $f_n \mod m$ and consider the sum This example can be easily generalized to any Lucas sequence of the first kind $u_n(a,b)$ (the Fibonacci sequence is given by $u_n(1,-1)$).

is of the same type as (**??**). It remains to show the periodicity of $F_{k;\mathbb{F}_q}$.

We start with the following lemma.

LEMMA 36. *Let p be prime and $a_1, \cdots, a_l$ be some elements in some field extension of $\mathbb{F}_p$. Define*

$$\Lambda^{(p)}_{a_1,\cdots,a_l}(k, m_1, \cdots, m_l) = \Lambda_{a_1,\cdots,a_l}(k, m_1^+, \cdots, m_l^+) \mod p, \tag{3.3.5}$$

where Then, $\Lambda^{(p)}_{a_1,\cdots,a_l}(k, m_1, \cdots, m_l)$ *is periodic in each of the variables* $m_1, \cdots, m_l$ *with period* $D = p^{\lfloor \log_p(k) \rfloor + 1}$.

We now present our closed formulas for $S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})$. This generalizes Cai et al.'s result for the binary case [**6**]. It also generalizes the recurrence exploited in [**10, 11**].

THEOREM 37. *Let* n *and* $k > 1$ *be positive integers and* p *be a prime and* $q = p^r$ *with* $r \geq 1$. *Let* $D = p^{\lfloor \log_p(k) \rfloor + 1}$. *Then,*

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

$\xi_m = \exp(2\pi i/m)$, *In particular, the sequence* $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})\}$ *satisfies the linear recurrence with integer coefficients whose characteristic polynomial is given by*

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

Theorem 37 also provides a bound for the degree of the minimal linear recurrence with integer coefficients satisfied by $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})\}$.

COROLLARY 38. *Let* $k > 1$ *be positive integers and* p *be a prime and* $q = p^r$ *with* $r \geq 1$. *Let* $D = p^{\lfloor \log_p(k) \rfloor + 1}$. *The degree of the minimal linear recurrence with integer coefficients that* $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})\}$ *satisfies is less than or equal to* $(D)_q/q!$, *where* $(a)_n = a(a+1)(a+2)\cdots(a+n-1)$ *is the Pochhammer symbol.*

EXAMPLE 39. Consider the sequence $\{S_{\mathbb{F}_4}(\boldsymbol{e}_{n,3})\}$. Theorem 37 implies that this sequence satisfies the linear recurrence whose characteristic is given by

$$\begin{aligned}F_8(\mathbf{X}) =& X_2X_3X_5 + X_1X_4X_5 + X_2X_4X_5 + X_2X_7X_5 + X_4X_7X_5 + X_1X_8X_5 + X_2X_8X_5 + \\ & X_3X_8X_5 + X_4X_8X_5 + X_1X_3X_6 + X_2X_3X_6 + X_1X_4X_6 + X_2X_3X_7 + X_1X_4X_7 + \\ & X_2X_4X_7 + X_1X_6X_7 + X_2X_6X_7 + X_3X_6X_7 + X_4X_6X_7 + X_1X_3X_8 + X_2X_3X_8 + \\ & X_1X_4X_8 + X_1X_6X_8 + X_3X_6X_8.\end{aligned}$$

Observe that $S_{\mathbb{F}_4}(\boldsymbol{e}_{4,3}) = S_{\mathbb{F}_2}(F_8) = 64$.

M

EXAMPLE 40. onsider the sequence $\{S_{\mathbb{F}_8}(\boldsymbol{e}_{n,3})\}$. Theorem 37 implies that this sequence satisfies the linear recurrence whose characteristic is given by

$$P_{8,3}(X) = \prod_{a_1=0}^{3}\prod_{a_2=0}^{a_1}\prod_{a_3=0}^{a_2}\prod_{a_4=0}^{a_3}\prod_{a_5=0}^{a_4}\prod_{a_6=0}^{a_5}\prod_{a_7=0}^{a_6}\left(X - (1 + i^{a_1} + i^{a_2} + i^{a_3} + i^{a_4} + i^{a_5} + i^{a_6} + i^{a_7})\right).$$

The minimal linear recurrence with integer coefficients that $\{S_{\mathbb{F}_8}(\boldsymbol{e}_{n,3})\}$ satisfies has characteristic polynomial given by As with the previous can be identified with a $3n$-variable Boolean function.

These two examples show a big difference between the degrees of the polynomials $P_{q,k}(X)$ and $\mu_{q,k}(X)$, where $\mu_{q,k}(X)$ represents the characteristic polynomial of the minimal linear recurrence with integer coefficients satisfied by the sequence $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})\}$. In particular, $P_{q,k}(X)$ does not seem to be tight. However, what you are seeing here is the

fact that when working over $\mathbb{F}_q$ with $q = p^r$ and $r > 1$, some of the factors of $P_{q,k}(X)$ are repeated multiple times. For instance, consider Example 39. Observe that when $(a_1, a_2, a_3) = (2, 1, 0)$ we get the factor $X - (1 + i)$. However when $(a_1, a_2, a_3) = (3, 1, 1)$, we also get the factor $X - (1 + i)$. Therefore, this factor is repeated twice. The factor $X - (1 - i)$ is also repeated twice. That is why the factor $X^2 - 2X + 2$ appears in $P_{4,3}(X)$ with 2 as exponent. This phenomenon does not occur over $\mathbb{F}_p$. In fact, there are examples where the polynomial $P_{p,k}(X)$ is tight.

