University of Puerto Rico
Río Piedras Campus
Faculty of Natural Sciences
Department of Mathematics

Linear recursivity of exponential sums of symmetric functions over Galois Field

By

Leonid Brehsner Sepúlveda Avendaño

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN MATHEMATICS AT THE UNIVERSITY OF PUERTO RICO, RÍO PIEDRAS CAMPUS

May, 2018

APPROVED BY THE DOCTORAL DISSERTATION COMMITTEE
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY IN MATHEMATICS
AT THE UNIVERSITY OF PUERTO RICO

ADVISOR:

Luis A. Medina, Ph.D.
University of Puerto Rico, Río Piedras

READERS:

Francis Castro, Ph.D.
University of Puerto Rico, Río Piedras

Ivelisse Rubio, Ph.D.
University of Puerto Rico, Río Piedras

Nameless, Ph.D.
University of Puerto Rico, Río Piedras

Nameless, Ph.D.
Syracuse University

Nameless, Ph.D.
NYU

Abstract of Ph. D Thesis Presented to the Graduate School
of the University of Puerto Rico, Río Piedras Campus in Partial Fulfillment of the
Requirements for the Degree of Doctor of Philosophy in Mathematics

Linear recursivity of exponential sums of symmetric functions over Galois Field

By

Leonid Brehsner Sepúlveda Avendaño

May 2018

In this thesis we derive bounds on the covering radius of Hermitian codes and give exact values for some. For arbitrary algebraic geometric codes only the lower bounds due to Janwa (1991, 1993) are known. No other prior results are known for the covering radius of Algebraic Geometry codes, including those for that of Hermitian codes. For Hermitian codes over $\mathbb{F}_{q^2}$, where $q = 2, 3,$ and 4, we use our methods to determine their covering radius and organize them in tables. For most of these codes, we get the exact value of the covering radius or they are off by no more than one.

We also derive some new upper bounds on the covering radius of general algebraic codes, and give another improvement to a known bound. Several bounds are conditional on the maximality of the code. We give an equivalent criterion for maximality that is useful for several applications.

Finally, we show that our techniques for determining the covering radius of Hermitian codes can be generalized to similarly nested codes. In particular we give a short new proof of the covering radius of nested Reed-Solomon (as AG codes of genus 0) and also the covering radius of some MDS codes.

To my mother Maria Luz Elena.

ACKNOWLEDGMENTS

I am indebted to my advisor, Professor Heeralal Janwa for his help, advice, constructive suggestions, and support during all the stages of this thesis. I am grateful to some of the excellent professors in the Department of Mathematics at UPR-RP from whom I learned a panorama of exciting mathematical topics. I would like to thank the Department of Mathematics for providing me with financial support that made it possible to study for my thesis. I have been fortunate to have had the support of very close friends in the Department, especially Jesus A. Ochoa, Rafael Aparicio, Luis Ramon Fuentes, Andres Arroyo, Leonid Sepulveda and Ana Yokaira Lopez, several of whom I had known for many years before.

PREFACE

The covering radius is one of the fundamental parameters of a code [?]. It has important applications in computer science, communications and mathematics [?], [?]. Whereas the minimum distance gives the measure of error-correcting capability, the covering radius gives the measure of minimal rate distortion.

This parameter has been intensely investigated during the last decades. Estimating the covering radius is a very difficult task. Likewise deriving good lower and upper bounds for this parameter is hard.

Some of the most widely used codes are those which arise from using methods of algebraic geometry, especially, Hermitian codes, which have very large automorphism groups. While the exact value of the minimum distance of Hermitian codes has been determined, we do not know much about their covering radius.

The main aim of this thesis is the investigation of the covering radius of Hermitian codes. We derive new results on the covering radius of Hermitian codes in Chapter 6. For example, one of our key results is Theorem 6.1.6. where we can obtain the exact covering radius of all the Hermitain codes in the huge range $2g_\chi = q^2 - q \leqslant m < q^3 - q^2$, under the condition of maximality (here g_χ is the genus of the Hermitian curve) We also give some new result on the covering radius of nested algebraic geometric codes in (Chapter 7). Other contributions of this thesis are some new results the covering radius of linear codes over $\mathbb{F}_q^n$ (Chapter 3).

In Chapter 1 we introduce the basic concepts of coding theory. We emphasize some of the relations between the Griesmer bound, Plotkin bound and Singleton bound.

In Chapter 2 we give fundamental results about the covering radius and some basic tools and techniques that we will use later.

In Chapter 3 we present our first new results of this thesis. We derive some new upper bounds on the covering radius, and give another improvement to a known bound due to Janwa [?] that connects all five fundamental parameters of a code. Three other improvements of this bound have appeared subject to various conditions. We also give another upper bound [?]. We also express Janwa's upper bound in a different way and derive some important consequences which allow for further improvements. Many of these bounds are conditional on the code being maximal. We give an equivalent criterion for maximality that is useful for several applications.

In Chapter 4 we give the background on Algebraic Geometry codes and give some basic notion of algebraic geometry, such as projective planes, affine curves, rational functions and divisors, Bezout's Theorem, and the Riemann Roch Theorem. We also show some properties of the Hermitian curves and present a survey of Hermitian codes. We describe these codes using algebraic geometry and give a survey of what is known about the covering radius of AG codes. Finally, we present some lower bounds due to Janwa. [[?],[?],[?]].

In Chapter 5 we introduce Hermitian codes and include some detailed derivations of the exact minimum distance of Hermitian codes given by Yang and Kumar.

Our new results on the covering radius of Hermitian codes are presented in Chapter 6. For Hermitian codes over $\mathbb{F}_{q^2}$, where $q = 2, 3$, we use our methods to determine their covering radius and organize them as tables. For most of these codes, we get values of the covering radius differing by no more than one from the exact value. Finally, in Chapter 7, we give a new proof of the exact covering radius of Reed-Solomon codes and also give new results on the covering radius of nested MDS codes. The material discussed in Chapters 6-7 form part of a paper that is currently being developed [?].

TABLE OF CONTENTS

LIST OF TABLES

LIST OF SYMBOLS

$\mathbb{N}$	Set of natural numbers
$\mathbb{Z}$	Set of integer numbers
$\mathbb{F}_q$	Finite field with q elements
$\mathbb{F}_q^n$	Vector space of dimension n with entries $\mathbb{F}_q$
n	Length of the code
$d_m(C)$	The minimum Hamming distance
$wt(x)$	Weight of the vector x
A^T	Matrix transpose of A
$[n, k, d]_q$	Parameter of a code
$\lfloor x \rfloor$	Floor function
I_k	Identity matrix
$G = (I_k\|A)$	Standard form generator matrix for $[n, k, d]$ code
$C^\perp$	Dual code
H	Check matrix
$C + u$	Coset of C determined by u
MDS	Maximum distance separable code
$Nm(\alpha)$	Norm of α
$Tr(\alpha)$	Trace of α
$R = R(C)$	Covering radius of code C
$B_r(x)$	Sphere of radius r and center x
$V_q^n(r)$	number of vector in $B_r(x)$
$\|A\|$	Cardinal of the set A
$\text{supp}(c)$	Set of coordinates at which c is nonzero.
$R(C; x)$	Residual code with respect to a vector x
$n_q(k, d)$	$= \min\{n : \exists [n, k, d]$q-ary code$\}$
$\mathbb{A}^n$	Affine n dimensional space
$\mathbb{P}^n$	Projective n dimensional space
$\mathbb{F}_q(\chi)$	Field of rational functions on a curve over $\mathbb{F}_q$
t_p	Local parameter
D	Divisor on a curve
$deg(D)$	Degree of a divisor

(f)	Divisor of a function (principal divisor)
$C_1 \bigoplus C_2$	Direct sum
$(f)_0$	Divisor of zeros
$(f)_\infty$	Divisor of poles
$\mathscr{L}(G)$	$\mathscr{L}(G) := \{f \in \mathbb{F}_q(\chi) : (f) + G \succeq 0\} \cup \{0\}$
$L(G)$	Dimension of $\mathscr{L}(G)$
$Im\varphi$	Image of a map
$ker\varphi$	Kernel of a map

CHAPTER 1
Introduction

CHAPTER 2
Recursions associated to trapezoid, symmetric and rotation symmetric functions over Galois fields

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.

In [35], Pieprzyk and Qu introduced rotation symmetric Boolean functions. As in the case of symmetric Boolean functions, these functions turned out to be good candidates for efficient implementations. Moreover, 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 [4, 17, 19, 20, 23, 30, 38, 39].

In some applications related to cryptography it is important for Boolean functions to be balanced. A balanced Boolean function is one for which the number of zeros and the number of ones are equal in its truth table. Let $F(\mathbf{X})$ be a Boolean function. List the elements of $\mathbb{F}_2^n$ in lexicographic order and label them as $\mathbf{x}_0 = (0, 0, \cdots, 0)$, $\mathbf{x}_1 = (0, 0, \cdots, 1)$ and so on. The vector $(F(\mathbf{x}_0), F(\mathbf{x}_1), \cdots, F(\mathbf{x}_{2^n-1}))$ is called the *truth table* of F.

Balancedness of Boolean functions can be studied from the point of view of Hamming weights. 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 study of weights of rotations symmetric Boolean functions has received some attention lately [4, 17, 19, 38]. In particular, it has been observed that weights of cubic rotation symmetric Boolean functions are linear recursive with constant coefficients [4, 17]. For example, consider the Boolean function

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

This Boolean function turns out to be a rotation symmetric Boolean function. The first few values of the sequence $\{\mathrm{wt}(F_n(\mathbf{X}))\}_{n\geq 4}$ are

$$4, 6, 24, 36, 112, 184, 440, 848, 1792, 3680, 7392, \cdots .$$

This sequence of weights satisfies the following linear recurrence with integer coefficients

$$a_n = 2a_{n-1} + 2a_{n-2} - 4a_{n-3} + 4a_{n-5} - 8a_{n-6}. \tag{2.1}$$

Recently, Cusick [16] showed that weights of any rotation symmetric Boolean function satisfy linear recurrences with integer coefficients. In this work, we generalize part of this result to other characteristics.

Balancedness of Boolean functions can also be linked to exponential sums. The *exponential sum* of an n-variable Boolean function $F(\mathbf{X})$ is defined as

$$S(F) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{F(\mathbf{x})}. \tag{2.2}$$

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 in this context. This point of view is also a very active area of research. For some examples, please refer to [1, 3, 9–12, 15, 25, 32, 33, 37].

Exponential sums over finite fields have been useful in mathematics since many problems can be formulated in terms of these sums. Some very well-known examples of exponential sums include the number-theoretical Gauss sums, Kloosterman sums, and Weyl sums. Our general goal is to better understand the behavior of exponential sums. We hope this will bring understanding to many problems in areas like analytic number theory.

The Hamming weight of a Boolean function F and its exponential sums are related by the equation

$$\mathrm{wt}(F) = \frac{2^n - S(F)}{2}. \tag{2.3}$$

Equation (2.3) implies that exponential sums of rotation symmetric Boolean functions also satisfy linear recurrences with integer coefficients.

A natural question to ask is if Cusick's result holds true in the general setting of exponential sums over finite fields or if it is just a particular result for the Boolean case. One of the most important results in this work is a generalization of Cusick's result 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 some 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 includes some preliminary definitions. Section 2.2 is an introduction to 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, he or she is encouraged to read the definition of trapezoid functions, as they are used through out the article. In section 2.3, linear recurrences with integer coefficients are obtained for exponential sums of trapezoid functions over Galois fields. Moreover, it is in this section where it is proved that exponential sums over $\mathbb{F}_q$ of some monomial rotation symmetric polynomials and linear combinations of them satisfy linear recurrences with integer coefficients. The same technique is used 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.