EXAMPLE 41. Consider the sequence $\{S_{\mathbb{F}_3}(\boldsymbol{e}_{n,7})\}$. The characteristic polynomial of the minimal linear recurrence with integer coefficients satisfied by this sequence is

$$\mu_{3,7}(X) = \frac{1}{X} P_{3,7}(X).$$

The te

The repetition of factors can be eliminated by using *least*

THEOREM 42. *Let n and $k > 1$ be positive integers and p be a prime and $q = p^r$ with $r \geq 1$. Let $D = p^{\lfloor \log_p(k) \rfloor + 1}$. Let $M_{a_1,\cdots,a_{q-1}}(X)$ be the minimal polynomial for the algebraic integer $1 + \xi_D^{a_1} + \cdots + \xi_D^{a_{q-1}}$. Then, $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})\}$ satisfies the linear recurrence with integer coefficients whose characteristic polynomial is given by*

REMARK 43. As expected, having these recurrences at hand allow us to compute exponential sums of elementary symmetric polynomials

for big values of n. For instance, it took *Mathematica* 37.504 seconds to calculate $S_{\mathbb{F}_3}(\boldsymbol{e}_{100,000,11})$, which is a integer with $47,712$ digits.

We point out that Theorem 37 and other results after it can be extended to linear combinations of elementary symmetric polynomials without too much effort. For instance, suppose that $0 \leq k_1 < \cdots < k_s$ are integers and $\beta_1, \cdots, \beta_s \in \mathbb{F}_q^{\times}$. The discussion prior Theorem 37 together with Corollary 21 implies that The statement of Theorem 37 can now be written almost verbatim for linear combinations of elementary symmetric polynomials. The only differences are that D is now $D = p^{\lfloor \log_p(k_s) \rfloor + 1}$ and Similar adjustments apply to the other results.

3.4. Concluding remarks

We

Bibliography

[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] 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* **86**, 693–701, 2018.

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

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

[5] A. Brown and T. W. Cusick. Recursive weights for some Boolean functions. *J. Math. Cryptology*, **6(2)**, 105–135, 2012.

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

[7] A. Canteaut and M. Videau. Symmetric Boolean Functions. *IEEE Trans. Inf. Theory* **51(8)**, 2791–2881, 2005.

[8] Philip Davis. Circulant Matrices. Chelsea publishing, Second Edition,1994.

[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*, **64(2)**, 1347–1360, 2018.

[10] 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.

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

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

[13] F. N. Castro, L. A. Medina and P. Stănică. Generalized Walsh transforms of symmetric and rotation symmetric Boolean functions are linear recurrent. *Appl. Algebra Eng. Commun. Comput.*, DOI 10.1007/s00200-018-0351-5, 2018.

[14] F. N. Castro, R. Chapman, L. A. Medina, and L. B. Sepúlveda. Recursions associated to trapezoid, symmetric and rotation symmetric functions over Galois fields. to appear in Discrete Math.

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

[16] T. W. Cusick. Weight recursions for any rotation symmetric Boolean functions. *IEEE Trans. Inf. Theory*, **64**, 2962 - 2968, 2018.

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

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

[19] T. W. Cusick, Y. Li, and P. Stănică. On a conjecture for balanced symmetric Boolean functions. *J. Math. Crypt.*, **3**, 1–18, 2009.

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

[21] 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.

[22] K. Feng and F. Liu. New Results On The Nonexistence of Generalized Bent Functions. *IEEE Trans. Inf. Theory* **49**, 3066–3071, 2003.

[23] Y. Guo, G. Gao, Y. Zhao. Recent Results on Balanced Symmetric Boolean Functions. *IEEE Trans. Inf. Theory* **62 (9)**, 5199–5203, 2016.

[24] 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.

[25] Y. Hu and G. Xiao. Resilient Functions Over Finite Fields. *IEEE Trans. Inf. Theory* **49**, 2040–2046, 2003.

[26] 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.

[27] P.V. Kumar, R.A. Scholtz, and L.R. Welch. Generalized Bent Functions and Their Properties. *J. Combinatorial Theory (A)*, **40**, 90–107, 1985.

[28] Y. Li and T.W. Cusick. Linear Structures of Symmetric Functions over Finite Fields. Inf. Processing Letters **97**, 124–127, 2006.

[29] Y. Li and T. W. Cusick. Strict Avalanche Criterion Over Finite Fields. *J. Math. Cryptology* **1(1)**, 65–78, 2006.

[30] M. Liu, P. Lu and G.L. Mullen. Correlation-Immune Functions over Finite Fields. *IEEE Trans. Inf. Theory* **44**, 1273–1276, 1998.

[31] 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.

[32] C. Mitchell. Enumerating Boolean functions of cryptographic significance. *J. Cryptology* **2** (3), 155–170, 1990.

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

[34] 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.

[35] M. G. Parker and A. Pott. On Boolean functions which are bent and negabent. *Proc. Int. Conf. Sequences, Subsequences, Consequences*, LNCS-4893, 9–23, 2007.

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

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

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

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

[40] 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.