2.1 Preliminaries

As mentioned in the introduction, Pieprzyk and Qu ([35]) 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 [38].

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

$$E_n^k(X_i) = \begin{cases} X_{i+k} & \text{if } i+k \leq n, \\ X_{i+k-n} & \text{if } i+k > n. \end{cases} \tag{2.4}$$

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

$$E_n^k(X_1, X_2, \cdots, X_n) = (E_n^k(X_1), E_n^k(X_2), \cdots, E_n^k(X_n)). \tag{2.5}$$

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

$$E_n^k(X_{i_1}X_{i_2}\cdots X_{i_t}) = E_n^k(X_{i_1})E_n^k(X_{i_2})\cdots E_n^k(X_{i_t}). \tag{2.6}$$

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

$$F(E_n^k(X_1, \cdots, X_n)) = F(X_1, \cdots, X_n) \tag{2.7}$$

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 [4, 17, 19, 20, 23, 30, 38, 39].

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 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

$$\begin{aligned} E_5^1(X_1X_2X_3) &= X_2X_3X_4 \\ E_5^2(X_1X_2X_3) &= X_3X_4X_5 \\ E_5^3(X_1X_2X_3) &= X_4X_5X_1 \\ E_5^4(X_1X_2X_3) &= X_5X_1X_2 \end{aligned} \tag{2.8}$$

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

$$\begin{aligned} R(\mathbf{X}) &= X_1X_2X_3 + X_2X_3X_4 + X_3X_4X_5 + X_4X_5X_1 + X_5X_1X_2 + \\ &\quad X_1X_3 + X_2X_4 + X_3X_5 + X_4X_1 + X_5X_2. \end{aligned} \tag{2.9}$$

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. This minimal information is known in the literature as the *short algebraic normal form* (or SANF). Please refer to [38] for more details.

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

$$R_{j_1,\cdots,j_s}(n) = X_1X_{j_1} \cdots X_{j_s} + X_2X_{j_1+1} \cdots X_{j_s+1} + \cdots + X_nX_{j_1-1} \cdots X_{j_s-1}, \tag{2.10}$$

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 (2.9) is given by

$$R(\mathbf{X}) = R_{2,3}(5) + R_3(5). \tag{2.11}$$

Sometimes the notation $(1, j_1, \cdots, j_s)_n$ is used to represent the monomial rotation Boolean function (2.10), 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

$$S_{\mathbb{F}_q}(F) = \sum_{\mathbf{x} \in \mathbb{F}_q^n} e^{\frac{2\pi i}{p} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(F(\mathbf{x}))}. \tag{2.12}$$

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. Some well-known examples of exponential sums are special cases of definition (2.12). For example, let p be a prime. If $F(X) = aX^2$ with $a \in \mathbb{F}_p$, then

$$S_{\mathbb{F}_p}(F) = \sum_{k=0}^{p-1} e^{2\pi i a k^2/p} = g(a;p), \tag{2.13}$$

where $g(a;p)$ represents the *quadratic Gauss sum mod p.* On the other hand, if $F(X) = aX$ with $a \in \mathbb{F}_p$, then

$$S_{\mathbb{F}_p}(F) = \sum_{k=0}^{p-1} e^{2\pi i a k/p} = 1 + c_p(a), \tag{2.14}$$

where $c_p(a)$ represents the *Ramanujan's sum.* Finally, if $q = p^r$ and $F(X) = X^d + aX$ where $\gcd(d, p^r - 1) = 1$ and $a \in \mathbb{F}_q$, then

$$S_{\mathbb{F}_q}(F) = \sum_{x \in \mathbb{F}_q} e^{\frac{2\pi i}{p} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x^d + ax)} = W_{q,d}(a), \tag{2.15}$$

where $W_{q,d}(a)$ represents a *Weil sum*.

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 2.3.

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

As mentioned in the introduction, Cusick [16] 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 [19], Cusick and Stănică provided a linear recurrence for the sequence of weights for the monomial rotation function $R_{2,3}(n)$. This recurrence, however, was not homogeneous, but it could be transformed into a homogeneous one, see [4]. Later, Cusick and Johns [17] provided recursion orders 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). As just mentioned, 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

$$\tau_{n,k} = \sum_{j=1}^{n-k+1} X_j X_{j+1} \cdots X_{j+k-1}. \tag{2.16}$$

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 these values and connecting the dots produces the shape of an isosceles trapezoid. 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. Trapezoid functions are very interesting objects. Moreover, a handful of them seems to have special properties. For example, a more general version of the trapezoid functions plays a central role in [5]. Also, the trapezoid function $\tau_{4,2} = X_1X_2 + X_2X_3 + X_3X_4$ is known to be a bent and negabent Boolean function [34].

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 ones satisfied by sequences of exponential sums of the rotation symmetric Boolean functions $R_{2,\cdots,k}(n)$. 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 2.2.1. *The sequence $\{S(\tau_{n,k})\}_{n=k}^{\infty}$ satisfies a homogeneous linear recurrence with integer coefficients whose characteristic polynomial is given by*

$$p_k(X) = X^k - 2(X^{k-2} + X^{k-3} + \cdots + X + 1). \tag{2.17}$$

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 2.3.

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

$$S(\tau_{n,3}) = S(\tau_{n-1,3}) + S(\tau_{n-1,3} + X_{n-2}X_{n-1}). \tag{2.18}$$

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

$$S(\tau_{n-1,3} + X_{n-2}X_{n-1}) = S(\tau_{n-2,3}) + S(\tau_{n-2,3} + X_{n-2} + X_{n-3}X_{n-2}). \tag{2.19}$$

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

$$S(\tau_{n-2,3} + X_{n-2} + X_{n-3}X_{n-2}) = S(\tau_{n-3,3}) - S(\tau_{n-3,3} + X_{n-3} + X_{n-4}X_{n-3}). \tag{2.20}$$

The last equation is equivalent (after relabeling) to

$$S(\tau_{n,3}) = S(\tau_{n+1,3} + X_{n+1} + X_nX_{n+1}) + S(\tau_{n,3} + X_n + X_{n-1}X_n). \tag{2.21}$$

Observe that equations (2.18) and (2.19) can be combined to obtain

$$S(\tau_{n,3}) = S(\tau_{n-1,3}) + S(\tau_{n-2,3}) + S(\tau_{n-2,3} + X_{n-2} + X_{n-3}X_{n-2}). \tag{2.22}$$

Let $a_{n,3} = S(\tau_{n,3} + X_n + X_{n-1}X_n)$. Note that (2.21) implies that $S(\tau_{n,3}) = a_{n+1,3} + a_{n,3}$. Therefore, (2.22) can be re-written as

$$(a_{n+1,3} + a_{n,3}) = (a_{n,3} + a_{n-1,3}) + (a_{n-1,3} + a_{n-2,3}) + a_{n-2,3}, \tag{2.23}$$

which is equivalent to

$$a_{n+1,3} = 2a_{n-1,3} + 2a_{n-2,3}. \tag{2.24}$$

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 was done in the case when $k = 3$, turning *OFF* and *ON* several variables leads to

$$\begin{aligned} S(\tau_{n,4}) &= S(\tau_{n-1,4}) + S(\tau_{n-2,4}) + S(\tau_{n-3,4}) \\ &\quad + S(\tau_{n-3,4} + X_{n-3} + X_{n-4}X_{n-3} + X_{n-5}X_{n-4}X_{n-3}) \end{aligned} \tag{2.25}$$

and

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

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 (2.25) can be re-written as

$$(a_{n+1,4} + a_{n,4}) = (a_{n,4} + a_{n-1,4}) + (a_{n-1,4} + a_{n-2,4}) + (a_{n-2,4} + a_{n-3,4}) + a_{n-3,4}, \tag{2.27}$$

which is equivalent to

$$a_{n+1,4} = 2a_{n-1,4} + 2a_{n-2,4} + 2a_{n-3,4}. \tag{2.28}$$

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

$$S(\tau_{n,k}) = \sum_{i=1}^{k-1} S(\tau_{n-i,k}) + S\left(\tau_{n-k+1,k} + \sum_{j=0}^{k-2}\prod_{i=0}^{j} X_{n-k+1-i}\right) \tag{2.29}$$

and as

$$S(\tau_{n,k}) = S\left(\tau_{n+1,k} + \sum_{j=0}^{k-2}\prod_{i=0}^{j} X_{n+1-i}\right) + S\left(\tau_{n,k} + \sum_{j=0}^{k-2}\prod_{i=0}^{j} X_{n-i}\right). \tag{2.30}$$

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

Remark 2.2.2. *We point out that a more general version of Theorem 2.2.1 for cubic functions appears in [5].*

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 the given $p_k(X)$. This is a well-known result for the case when $k = 3$ ([4, 5, 17]), 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 2.2.1.

Lemma 2.2.3. *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 is almost identical to the proof of Theorem 2.2.1. We present it for the case when $k = 4$ and $F(\mathbf{X}) = X_1X_2 + X_1X_2X_3$ in order to convince the reader that the proof follows almost verbatim.

As was done in the proof of Theorem 2.2.1, by turning *OFF* and *ON* several variables one can obtain

$$\begin{aligned} S(\tau_{n,4}+F(\mathbf{X})) &= S(\tau_{n-1,4}+F(\mathbf{X}))+S(\tau_{n-2,4}+F(\mathbf{X}))+S(\tau_{n-3,4}+F(\mathbf{X})) \\ &\quad +S(\tau_{n-3,4}+F(\mathbf{X})+X_{n-3}+X_{n-4}X_{n-3}+X_{n-5}X_{n-4}X_{n-3}) \quad (2.31) \end{aligned}$$

and

$$\begin{aligned} S(\tau_{n,4}+F(\mathbf{X})) &= S(\tau_{n+1,4}+F(\mathbf{X})+X_{n+1}+X_nX_{n+1}+X_{n-1}X_nX_{n+1}) \quad (2.32) \\ &\quad +S(\tau_{n,4}+F(\mathbf{X})+X_n+X_{n-1}X_n+X_{n-2}X_{n-1}X_n). \end{aligned}$$

Let $a_{n,4,F}=S(\tau_{n,4}+F(\mathbf{X})+X_n+X_{n-1}X_n+X_{n-2}X_{n-1}X_n)$ and use (2.31) and (2.32) to get

$$a_{n+1,4,F}=2a_{n-1,4,F}+2a_{n-2,4,F}+2a_{n-3,4,F}. \quad (2.33)$$

Thus, $\{a_{n,4,F}\}$ satisfies the linear recurrence whose characteristic polynomial is $p_4(X)$. Since $S(\tau_{n,4}+F(\mathbf{X}))=a_{n+1,4,F}+a_{n,4,F}$, then $\{S(\tau_{n,4}+F(\mathbf{X}))\}$ satisfies the same recurrence and the result holds for this case. This concludes the proof. □

Theorem 2.2.1 and Lemma 2.2.3 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 2.2.4. *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

$$S(R_{2,3,4}(n))=S(\tau_{n-1,4})+S(\tau_{n-1,4}+X_1X_2X_3+X_1X_2X_{n-1}+X_1X_{n-2}X_{n-1}+X_{n-3}X_{n-2}X_{n-1}). \quad (2.34)$$

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

$$\begin{aligned} &S(\tau_{n-1,4}+X_1X_2X_3+X_1X_2X_{n-1}+X_1X_{n-2}X_{n-1}+X_{n-3}X_{n-2}X_{n-1}) \\ &\qquad = S(\tau_{n-2,4}+X_1X_2X_3) \\ &\qquad\quad + S(\tau_{n-2,4}+X_1X_2+X_1X_2X_3+X_1X_{n-2}+X_{n-3}X_{n-2}+X_{n-4}X_{n-3}X_{n-2}). \end{aligned} \tag{2.35}$$

Again, consider the second term of the right hand side of equation (2.35). Turn X_{n-2} *OFF* and *ON* to get

$$\begin{aligned} &S(\tau_{n-2,4}+X_1X_2+X_1X_2X_3+X_1X_{n-2}+X_{n-3}X_{n-2}+X_{n-4}X_{n-3}X_{n-2}) \\ &\qquad = S(\tau_{n-3,4}+X_1X_2+X_1X_2X_3) \\ &\qquad\quad + S(\tau_{n-3,4}+X_1+X_1X_2+X_1X_2X_3+X_{n-3}+X_{n-4}X_{n-3}+X_{n-5}X_{n-4}X_{n-3}). \end{aligned} \tag{2.36}$$

Equations (2.34), (2.35) and (2.36) lead to the equation

$$\begin{aligned} S(R_{2,3,4}(n)) &= S(\tau_{n-1,4})+S(\tau_{n-2,4}+X_1X_2X_3)+S(\tau_{n-3,4}+X_1X_2+X_1X_2X_3) \\ &\quad + S(\tau_{n-3,4}+X_1+X_1X_2+X_1X_2X_3+X_{n-3}+X_{n-4}X_{n-3}+X_{n-5}X_{n-4}X_{n-3}). \end{aligned} \tag{2.37}$$

Theorem 2.2.1 and Lemma 2.2.3 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

$$S(R_{2,3,\cdots,k}(n)) = S(\tau_{n-1,k}) + \sum_{m=0}^{k-3} S\left(\tau_{n-2-m,k} + \sum_{j=0}^{m} \prod_{i=1}^{k-1-j} X_i\right) + S\left(\tau_{n-k+1,k} + \sum_{j=1}^{k-1}\left(\prod_{i=1}^{j} X_i + \prod_{i=0}^{j-1} X_{n-k+1-i}\right)\right) \tag{2.38}$$

Invoke Theorem 2.2.1 and Lemma 2.2.3 to get the result. This concludes the proof. □

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

$$R_{j_1,\cdots,j_s}(n) = X_1X_{j_1}\cdots X_{j_s} + X_2X_{j_1+1}\cdots X_{j_s+1} + \cdots + X_nX_{j_1-1}\cdots X_{j_s-1}, \tag{2.39}$$

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

$$T_{j_1,\cdots,j_s}(n) = X_1X_{j_1}\cdots X_{j_s} + X_2X_{j_1+1}\cdots X_{j_s+1} + \cdots + X_{n+1-j_s}X_{j_1+n-j_s}\cdots X_{j_{s-1}+n-j_s}X_n. \tag{2.40}$$

For instance, under this notation one has

$$\tau_{n,k} = T_{2,3,\cdots,k}(n). \tag{2.41}$$

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

$$q_k(X) = X^{k+1} - 2X^{k-1} - 2X^{k-2} - \cdots - 2X^3 - 4. \tag{2.42}$$

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.

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

$$\{S(R_{2,3,\cdots,k}(n) + R_{2,3,\cdots,k-1}(n))\}, \tag{2.43}$$

which satisfies the linear recurrence with characteristic polynomial

$$X^k - 2X^{k-1} + 2, \tag{2.44}$$

the sequence

$$\{S(R_{2,3,\cdots,k-1,k}(n) + R_{2,3,\cdots,k-2,k}(n))\}, \tag{2.45}$$

which satisfies the linear recurrence with characteristic polynomial

$$X^k - 2X^{k-1} + 2X - 2, \tag{2.46}$$

and the sequence

$$\{S(R_{2,3,\cdots,k-2,k}(n) + R_{2,3,\cdots,k-1}(n) + R_{2,3,\cdots,k}(n))\}, \tag{2.47}$$

which satisfies the linear recurrence with characteristic polynomial

$$X^k - 2(X^{k-2} + X^{k-3} + \cdots + X^2 + 1). \tag{2.48}$$

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 [16], which includes *Mathematica* code that calculates a linear recurrence for the weights of a given rotation.

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

$$S_{\mathbb{F}_q}(F) = \sum_{\mathbf{x}\in\mathbb{F}_q^n} e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(F(\mathbf{x}))}, \tag{2.49}$$

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

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{n-l}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j} \prod_{l=0}^{k-s-1} X_{n-l}\right) \tag{2.50}$$

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

$$\begin{aligned} T_{2,3,\cdots,k}(k) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{k-l} &= X_1X_2\cdots X_k + \beta_j X_{j+1}X_{j+2}\cdots X_k + \beta_{j-1}X_jX_{j+1}\cdots X_k \\ &\quad + \cdots + \beta_2 X_3X_4\cdots X_k + \beta_1 X_2X_3\cdots X_k. \end{aligned} \tag{2.51}$$

Consider the right hand side of (2.51). 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 (2.51) into

$$Y_1 Y_2 \cdots Y_k + \sum_{s=1}^{j} \prod_{l=0}^{k-s-1} Y_{k-l}. \tag{2.52}$$

Therefore,

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(k) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{k-l}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(k) + \sum_{s=1}^{j} \prod_{l=0}^{k-s-1} X_{k-l}\right). \tag{2.53}$$

This concludes the base case.

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

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{n-l}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j} \prod_{l=0}^{k-s-1} X_{n-l}\right). \tag{2.54}$$

Consider

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n+1) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{n+1-l}\right). \tag{2.55}$$

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

$$\begin{aligned} S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n+1) + \sum_{s=1}^{j} \beta_s \prod_{l=0}^{k-s-1} X_{n+1-l}) &= S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)\right) \\ &+ \sum_{\alpha \in \mathbb{F}_q^\times} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j+1} \gamma_s(\alpha) \prod_{l=0}^{k-s-1} X_{n-l}\right), \end{aligned} \tag{2.56}$$

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

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j+1} \gamma_s(\alpha) \prod_{l=0}^{k-s-1} X_{n-l}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{s=1}^{j+1} \prod_{l=0}^{k-s-1} X_{n-l}\right). \tag{2.57}$$

Therefore,

$$S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n+1)+\sum_{s=1}^{j}\beta_s\prod_{l=0}^{k-s-1}X_{n+1-l}) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)\right) \\ +\sum_{\alpha\in\mathbb{F}_q^{\times}} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{s=1}^{j+1}\prod_{l=0}^{k-s-1}X_{n-l}\right). \quad (2.58)$$

However, (2.58) 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

$$S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n+1)+\sum_{s=1}^{k-1}\beta_s\prod_{l=0}^{k-s-1}X_{n+1-l}) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)\right) \\ +\sum_{\alpha\in\mathbb{F}_q^{\times}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha\beta_{k-1})} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{s=1}^{k-1}\gamma_s(\alpha)\prod_{l=0}^{k-s-1}X_{n-l}\right), \quad (2.59)$$

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

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{s=1}^{k-1}\gamma_s(\alpha)\prod_{l=0}^{k-s-1}X_{n-l}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{s=1}^{j+1}\prod_{l=0}^{k-s-1}X_{n-l}\right). \quad (2.60)$$

Since

$$\sum_{\alpha\in\mathbb{F}_q^{\times}} e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha\beta_{k-1})} = -1, \quad (2.61)$$

then it follows that

$$S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n+1)+\sum_{s=1}^{k-1}\beta_s\prod_{l=0}^{k-s-1}X_{n+1-l}) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)\right) \\ - S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{s=1}^{k-1}\prod_{l=0}^{k-s-1}X_{n-l}\right). \quad (2.62)$$

Since (2.58) 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 linear recurrence for exponential sums of trapezoid functions over any Galois field.

Theorem 2.3.2. *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*

$$Q_{T,k,\mathbb{F}_q}(X) = X^k - q\sum_{l=0}^{k-2}(q-1)^l X^{k-2-l}. \tag{2.63}$$

In particular, when $q = 2$ we recover Theorem 2.2.1.

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

$$S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) = S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n-1)) + \sum_{\beta\in\mathbb{F}_q^\times} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-1)+\beta\prod_{j=1}^{k-1}X_{n-j}\right) \tag{2.64}$$

However, Lemma 2.3.1 implies

$$S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-1)+\beta\prod_{j=1}^{k-1}X_{n-j}\right) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-1)+\prod_{j=1}^{k-1}X_{n-j}\right) \tag{2.65}$$

for every $\beta \in \mathbb{F}_q^\times$. Therefore, (2.64) reduces to

$$S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) = S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n-1)) + (q-1)S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-1)+\prod_{j=1}^{k-1}X_{n-j}\right) \tag{2.66}$$

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

$$\begin{aligned} S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n-1)+\prod_{j=1}^{k-1} X_{n-j}) = \big(S_{\mathbb{F}_p} T_{2,3,\cdots,k}(n-2)\big) \\ + (q-1) S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-2)+\prod_{j=1}^{k-2} X_{n-1-j}+\prod_{j=1}^{k-1} X_{n-1-j}\right) \end{aligned} \tag{2.67}$$

Thus, (2.66) reduces to

$$\begin{aligned} S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) &= S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n-1)) + (q-1) S_{\mathbb{F}_q}\,(T_{2,3,\cdots,k}(n-2)) \\ &+ (q-1)^2 S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-2)+\prod_{j=1}^{k-2} X_{n-1-j}+\prod_{j=1}^{k-1} X_{n-1-j}\right). \end{aligned} \tag{2.68}$$

Continue in this manner to get the following equation

$$\begin{aligned} S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) &= \sum_{l=1}^{k-1} (q-1)^{l-1} S_{\mathbb{F}_q} T_{2,3,\cdots,k}(n-l)) \qquad (2.69) \\ &+ (q-1)^{k-1} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n-k+1)+\sum_{j=0}^{k-2}\prod_{l=0}^{j} X_{n-k+1-l}\right). \end{aligned}$$

On the other hand, let X_{n+1} assume all its possible values and use Lemma 2.3.1 to get the equation

$$\begin{aligned} S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n+1)+\sum_{j=0}^{k-2}\prod_{l=0}^{j} X_{n+1-l}) = S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) \\ + \sum_{\beta\in\mathbb{F}_q^\times} e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta)} S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{j=0}^{k-2}\prod_{l=0}^{j} X_{n-l}\right). \end{aligned} \tag{2.70}$$

Now use the well-known formula

$$\sum_{\beta\in\mathbb{F}_q^\times} e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta)} = -1. \tag{2.71}$$

to reduce (2.70) to

$$\begin{aligned} S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n+1)+\sum_{j=0}^{k-2}\prod_{l=0}^{j}X_{n+1-l}) &= S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) \\ &- S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{j=0}^{k-2}\prod_{l=0}^{j}X_{n-l}\right). \end{aligned} \tag{2.72}$$

This last equation is equivalent to

$$\begin{aligned} S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) &= S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n+1)+\sum_{j=0}^{k-2}\prod_{l=0}^{j}X_{n+1-l}) \\ &+ S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n)+\sum_{j=0}^{k-2}\prod_{l=0}^{j}X_{n-l}\right). \end{aligned} \tag{2.73}$$

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

$$S_{\mathbb{F}_q}(T_{2,3,\cdots,k}(n)) = a_{n+1}+a_n \tag{2.74}$$

and equation (2.69) is now

$$(a_{n+1}+a_n) \;=\; \sum_{l=1}^{k-1}(q-1)^{l-1}(a_{n+1-l}+a_{n-l})+(q-1)^{k-1}a_{n-k+1}. \tag{2.75}$$

The last equation reduces to

$$a_{n+1} = \sum_{l=0}^{k-2} q(q-1)^l a_{n-1-l} \tag{2.76}$$

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 the Eisenstein-Dumas criterion.

Theorem 2.3.3 (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 2.3.4. *Let* $q = p^r$ *with* p *prime. Suppose that* $\gcd(k, r) = 1$. *Then, the polynomial*

$$Q_{T,k,\mathbb{F}_q}(X) = X^k - q\sum_{l=0}^{k-2}(q-1)^l X^{k-2-l} \tag{2.77}$$

is irreducible over $\mathbb{Q}$.

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

Exponential sums over $\mathbb{F}_q$ of rotation functions $R_{2,\cdots,k}(n)$ 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

$$R_2(n) = X_1X_2 + X_2X_3 + \cdots + X_{n-1}X_n + X_nX_1, \tag{2.78}$$

then we have the following result.

Theorem 2.3.5. *Suppose that* $p > 2$ *is prime. Then,* $\{S_{\mathbb{F}_p}(R_2(n)\}$ *satisfy the homogeneous linear recurrence with characteristic polynomial*

$$Q_{R,2,\mathbb{F}_p}(X) = X^4 - p^2. \tag{2.79}$$

Proof. This is the first result whose proof relies on linear algebra. 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

$$S_{\mathbb{F}_p}(T_2(n) + \beta X_n) = S_{\mathbb{F}_p}(T_2(n) + X_n), \text{ for } \beta \in \mathbb{F}_p^\times \tag{2.80}$$

to get the equation

$$\begin{aligned} S_{\mathbb{F}_p}(R_2(n)) &= S_{\mathbb{F}_p}(T_2(n-2)) + (p-1)S_{\mathbb{F}_p}(T_2(n-2)+X_{n-2}) \\ &\quad + \sum_{\alpha\in\mathbb{F}_p^\times}\sum_{\beta\in\mathbb{F}_p} e^{\frac{2\pi i}{p}\alpha\beta} S_{\mathbb{F}_p}(T_2(n-2)+\alpha X_1+\beta X_{n-2}), \end{aligned} \tag{2.81}$$

Let

$$\begin{aligned} a_0(n) &= S_{\mathbb{F}_p}(T_2(n)) \\ a_1(n) &= S_{\mathbb{F}_p}(T_2(n)+X_n) \\ b_{\alpha,\beta}(n) &= S_{\mathbb{F}_p}(T_2(n)+\alpha X_1+\beta X_n) \ \text{ for } \alpha\in\mathbb{F}_p^\times, \beta\in\mathbb{F}_p. \end{aligned} \tag{2.82}$$

Then,

$$S_{\mathbb{F}_p}(R_2(n)) = a_0(n-2) + (p-1)a_1(n-2) + \sum_{\alpha\in\mathbb{F}_p^\times}\sum_{\beta\in\mathbb{F}_p} e^{\frac{2\pi i}{p}\alpha\beta} b_{\alpha,\beta}(n-2). \tag{2.83}$$

Observe that

$$\begin{aligned} a_0(n) &= a_0(n-1) + (p-1)a_1(n-1) \\ a_1(n) &= a_0(n-1) - a_1(n-1) \\ b_{\alpha,\beta}(n) &= \sum_{\gamma\in\mathbb{F}_p} e^{\frac{2\pi i}{p}(\beta\gamma)} b_{\alpha,\gamma}(n-1), \end{aligned} \tag{2.84}$$

which can be written in matrix form as

$$\begin{pmatrix} a_0(n) \\ a_1(n) \\ b_{1,0}(n) \\ b_{1,1}(n) \\ \vdots \\ b_{p-1,p-1}(n) \end{pmatrix} = A(p) \begin{pmatrix} a_0(n-1) \\ a_1(n-1) \\ b_{1,0}(n-1) \\ b_{1,1}(n-1) \\ \vdots \\ b_{p-1,p-1}(n-1) \end{pmatrix} \tag{2.85}$$

where

$$A(p) \;\;= \left(\begin{array}{c|c|c|c|c} A_0(p) & O & O & \cdots & O \\ \hline O & A_1(p) & O & \cdots & O \\ \hline O & O & A_2(p) & \cdots & O \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline O & O & O & \cdots & A_{p-1}(p) \end{array}\right), \tag{2.86}$$

and

$$A_0(p) = \begin{pmatrix} 1 & p-1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad A_j(p) = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & e^{\frac{2\pi i}{p}} & e^{\frac{4\pi i}{p}} & \cdots & e^{\frac{2(p-1)\pi i}{p}} \\ 1 & e^{\frac{4\pi i}{p}} & e^{\frac{8\pi i}{p}} & \cdots & e^{\frac{2\times 2(p-1)\pi i}{p}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & e^{\frac{2(p-1)\pi i}{p}} & e^{\frac{4(p-1)\pi i}{p}} & \cdots & e^{\frac{2\times(p-1)^2\pi i}{p}} \end{pmatrix}, \tag{2.87}$$

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

$$A_j(p)^2 = \begin{pmatrix} p & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & p \\ 0 & 0 & \cdots & p & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & p & \cdots & 0 & 0 \end{pmatrix}. \tag{2.88}$$

Therefore,

$$A_j(p)^4 = p^2 I_p, \tag{2.89}$$

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

$$Q_{R,2,\mathbb{F}_p}(X) = X^4 - p^2. \tag{2.90}$$

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 this recurrence. This concludes the proof. □

We are now ready to prove one of the main results of this article. That is, exponential sums of $R_{2,\cdots,k}(n)$ satisfy linear recurrences with integer coefficients.

Theorem 2.3.6. *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+1} 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

$$a_{\boldsymbol{\alpha};\boldsymbol{\beta}}(n) = S_{\mathbb{F}_q}\left(T_{2,3,\cdots,k}(n) + \sum_{j=1}^{k-1}\left(\alpha_j \prod_{l=1}^{j} X_{n+1-l} + \beta_j \prod_{l=1}^{j} X_l\right)\right), \tag{2.91}$$

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

$$a_{\boldsymbol{\alpha};\boldsymbol{\beta}}(n) = \sum_{\boldsymbol{\gamma},\boldsymbol{\lambda} \in \mathbb{F}_q^{k-1}} c_{\boldsymbol{\gamma},\boldsymbol{\lambda}} \cdot a_{\boldsymbol{\gamma},\boldsymbol{\lambda}}(n-1), \tag{2.92}$$

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 (2.92) and $F(X)$ be some 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. In other words, if $m(X)$ is the minimal polynomial of $A_{2,3,\cdots,k}(q)$, then there is a polynomial with integer coefficients $F(X)$ such that $m(x)$ divides $F(X)$. This polynomial $F(X)$ is an annihilating polynomial for $A_{2,3,\cdots,k}(q)$.

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. □

Definition 2.3.7. *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 2.3.8. *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 2.3.5 and 2.3.6.*

Theorem 2.3.6 can be generalized to monomial rotation functions of the form $R_{j_1,\cdots,j_s}(n)$, for integers $j_0=1<j_1<\cdots<j_s$, and linear combinations of them. Consider

$$S_{\mathbb{F}_q}(R_{j_1,\cdots,j_s}(n+j_s)).$$

Observe that

$$R_{j_1,\cdots,j_s}(n+j_s) = T_{j_1,\cdots,j_s}(n) + X_{n+1}X_{n+j_1}\cdots X_{n+j_s} \\ + \sum_{m=0}^{s-1}\sum_{l=j_s-j_{m+1}+1}^{j_s-j_m}\left(\prod_{i=0}^{m} X_{j_i+l+n}\prod_{i=m+1}^{s} X_{j_i-j_s+l} + \prod_{i=0}^{s} X_{j_i-j_s+l+n}\right).$$

Therefore, by turning *OFF* and *ON* the variables $X_{n+j_s},\cdots,X_{n+j_1},X_{n+j_0}$ we can express $S_{\mathbb{F}_q}(R_{j_1,\cdots,j_s}(n+j_s))$ as a linear combination of terms $a_{\boldsymbol{\alpha},\boldsymbol{\beta}}(n)$ similar to (2.91). In fact, the equivalent of the sequence in the argument of $S_{\mathbb{F}_q}(\,\cdot\,)$ in (2.91) is the trapezoid $T_{j_1,\cdots,j_s}(n)$ plus $2(j_s-1)$ terms of lower degree, similar to what happened in (2.91). The set

$$\{\{a_{\boldsymbol{\alpha},\boldsymbol{\beta}}(n)\}\}_{\boldsymbol{\alpha},\boldsymbol{\beta}\in\mathbb{F}_q^{j_s-1}}$$

turns out to be a recursive generating set and therefore the sequence $\{R_{j_1,\cdots,j_s}(n)\}$ satisfies a linear recurrence with constant coefficients. As in Theorem 2.3.6, it can be argued that a linear recurrence with integer coefficients is guaranteed to exist. The argument for linear combinations of monomial rotation functions $R_{j_1,\cdots,j_s}(n)$ is very similar.

As an example of this discussion, consider the sequence $\{S_{\mathbb{F}_q}(R_{2,4,5}(n+5))\}$. Turning *OFF* and *ON* the variables $X_{n+5},\cdots,X_{n+1}$, the exponential sum $S_{\mathbb{F}_q}(R_{2,4,5}(n+5))$ can be expressed as linear combination of terms of the form

$$a_{\boldsymbol{\alpha},\boldsymbol{\beta}}(n) = S_{\mathbb{F}_q}(T_{2,4,5}(n) + \alpha_1X_1 + \alpha_2X_1X_2 + \alpha_3X_2X_3 + \alpha_4X_1X_3X_4 \\ + \beta_1X_{n-2}X_{n-1} + \beta_2X_n + \beta_3X_{n-3}X_{n-2}X_n + \beta_4X_{n-1}X_n)$$

For each $\boldsymbol{\alpha},\boldsymbol{\beta}\in\mathbb{F}_q^4$, we have

$$a_{\boldsymbol{\alpha},\boldsymbol{\beta}}(n) = \sum_{\boldsymbol{\gamma},\boldsymbol{\lambda}\in\mathbb{F}_q^4} c_{\boldsymbol{\gamma},\boldsymbol{\lambda}}a_{\boldsymbol{\gamma},\boldsymbol{\lambda}}(n-1),$$

where $c_{\boldsymbol{\gamma},\boldsymbol{\lambda}}\in\mathbb{Z}[\zeta_p]$, where $\zeta_p = e^{2\pi i/p}$. Thus, $\{S_{\mathbb{F}_q}(R_{2,4,5}(n))\}$ satisfies a linear recurrence with integer coefficients. All this information is summarized in the following theorem.

Theorem 2.3.9. *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.

The method of turning *OFF* and *ON* is very elementary, but quite powerful. For instance, it can also be 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. This was already hinted by the Boolean case, which is already known, that is, exponential sums of symmetric Boolean functions are linear recurrent. This was first established by Cai, Green and Thierauf [6] and was used in [10] to show that a conjecture of Cusick, Li and Stănică [18] is true asymptotically. In [11], some of the results of [10] where extended to some perturbations of symmetric Boolean functions. This recursivity was also used in [12, 15] to study the periodicity mod p (p prime) of exponential sums of symmetric Boolean functions.

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

$$\sigma_{4,3} = X_1X_2X_3 + X_1X_4X_3 + X_2X_4X_3 + X_1X_2X_4. \tag{2.93}$$

We have the following result.

Theorem 2.3.10. *Let $k \geq 2$ be an integer and $q = p^r$ with p prime and $r \geq 1$. The sequence*

$$\left\{ S_{\mathbb{F}_q}\left(\sum_{j=0}^{k-1} \beta_j \sigma_{n,k-j} \right) \right\} \tag{2.94}$$

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

Proof. We present the proof for $\{S_{\mathbb{F}_q}(\sigma_{n,k})\}$. The general proof follows the same argument. Consider the expression $S_{\mathbb{F}_q}(\sigma_{n+k,k})$. Define

$$a_{\boldsymbol{\beta}}(n) = S_{\mathbb{F}_q}\left(\sigma_{n,k} + \sum_{j=1}^{k-1} \beta_j \sigma_{n,k-j} \right), \tag{2.95}$$

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 $\{S_{\mathbb{F}_q}(\sigma_{n+k,k})\}_{n\geq k}$ satisfies a linear recurrence with constant coefficients. As in the proof of Theorem 2.3.6, it can be argued that a linear recurrence with integer coefficients is guaranteed to exist. This concludes the proof. □

We will not go into more details with elementary symmetric polynomials because the discussion does not bring anything new. We will, however, consider the quadratic case because we consider it fascinating. Moreover, we can calculate the spectrum of the corresponding matrix.

Observe that the collection of sequences

$$\{a_s(n)\} = \{S_{\mathbb{F}_p}(\sigma_{n,2} + s\sigma_{n,1})\}, \tag{2.96}$$

where $s \in \mathbb{F}_p$, is a recursive generating set for $\{S_{\mathbb{F}_p}(\sigma_{n,2})\}$. Also,

$$\begin{pmatrix} a_0(n) \\ a_1(n) \\ \vdots \\ a_{p-1}(n) \end{pmatrix} = M(p) \begin{pmatrix} a_0(n-1) \\ a_1(n-1) \\ \vdots \\ a_{p-1}(n-1) \end{pmatrix}, \tag{2.97}$$

where 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

$$RTC(a_1, a_2, a_3, \cdots, a_n) = (a_n, a_1, a_2, \cdots, a_{n-1}) \tag{2.98}$$

and RTC^m represents m iterations of RTC. In other words, the matrix $M(p)$ has (j,k)-entry $\zeta_p^{j(k-j)}$ where $\zeta_p = \exp(2\pi i/p)$ and j and k run from 0 to $p-1$ inclusive.

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

$$M(p)\overline{M(p)}^T = \overline{M(p)}^T M(p) = pI_p, \tag{2.99}$$

where I_p represents the $p \times p$ identity matrix. This implies that $M(p)$ is diagonalizable and that all its eigenvalues satisfy $|\lambda| = \sqrt{p}$. Moreover, its eigenvalues are related to $g(a;p)$, the number-theoretical quadratic Gauss sum mod p . It is well-established that

$$g(a;p) = \left(\frac{a}{p}\right) g(1;p) \quad \text{and} \quad g(1;p) = \begin{cases} \sqrt{p} & p \equiv 1 \mod 4 \\ i\sqrt{p} & p \equiv 3 \mod 4. \end{cases} \tag{2.100}$$

where (a/p) denotes the Legendre's symbol.

Theorem 2.3.11. *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*

$$\lambda = \left(\frac{-2}{p}\right) g(1;p)\zeta_p^{-sa^2}. \tag{2.101}$$

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

Proof. Let p be an odd prime number and $\zeta_p = \exp(2\pi i/p)$. The matrix $M(p)$ has (j,k)-entry $\zeta_p^{j(k-j)}$ 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 $\zeta_p^{s(k-a)^2}$ 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

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

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

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

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 $\left(\frac{-2}{p}\right) g(1,p)\zeta_p^{-sa^2}$ for $1 \leq a \leq \frac{1}{2}(p-1)$. This completes the proof. □

Note that if λ is defined as in (2.101), then equation (2.100) implies

$$\lambda^p = (-i)^{\frac{p-1}{2}} \sqrt{p^p} \tag{2.102}$$

for every odd prime p. Therefore, Theorem 2.3.11 leads to

$$M(p)^{2p} = \left(\frac{-1}{p}\right) p^p I_p, \tag{2.103}$$

where I_p represents the $p \times p$ identity matrix. Thus,

$$X^{2p} - \left(\frac{-1}{p}\right) p^p \tag{2.104}$$

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 (2.104). The eigenvalues provided in Theorem 2.3.11 can also be used to find closed formulas for $S_{\mathbb{F}_p}(\sigma_{n,2})$.

2.4 Concluding remarks

We have shown that exponential sums over Galois fields of trapezoid polynomials and linear combinations of rotation polynomials of the form $R_{j_1,\cdots,j_s}(n)$ satisfy linear recurrences with integer coefficients. Moreover, this fact can be proved by playing a simple game of turning *OFF* and *ON* some variables. This method is elementary, but quit powerful. Perhaps it can be also be used to show that exponential sums over Galois fields of other rotation symmetric functions satisfy linear recurrences. For example, consider

$$F_1(n) = X_1^2X_2X_3 + X_2^2X_3X_4 + \cdots + X_n^2X_1X_2,$$

where the indices are taken modulo n and the complete system of residues is $\{1, 2, \cdots, n\}$. Then, $\{S_{\mathbb{F}_3}(F_1(n))\}$ satisfies the linear recurrence whose characteristic polynomial is given by $(X^2+3)(X^3-3X-6)$. Also, if

$$F_2(n) = X_1^2X_2^2X_3^2 + X_2^2X_3^2X_4^2 + \cdots + X_n^2X_1^2X_2^2,$$

then $\{S_{\mathbb{F}_3}(F_2(n))\}$ satisfies the linear recurrence whose characteristic polynomial is given by

$$\left(X^2+3\right)\left(X^2-12X+48\right)\left(X^2-6X+12\right).$$

The question if exponential sums over Galois fields of any rotation symmetric polynomial satisfy linear recurrence with integer coefficients is part of future work.

CHAPTER 3
Closed formulas for exponential sums of symmetric polynomials over Galois fields

Combinatorics and number theory are classic areas of mathematics with fascinating objects that captivate the attention of mathematicians. One subject that lies in the intersection of these two areas is the theory of Boolean functions. These beautiful functions have plenty of applications to different scientific fields. Some examples include electrical engineering, game theory, cryptography, coding theory and information theory.

An n-variable *Boolean function* is a function $F(\mathbf{X})$ from the vector space $\mathbb{F}_2^n$ to $\mathbb{F}_2$ where $\mathbb{F}_2 = \{0, 1\}$ is the binary field and n is a positive number. 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 (output table). Balancedness of Boolean functions can be studied from the point of exponential sums. The *exponential sum* of a Boolean function $F(\mathbf{X})$ over $\mathbb{F}_2$ is defined as

$$S(F) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{F(\mathbf{x})}. \tag{3.1}$$

Observe that a Boolean function is balanced if and only if $S(F) = 0$.

Memory restrictions of current technology have made the problem of efficient implementations of Boolean functions a challenging one. In general, this problem is very hard to tackle, but imposing conditions on these functions may ease the problem. For instance, symmetric Boolean functions are good candidates for efficient implementations and today they are an active area research [6, 10–12, 14, 15, 18].

In general, to find closed formulas for exponential sums of symmetric Boolean functions was an open problem until Cai, Green and Thierauf found formulas for them in the 1990's [6]. Moreover, their formulas imply that exponential sums of symmetric Boolean functions have a recursive nature. This has been exploited in [10–12, 15**?**]. In the particular case of [10], the recursive nature of these sequences and their closed formulas were used to prove asymptotically a conjecture about the balancedness of elementary symmetric Boolean polynomials [18].

Many cryptographic properties, like correlation immune functions, resilient functions and bent functions have been extended to other finite fields [21, 24, 26–29]. Thus, a natural problem to explore is the possibility that the results mentioned in the above paragraph can be extended to other finite fields or perhaps they are just natural consequences of working over the binary field. Recently in [14], it has been showed that exponential sums of linear combinations of elementary symmetric polynomials over Galois fields also satisfy linear recurrences. Therefore, at least the recursive nature of these sequences is not unique to the binary field.

The recursive nature of exponential sums of symmetric polynomials over Galois fields presented in [14] did not include explicit linear recurrences for these sequences. Instead, they proved the existence of such recurrences and provided a method to find them. In this article, we find explicit linear recurrences for these sequences. This is done by providing closed formulas for exponential sums of symmetric polynomials over Galois fields. In other words, in this chapter we settle the problem of finding closed formulas for exponential sums of linear combinations of elementary symmetric polynomials over any Galois field. This extends the work of Cai, Green and Thierauf for the binary field [6] to every finite field. As far as we know, this is new.

Our closed formulas depend on some multinomial sum expressions for our exponential sums. These expressions provide 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. A solution $(\delta_0, \delta_1, \cdots, \delta_n)$ to the equation

$$\sum_{j=0}^{n} \delta_j \binom{n}{j} = 0, \quad \delta_j \in \{-1, 1\}, \tag{3.2}$$

is said to give a *bisection of the binomial coefficients* $\binom{n}{j}$, $0 \leq j \leq n$. Observe that a solution to (3.10) provides us with two disjoints sets A, B such that $A \cup B = \{0, 1, 2, \cdots, n\}$ and

$$\sum_{j \in A} \binom{n}{j} = \sum_{j \in B} \binom{n}{j} = 2^{n-1}. \tag{3.3}$$

The problem of bisecting binomial coefficients is a very interesting problem in its own right, but it is out of the scope of this work. However, we believe that the connection between exponential sums of symmetric polynomials and a problem similar to bisecting binomial coefficients is very appealing and underlines the balancedness of symmetric polynomials over finite fields. It also has the potential to spark further research.

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.

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

$$F(\mathbf{X}) = \boldsymbol{e}_{n,k_1} \oplus \boldsymbol{e}_{n,k_2} \oplus \cdots \oplus \boldsymbol{e}_{n,k_s}, \tag{3.4}$$

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 (3.4). For example,

$$\begin{aligned} \boldsymbol{e}_{3,[2,1]} &= \boldsymbol{e}_{3,2} \oplus \boldsymbol{e}_{3,1} \qquad (3.5) \\ &= X_1X_2 \oplus X_3X_2 \oplus X_1X_3 \oplus X_1 \oplus X_2 \oplus X_3. \end{aligned}$$

As mentioned in the introduction, it is known that exponential sums of symmetric Boolean functions are linear recursive [6, 10]. Moreover, closed formulas for them are well known. In fact, Cai et al. [6] proved the following theorem.

Theorem 3.1.1 ([6])**.** *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*

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

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

$$c_j(k_1,\cdots,k_s) = \frac{1}{2^r}\sum_{t=0}^{2^r-1}(-1)^{\binom{t}{k_1}+\cdots+\binom{t}{k_s}}\zeta_j^{-t}. \tag{3.6}$$

Theorem 3.1.1 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 3.1.1 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 [22]. The same behavior holds true for perturbations of symmetric Boolean functions.

One of the goals of this article is to generalize Theorem 3.1.1 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

$$S_{\mathbb{F}_q}(F) = \sum_{\mathbf{x}\in\mathbb{F}_q^n} e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(F(\mathbf{x}))}, \tag{3.7}$$

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

$$\mathrm{Tr}_{\mathbb{F}_{p^l}/\mathbb{F}_p}(\alpha) = \sum_{j=0}^{l-1} \alpha^{p^j}, \tag{3.8}$$

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, does not provide specific linear recurrences for these functions. Instead, it gives a procedure that relies on linear algebra to calculate them. A closed formula for these sequences, like the one presented in Theorem 3.1.1, would allow us to find such recurrences. Perhaps it can also be used to settle, at least asymptotically, the generalization of Cusick, Li and Stănică conjecture for Galois fields, see [2].

The formal definition of an exponential sum is not very useful if one desires to calculate the value of $S_{\mathbb{F}_q}(F)$. In fact, in general, this problem is clearly exponentially hard. However, imposing conditions on the function F sometimes simplifies matters. For example, in the case of symmetric Boolean functions, it is not hard to show that

$$S(\boldsymbol{e}_{n,[k_1,\cdots,k_s]}) = \sum_{j=0}^{n} (-1)^{\binom{j}{k_1}+\cdots+\binom{j}{k_s}} \binom{n}{j}. \tag{3.9}$$

Equation (3.9) is a clear computational improvement over (3.1). It also connects (as mentioned in the introduction) the problem of balancedness of symmetric Boolean functions to the problem of bisecting binomial coefficients (see Mitchell [31]). As mentioned in the introduction, a solution $(\delta_0, \delta_1, \cdots, \delta_n)$ to the equation

$$\sum_{j=0}^{n} \delta_j \binom{n}{j} = 0, \;\; \delta_j \in \{-1, 1\}, \tag{3.10}$$

is said to give a *bisection of the binomial coefficients* $\binom{n}{j}$, $0 \leq j \leq n$. The problem of bisecting binomial coefficients is an interesting problem in its own right, however, it is out of the scope of this work. The interested reader is invited to read [31**?**].

In the next section, we proved a formula similar to (3.9) for $S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})$ using multinomial coefficients. The formula is not only a computational improvement over the formal definition of $S_{\mathbb{F}_q}(F)$, but also provide a connection to a problem similar to the problem of bisecting of binomial coefficients for multinomial coefficients. 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. We decided to include it here for completeness purposes.

Theorem 3.1.2 (Lucas' Theorem)**.** *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

$$\binom{n+D}{k} \equiv \binom{n}{k} \mod p. \tag{3.11}$$

This will be used throughout the rest of the chapter.

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 (3.7). 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

$$\Lambda_{a_1}(k, m) = a_1^k \binom{m}{k} \tag{3.12}$$

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

$$\Lambda_{a_1,a_2,\cdots,a_{l+1}}(k, m_1, m_2, \cdots, m_{l+1}) = \sum_{j=0}^{m_{l+1}} \binom{m_{l+1}}{j} a_{l+1}^j \Lambda_{a_1,\cdots,a_l}(k-j, m_1, m_2, \cdots, m_l), \tag{3.13}$$

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

Lemma 3.2.1. *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,*

$$\boldsymbol{e}_{n,k}(\mathbf{x}) = \Lambda_{a_1,\cdots,a_l}(k, m_1, \cdots, m_l). \tag{3.14}$$

Proof. First observe that if $l = 1$, that is, $\mathbf{x} \in A_1^n$, then

$$\boldsymbol{e}_{n,k}(\mathbf{x}) = a_1^k \binom{m_1}{k}. \tag{3.15}$$

Now observe that if the variables $X_n, X_{n-1}, \cdots, X_{n-r+1}$ are set to be α, then

$$\boldsymbol{e}_{n,k}(X_1, \cdots, X_{n-r}, \alpha, \cdots, \alpha) = \sum_{j=0}^{r} \binom{r}{j} \alpha^j \boldsymbol{e}_{n-r,k-j}(X_1, \cdots, X_{n-r}). \tag{3.16}$$

Symmetry and an induction argument finish the proof. □

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

Theorem 3.2.2. *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,*

$$\begin{aligned} S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k}) &= \sum_{m_1=0}^{n} \sum_{m_2=0}^{n-m_1} \sum_{m_3=0}^{n-m_1-m_2} \cdots \sum_{m_{q-1}=0}^{n-m_1-\cdots-m_{q-2}} \binom{n}{m_0^*, m_1, m_2, \cdots, m_{q-1}} \\ &\quad \times \exp\left(\frac{2\pi i}{p} Tr_{\mathbb{F}_q/\mathbb{F}_p}(\Lambda_{\alpha_1,\cdots,\alpha_{q-1}}(k, m_1, \cdots, m_{q-1})\right), \end{aligned}$$

where $m_0^* = n - (m_1 + \cdots + m_{q-1})$.

Proof. Consider a tuple $\mathbf{x} \in \mathbb{F}_q^n$. Suppose that α_j appears m_j times in $\mathbf{x}$. Clearly, this implies

$$n = m_0^* + m_1 + m_2 + \cdots + m_{q-1}.$$

A simple counting argument shows that there are

$$\binom{n}{m_1}\binom{n-m_1}{m_2}\binom{n-m_1-m_2}{m_3}\cdots\binom{n-m_1-m_2-\cdots-m_{q-2}}{m_{q-1}} \tag{3.17}$$

of such tuples. This number can be written in multinomial form as

$$\binom{n}{m_0^*, m_1, m_2, \cdots, m_{q-1}}. \tag{3.18}$$

Observe that Lemma 3.2.1 implies that the value of $\boldsymbol{e}_{n,k}$ on each of these tuples is

$$\boldsymbol{e}_{n,k}(\mathbf{x}) = \Lambda_{\alpha_1,\cdots,\alpha_{q-1}}(k, m_1, \cdots, m_{q-1}). \tag{3.19}$$

Adding over all possible choices of $m_1, m_2, \cdots, m_{q-1}$ produces the result. □

An easy adjustment to the proof of Theorem 3.2.2 leads the following corollary.

Corollary 3.2.3. *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*

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

Then,

$$\begin{aligned} S_{\mathbb{F}_q}\left(\sum_{j=1}^{s} \beta_j \boldsymbol{e}_{n,k_j}\right) &= \sum_{m_1=0}^{n} \sum_{m_2=0}^{n-m_1} \sum_{m_3=0}^{n-m_1-m_2} \cdots \sum_{m_{q-1}=0}^{n-m_1-\cdots-m_{q-2}} \binom{n}{m_0^*, m_1, m_2, \cdots, m_{q-1}} \\ &\quad \times \exp\left(\frac{2\pi i}{p} Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\sum_{j=1}^{s} \beta_j \Lambda_{\alpha_1,\cdots,\alpha_{q-1}}(k_j, m_1, \cdots, m_{q-1})\right)\right). \end{aligned}$$

Proof. The proof follows the same argument as in Theorem 3.2.2. □

Theorem 3.2.2 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

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

The notation $\boldsymbol{\lambda} \dashv_q n$ implies that $\boldsymbol{\lambda}$ is a partition of n and has at most q entries. For example, if $\boldsymbol{\lambda} = (6, 3, 1)$, then $\boldsymbol{\lambda} \dashv_4 10$ because it has 3 entries and $3 \leq 4$. On the other hand, if $\boldsymbol{\lambda} = (4, 2, 2, 1, 1)$, then $\boldsymbol{\lambda} \dashv 10$, but $\boldsymbol{\lambda} \not\dashv_4 10$. From now on, we will see partitions $\boldsymbol{\lambda} \dashv_q n$ as lists of length q. Of course, by definition, a partition $\boldsymbol{\lambda} \dashv_q n$ may have less than q entries. If that is the case, right-pad zeros to the list until it has q entries. For example, $\boldsymbol{\lambda} = (6, 3, 1)$ is such that $\boldsymbol{\lambda} \dashv_4 10$. In this case, we view $\boldsymbol{\lambda}$ as $\boldsymbol{\lambda} = (6, 3, 1, 0)$.

If $\boldsymbol{\lambda} \dashv n$, then the symbol

$$\binom{n}{\boldsymbol{\lambda}}$$

represents the multinomial obtained from $\boldsymbol{\lambda}$. For example, if $\boldsymbol{\lambda} = (6, 3, 1)$, then

$$\binom{10}{\boldsymbol{\lambda}} = \binom{10}{6, 3, 1}.$$

By a *rearrangement* of $\boldsymbol{\lambda}$ we mean a permutation of the symbols in $\boldsymbol{\lambda}$. For example, the set of all different rearrangements of $\boldsymbol{\lambda} = (2,2,1,1)$ is

$$\begin{array}{ll} (2,2,1,1), & (2,1,2,1) \\ (2,1,1,2), & (1,2,2,1) \\ (1,2,1,2), & (1,1,2,2). \end{array}$$

We use $\mathrm{Sym}(\boldsymbol{\lambda})$ 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 3.2.2 and Corollary 3.2.3 can be re-stated as follows.

Theorem 3.2.4. *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,*

$$S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k}) \;=\; \sum_{\boldsymbol{\lambda} \dashv_q n} \binom{n}{\boldsymbol{\lambda}} \sum_{\boldsymbol{\gamma} \in \mathrm{Sym}(\boldsymbol{\lambda})} \exp\left(\frac{2\pi i}{p} Tr_{\mathbb{F}_q/\mathbb{F}_p}(\Lambda_{\alpha_1, \cdots, \alpha_{q-1}}(k, \boldsymbol{\gamma}^*)) \right).$$

Corollary 3.2.5. *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*

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

Then,

$$S_{\mathbb{F}_q}\left(\sum_{j=1}^{s} \beta_j \boldsymbol{e}_{n,k_j} \right) \;=\; \sum_{\boldsymbol{\lambda} \dashv_q n} \binom{n}{\boldsymbol{\lambda}} \sum_{\boldsymbol{\gamma} \in \mathrm{Sym}(\boldsymbol{\lambda})} \exp\left(\frac{2\pi i}{p} Tr_{\mathbb{F}_q/\mathbb{F}_p}\left(\sum_{j=1}^{s} \beta_j \Lambda_{\alpha_1, \cdots, \alpha_{q-1}}(k_j, \boldsymbol{\gamma}^*) \right) \right).$$

For small q, Theorem 3.2.2 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 3.2.2 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

$$S_{\mathbb{F}_3}(\boldsymbol{e}_{12,5}) = 346113 + 92664e^{\frac{2i\pi}{3}} + 92664e^{-\frac{2i\pi}{3}} = 253449. \tag{3.20}$$

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

$$S_{\mathbb{F}_3}(\boldsymbol{e}_{100,7}) = 113935090835950800739864834563949291416514642941, \tag{3.21}$$

and 41.28 seconds to calculate

$$S_{\mathbb{F}_4}(\boldsymbol{e}_{50,5}) = 15873509746687443287473232816. \tag{3.22}$$

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.

Theorem 3.2.2 and Corollary 3.2.3 also offers a hint to a problem similar to bisections of binomial coefficients for multinomial coefficients. Emulating the binary case, we define (p, q)-*section* of multinomial coefficients (q being a power of p) to be the process of dividing the list

$$\mathscr{L}(n; q) = \left\{ \binom{n}{m_0, m_1, m_2, \cdots, m_{q-1}^*} \right\}, \tag{3.23}$$

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

$$\mathscr{L}(5;3) = \{1,5,10,10,5,1,5,20,30,20,5,10,30,30,10,10,20,10,5,5,1\}. \tag{3.24}$$

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

$$\begin{aligned} l_1(5;3) &= \{1,5,5,10,10,20,30\} \qquad (3.25)\\ l_2(5;3) &= \{1,5,5,10,10,20,30\}\\ l_3(5;3) &= \{1,5,5,10,10,20,30\}. \end{aligned}$$

Example 3.2.7. *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,*

$$\mathscr{L}(6;3) = \{1,6,15,20,15,6,1,6,30,60,60,30,6,15,60,90,60,15,20,60,60,20,15,30,15,6,6,1\}. \tag{3.26}$$

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

$$\begin{aligned} l_1(6;3) &= \{1,6,6,15,15,20,30,30,30,90\} \qquad (3.27)\\ l_2(6;3) &= \{1,6,6,15,15,20,60,60,60\}\\ l_3(6;3) &= \{1,6,6,15,15,20,60,60,60\}. \end{aligned}$$

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 3.2.4 and Corollary 3.2.5, to the Diophantine equation

$$\sum_{\boldsymbol{\lambda} \dashv_q n} \binom{n}{\boldsymbol{\lambda}} x_{\boldsymbol{\lambda}} = 0. \tag{3.28}$$

Observe that every time

$$S_{\mathbb{F}_q}\left(\sum_{j=1}^{s} \beta_j \boldsymbol{e}_{n,k_j}\right) = 0,$$

we find a solution to (3.28).

Example 3.2.8. *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

$$S_{\mathbb{F}_4}\left((1+\alpha)\boldsymbol{e}_{8,3} + (1+\alpha)\boldsymbol{e}_{8,2} + \alpha\boldsymbol{e}_{8,1}\right) = 0. \tag{3.29}$$

Therefore, we have a solution to (3.28) for $n = 8$ *and* $q = 4$. *The integer partitions* $\boldsymbol{\lambda}$ *of* 8 *that satisfies* $\boldsymbol{\lambda} \dashv_4 8$ *are*

$$\begin{array}{llll}
\boldsymbol{\lambda}_1 = (8), & \boldsymbol{\lambda}_2 = (7,1), & \boldsymbol{\lambda}_3 = (6,2), & \boldsymbol{\lambda}_4 = (6,1,1), \\
\boldsymbol{\lambda}_5 = (5,3), & \boldsymbol{\lambda}_6 = (5,2,1), & \boldsymbol{\lambda}_7 = (5,1,1,1), & \boldsymbol{\lambda}_8 = (4,4), \\
\boldsymbol{\lambda}_9 = (4,3,1), & \boldsymbol{\lambda}_{10} = (4,2,2), & \boldsymbol{\lambda}_{11} = (4,2,1,1), & \boldsymbol{\lambda}_{12} = (3,3,2), \\
\boldsymbol{\lambda}_{13} = (3,3,1,1), & \boldsymbol{\lambda}_{14} = (3,2,2,1), & \boldsymbol{\lambda}_{15} = (2,2,2,2). &
\end{array}$$

The solution to (3.28) provided by (3.29) is given by

$$(\delta_1, \delta_2, \cdots, \delta_{15}) = (4, -4, -4, 4, -4, 8, -4, 6, -8, -4, 4, 4, 2, -4, 1).$$

In other words,

$$\sum_{j=1}^{15} \binom{8}{\boldsymbol{\lambda}_j} \delta_j = 0.$$

A natural problem to explore is to see how solutions to (3.28) 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 3.1.1, 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 $\alpha = (c_0, c_1, \dots, c_{D-1}) \in \mathbb{C}^D$. The *$D$-circulant matrix* associated to α, denoted by $\operatorname{circ}(\alpha)$, is defined by

$$\operatorname{circ}(\alpha) := \begin{pmatrix} c_0 & c_1 & \cdots & c_{D-2} & c_{D-1} \\ c_{D-1} & c_0 & \cdots & c_{D-1} & c_{D-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_2 & c_3 & \cdots & c_0 & c_1 \\ c_1 & c_2 & \cdots & c_{D-1} & c_0 \end{pmatrix}. \tag{3.30}$$

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

$$\pi = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}, \tag{3.31}$$

then $\operatorname{circ}(\alpha) = p_\alpha(\pi)$.

Circulant matrices are well-understood objects. For example, it is known that the (normalized) eigenvectors of any circulant matrix circ(α) are given by

$$v_j = \frac{1}{\sqrt{n}}(1, \omega_j, \omega_j^2, \cdots, \omega_j^{D-1})^T, \tag{3.32}$$

where $\omega_j = \exp(2\pi \mathrm{i} j/D)$ and $i = \sqrt{-1}$, with corresponding eigenvalues

$$\lambda_j(\alpha) = p_\alpha(\omega_j) = c_0 + c_1\omega_j + c_2\omega_j^2 + \cdots + c_{D-1}\omega_j^{D-1}. \tag{3.33}$$

Moreover, any circulant matrix circ(α) can be diagonalized in the following form. Consider the *Discrete Fourier Transform* matrix

$$F_n = \begin{pmatrix} \xi_n^{0\cdot 0} & \xi_n^{0\cdot 1} & \cdots & \xi_n^{0\cdot(n-1)} \\ \xi_n^{1\cdot 0} & \xi_n^{1\cdot 1} & \cdots & \xi_n^{1\cdot(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \xi_n^{(n-1)\cdot 0} & \xi_n^{(n-1)\cdot 1} & \cdots & \xi_n^{(n-1)\cdot(n-1)} \end{pmatrix}, \tag{3.34}$$

where $\xi_n = \exp(-2\pi i/n)$. Let $U_n = (1/\sqrt{n})F_n$ be its normalization and define

$$\Delta(\alpha) = \mathrm{diag}(\lambda_0(\alpha), \lambda_1(\alpha), \cdots, \lambda_{D-1}(\alpha)). \tag{3.35}$$

Then,

$$\mathrm{circ}(\alpha) = U_D \Delta(\alpha) U_D^*. \tag{3.36}$$

See [8, Th.3.2.2, p. 72] for more information.

We say that a function $f : \mathbb{Z} \to \mathbb{Z}$ is *periodic* with period D if $f(j + D) = f(j)$ for any $j \in \mathbb{Z}$. Periodicity can be extended to functions $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ without too much effort. The periodicity of a function $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is usually divided by components. We say that a positive integer D_1 is a *period in the first component of* g if

$$g(j_1 + D_1, j_2) = g(j_1, j_2) \tag{3.37}$$

for every $j_1, j_2 \in \mathbb{Z}$. Similarly, we say that a positive integer D_2 is a *period in the second component of* g if

$$g(j_1, j_2 + D_2) = g(j_1, j_2) \tag{3.38}$$

for every $j_1, j_2 \in \mathbb{Z}$. Of course, if g is periodic in its first and second components, then we say that g is periodic. Moreover, $D = \operatorname{lcm}(D_1, D_2)$ is such that

$$g(j_1 + D, j_2 + D) = g(j_1, j_2) \tag{3.39}$$

for every $j_1, j_2 \in \mathbb{Z}$. The concept of periodicity can be extended further to functions from $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ to $\mathbb{Z}$. The discussion is the same as for the case $\mathbb{Z} \times \mathbb{Z}$, so we do not write the details.

We are now ready to start with the argument for our formulas. Consider the summation

$$\sum_{l=0}^{n} a^l \binom{n}{l}. \tag{3.40}$$

Later it will become clear why we choose this sum. Given a positive integer $D > 1$, the sum (3.40) can be splitted as

$$\sum_{l=0}^{n} a^l \binom{n}{l} = \sum_{t=0}^{D-1} r_t(n; a), \tag{3.41}$$

where

$$r_t(n; a) = \sum_{j \equiv t \bmod D} a^j \binom{n}{j}. \tag{3.42}$$

Proposition 3.3.1. *Let $n \in \mathbb{N}$ and $0 \le t \le D - 1$. Then,*

$$r_t(n; a) = \frac{1}{D} \sum_{m=0}^{D-1} \xi_D^{tm} \lambda_m^n, \tag{3.43}$$

where $\xi_D = \exp(2\pi i/D)$ and $\lambda_m = 1 + a\xi_D^{-m}$ are the eigenvalues of $\operatorname{circ}(1, 0, \cdots, 0, a)$.

Proof. The approach of this proof is similar to the one presented in [6]. Note that for $1 \le t \le D - 1$, we have

$$r_t(n; a) = r_t(n - 1; a) + a\, r_{t-1}(n - 1; a). \tag{3.44}$$

Also,

$$r_0(n;a) = r_0(n-1;a) + a\, r_{D-1}(n-1;a). \tag{3.45}$$

Therefore, if we define

$$\boldsymbol{r}(n;a) = \begin{pmatrix} r_0(n;a) \\ r_1(n;a) \\ \vdots \\ r_{D-1}(n;a) \end{pmatrix}, \tag{3.46}$$

then

$$\boldsymbol{r}(n;a) \;\; = \;\; \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & a \\ a & 1 & 0 & \cdots & 0 & 0 \\ 0 & a & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a & 1 \end{pmatrix} \boldsymbol{r}(n-1;a). \tag{3.47}$$

Let $\alpha = (1, 0, \cdots, 0, a)$. The last equation is equivalent to

$$\boldsymbol{r}(n;a) = A_D(a)\boldsymbol{r}(n-1;a), \tag{3.48}$$

where $A_D(a) = \mathrm{circ}(\alpha)$.

Iteration of (3.48) leads to $\boldsymbol{r}(n;a) = A_D(a)^n \boldsymbol{r}(0;a)$. Observe that

$$r_0(0;a) = \binom{0}{0} = 1 \;\text{ and }\; r_t(0;a) = 0 \text{ for } t > 0. \tag{3.49}$$

Thus,

$$\boldsymbol{r}(0;a) = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{3.50}$$

Equation (3.36) now implies that

$$\begin{aligned}\boldsymbol{r}(n;a) &= \frac{1}{D}U_D\Delta(\alpha)^n U_D^*\boldsymbol{r}(0;a) = \frac{1}{D}U_D\Delta(\alpha)^n\begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix} \qquad (3.51)\\ &= \frac{1}{D}U_D\begin{pmatrix}\lambda_0(\alpha)^n\\\lambda_1(\alpha)^n\\\vdots\\\lambda_{D-1}(\alpha)^n\end{pmatrix} = \begin{pmatrix}\frac{1}{D}\sum_{j=0}^{D-1}\xi_D^{(s-1)j}\lambda_0(\alpha)^n\\\frac{1}{D}\sum_{j=0}^{D-1}\xi_D^{(s-1)j}\lambda_1(\alpha)^n\\\vdots\\\frac{1}{D}\sum_{j=0}^{D-1}\xi_D^{(s-1)j}\lambda_{D-1}(\alpha)^n\end{pmatrix}.\end{aligned}$$

It follows that

$$r_t(n;a) = \frac{1}{D}\sum_{j=0}^{D-1}\xi_D^{tj}\lambda_j(\alpha)^n \qquad (3.52)$$

where $\lambda_j(\alpha) = 1 + a\xi_D^{-j}$. □

The following results are easy consequences of the above proposition.

Corollary 3.3.2. *Let F be a periodic function with period D. Suppose that $\xi^D = 1$ (not necessarily primitive). Then,*

$$\sum_{l=0}^{n}\binom{n}{l}a^l\xi^{F(l)} = \frac{1}{D}\sum_{t=0}^{D-1}\xi^{F(t)}\sum_{j=0}^{D-1}\xi_D^{tj}\lambda_j^n, \qquad (3.53)$$

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

Proof. Observe that

$$\begin{aligned}\sum_{l=0}^{n}\binom{n}{l}a^l\xi^{F(l)} &= \sum_{t=0}^{D-1}\left(\sum_{j\equiv t \bmod D}\xi^{F(t)}a^l\binom{n}{j}\right) \qquad (3.54)\\ &= \sum_{t=0}^{D-1}\xi^{F(t)}r_t(n;a).\end{aligned}$$

The result now follows from Proposition 3.3.1. □

Corollary 3.3.3. *Let F be a periodic function with period D. Suppose that $\xi^D = 1$ (not necessarily primitive). Then,*

$$\sum_{l=0}^{n} \binom{n}{l} \xi^{F(l)} = \frac{1}{D} \sum_{t=0}^{D-1} \xi^{F(t)} \sum_{j=0}^{D-1} \xi_D^{tj} \left(1 + \xi_D^{-j}\right)^n, \tag{3.55}$$

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

Proof. Set $a = 1$ in the previous corollary. □

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

Theorem 3.3.4. *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,*

$$S(n) = \sum_{q_1=0}^{n} \sum_{q_2=0}^{n-q_1} \cdots \sum_{q_r=0}^{n-q_1-\cdots-q_{r-1}} \binom{n}{q_1} \binom{n-q_1}{q_2} \cdots \binom{n-q_1-\cdots-q_{r-1}}{q_r} \xi^{F(q_1,\cdots,q_r)}. \tag{3.56}$$

Then,

$$S(n) = \frac{1}{D^r} \sum_{b_r=0}^{D-1} \sum_{b_{r-1}=0}^{D-1} \cdots \sum_{b_1=0}^{D-1} \sum_{j_1=0}^{D-1} \sum_{j_2=0}^{D-1} \cdots \sum_{j_r=0}^{D-1} \xi^{F(b_1,\cdots,b_r)} \xi_D^{j_1 b_r + \cdots + j_r b_1} \lambda_{j_1,\cdots,j_r}^n, \tag{3.57}$$

where $\xi_D = \exp(2\pi i/D)$ and $\lambda_{j_1,\cdots,j_r} = 1 + \xi_D^{-j_1} + \xi_D^{-j_2} + \cdots + \xi_D^{-j_r}$.

Proof. We present the proof for the case when $r = 3$. We decided to do this in order to simplify the writing of the proof. The general case is the same argument repeated multiple times.

Write $S(n)$ as

$$S(n) = \sum_{q_1=0}^{n} \sum_{q_2=0}^{n-q_1} \binom{n}{q_1} \binom{n-q_1}{q_2} \sum_{q_3=0}^{n-q_1-q_2} \binom{n-q_1-q_2}{q_3} \xi^{F(q_1,q_2,q_3)}. \tag{3.58}$$

Apply Corollary 3.3.3 to the last sum to get

$$S(n) = \sum_{q_1=0}^{n} \sum_{q_2=0}^{n-q_1} \binom{n}{q_1} \binom{n-q_1}{q_2} \left(\frac{1}{D} \sum_{b_3=0}^{D-1} \xi^{F(q_1,q_2,b_3)} \sum_{j_1=0}^{D-1} \xi_D^{j_1 b_3} \lambda_{j_1}^{n-q_1-q_2} \right), \tag{3.59}$$

where $\lambda_{j_1} = 1 + \xi_D^{-j_1}$. Re-write this equation as

$$S(n) = \frac{1}{D}\sum_{b_3=0}^{D-1}\sum_{j_1=0}^{D-1}\xi_D^{j_1b_3}\sum_{q_1=0}^{n}\binom{n}{q_1}\lambda_{j_1}^{n-q_1}\sum_{q_2=0}^{n-q_1}\binom{n-q_1}{q_2}(\lambda_{j_1}^{-1})^{q_2}\xi^{F(q_1,q_2,b_3)}. \tag{3.60}$$

Now apply Corollary 3.3.2 to the last sum to get

$$S(n) = \frac{1}{D}\sum_{b_3=0}^{D-1}\sum_{j_1=0}^{D-1}\xi_D^{j_1b_3}\sum_{q_1=0}^{n}\binom{n}{q_1}\lambda_{j_1}^{n-q_1}\left(\frac{1}{D}\sum_{b_2=0}^{D-1}\xi^{F(q_1,b_2,b_3)}\sum_{j_2=0}^{D-1}\xi_D^{j_2b_2}\right)(1+\lambda_{j_1}^{-1}\xi_D^{-j_2})^{n-q_1}. \tag{3.61}$$

However, observe that

$$\lambda_{j_1}^{n-q_1}(1+\lambda_{j_1}^{-1}\xi_D^{-j_2})^{n-q_1} = (\lambda_{j_1}+\xi_D^{-j_2})^{n-q_1} = (1+\xi_D^{-j_1}+\xi_D^{-j_2})^{n-q_1} = \lambda_{j_1,j_2}^{n-q_1}.$$

Therefore,

$$S(n) = \frac{1}{D}\sum_{b_3=0}^{D-1}\sum_{j_1=0}^{D-1}\xi_D^{j_1b_3}\sum_{q_1=0}^{n}\binom{n}{q_1}\left(\frac{1}{D}\sum_{b_2=0}^{D-1}\xi^{F(q_1,b_2,b_3)}\sum_{j_2=0}^{D-1}\xi_D^{j_2b_2}\right)\lambda_{j_1,j_2}^{n-q_1}. \tag{3.62}$$

Rearrange terms to get

$$S(n) = \frac{1}{D^2}\sum_{b_3=0}^{D-1}\sum_{b_2=0}^{D-1}\sum_{j_1=0}^{D-1}\sum_{j_2=0}^{D-1}\xi_D^{j_1b_3+j_2b_2}\lambda_{j_1,j_2}^{n}.\sum_{q_1=0}^{n}\binom{n}{q_1}\xi^{F(q_1,b_2,b_3)}\xi_D^{j_2b_2}(\lambda_{j_1,j_2}^{-1})^{q_1}. \tag{3.63}$$

Apply Corollary 3.3.2 once again. After simplification, we have

$$S(n) = \frac{1}{D^3}\sum_{b_3=0}^{D-1}\sum_{b_2=0}^{D-1}\sum_{b_1=0}^{D-1}\sum_{j_1=0}^{D-1}\sum_{j_2=0}^{D-1}\sum_{j_3=0}^{D-1}\xi_D^{j_1b_3+j_2b_2+j_3b_1}\xi^{F(b_1,b_2,b_3)}\lambda_{j_1,j_2,j_3}^{n}. \tag{3.64}$$

The general case follows using the same method. This concludes the proof. □

Observe that equation (3.57) can be written as

$$S(n) = \sum_{j_1=0}^{D-1}\sum_{j_2=0}^{D-1}\cdots\sum_{j_r=0}^{D-1}d_{j_1,\cdots,j_r}(D)\lambda_{j_1,\cdots,j_r}^{n}, \tag{3.65}$$

where

$$d_{j_1,\cdots,j_r}(D) = \frac{1}{D^r}\sum_{b_r=0}^{D-1}\sum_{b_{r-1}=0}^{D-1}\cdots\sum_{b_1=0}^{D-1}\xi^{F(b_1,\cdots,b_r)}\xi_D^{j_1b_r+\cdots+j_rb_1}. \tag{3.66}$$

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 (3.57) is the sum of all $d_{t'_1,\cdots,t'_r}(D)$ where $(t'_1,\cdots,t'_r)$ is a rearrangement of $(t_1,\cdots,t_r)$. Recall that $\mathrm{Sym}(t_1,\cdots,t_r)$ represents the set of all rearrangements of $(t_1,\cdots,t_r)$. Theorem 3.3.4 now can be re-stated as follows.

Theorem 3.3.5. *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,*

$$S(n) = \sum_{q_1=0}^{n}\sum_{q_2=0}^{n-q_1}\cdots\sum_{q_r=0}^{n-q_1-\cdots-q_{r-1}} \binom{n}{q_1}\binom{n-q_1}{q_2}\cdots\binom{n-q_1-\cdots-q_{r-1}}{q_r}\xi^{F(q_1,\cdots,q_r)}. \tag{3.67}$$

Then,

$$S(n) = \sum_{j_1=0}^{D-1}\sum_{j_2=0}^{j_1}\cdots\sum_{j_r=0}^{j_{r-1}} c_{j_1,\cdots,j_r}(D)\left(1+\xi_D^{-j_1}+\cdots+\xi_D^{-j_r}\right)^n, \tag{3.68}$$

where

$$c_{j_1,\cdots,j_r}(D) = \frac{1}{D^r}\sum_{b_r=0}^{D-1}\sum_{b_{r-1}=0}^{D-1}\cdots\sum_{b_1=0}^{D-1}\xi^{F(b_1,\cdots,b_r)}\sum_{(j'_1,\cdots,j'_r)\in\mathrm{Sym}(j_1,\cdots,j_r)}\xi_D^{j'_1b_r+\cdots+j'_rb_1}, \tag{3.69}$$

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

Proof. This is just a re-statement of Theorem 3.3.4. □

A nice consequence of this result is that sequences of the form $\{S(n)\}$, with $S(n)$ defined as in (3.67), satisfy linear recurrences with integer coefficients. Moreover, we can provide explicit characteristic polynomials for such recurrences.

Corollary 3.3.6. *Let $S(n)$ be defined as in (3.67). Then, the sequence $\{S(n)\}$ satisfies the linear recurrence with integer coefficients whose characteristic polynomial is given by*

$$P_S(X) = \prod_{a_1=0}^{D-1}\prod_{0\le a_2\le a_1}\cdots\prod_{0\le a_r\le a_{r-1}}\left(X-(1+\xi_D^{a_1}+\cdots+\xi_D^{a_r})\right). \tag{3.70}$$

Proof. This is a direct consequence of the above theorem. □

The linear recurrence given in Corollary 3.3.6 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 3.3.7. *Let F be a n-variable Boolean function. The nega-Hadamard transform of F is defined as the complex valued function given by*

$$\mathscr{N}_F(\boldsymbol{a}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{F(\mathbf{x})\oplus\boldsymbol{a}\cdot\mathbf{x}}\ i^{w(\mathbf{x})}, \tag{3.71}$$

where $i = \sqrt{-1}$ and $w(\mathbf{x})$ is the Hamming weight of the vector $\mathbf{x}$. According to Riera and Parker [36], the nega-Hadamard transform is central to the structural analysis of pure n-qubit stabilizer quantum states.

Consider the case $\boldsymbol{a} = \mathbf{0}$, which is the equivalent of the exponential sum in this setting. If F is symmetric, then $\mathscr{N}_F(\mathbf{0})$ can be written as a binomial sum. In particular,

$$\mathscr{N}_{\boldsymbol{e}_{n,[k_1,\cdots,k_s]}}(\mathbf{0}) = \sum_{q=0}^{n}\binom{n}{q} i^q (-1)^{\binom{q}{k_1}+\cdots+\binom{q}{k_s}}. \tag{3.72}$$

Let $r = \lfloor\log_2(k_s)\rfloor + 1$ and $D = 2^r$. Lucas' Theorem and Corollary 3.3.2 imply that

$$\mathscr{N}_{\boldsymbol{e}_{n,[k_1,\cdots,k_s]}}(\mathbf{0}) = \sum_{j=0}^{D-1}\left(\frac{1}{D}\sum_{t=0}^{D-1}(-1)^{\binom{t}{k_1}+\cdots+\binom{t}{k_s}}\xi_D^{tj}\right)\lambda_j^n, \tag{3.73}$$

where $\lambda_j = 1 + i\xi_D^{-j}$. Moreover, Corollary 3.3.6 implies that the sequence $\{\mathscr{N}_{\boldsymbol{e}_{n,[k_1,\cdots,k_s]}}(\mathbf{0})\}$ satisfies the linear recurrence with integer coefficients given by

$$\begin{aligned} P(X) &= \prod_{a=0}^{2^r-1}(X - (1 + i\xi_D^a)) \\ &= (X-2)\Phi_4(X-1)\Phi_8(X-1)\cdots\Phi_{2^r}(X-1), \end{aligned} \tag{3.74}$$

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 3.3.8. *Consider the sum*

$$S(n) = \sum_{q_1=0}^{n} \sum_{q_2=0}^{n-q_1} \sum_{q_3=0}^{n-q_1-q_2} \binom{n}{q_1} \binom{n-q_1}{q_2} \binom{n-q_1-q_2}{q_3} \xi_5^{q_1+q_2+q_3}, \tag{3.75}$$

where $\xi_5 = \exp(2\pi i/5)$. *Let* $F(q_1, q_2, q_3) = q_1 + q_2 + q_3$. *Note that* $F(q_1, q_2, q_3) \mod 5$ *is clearly periodic in each component with period 5. Therefore, Corollary 3.3.6 implies that* $\{S(n)\}$ *satisfies the linear recurrence whose characteristic polynomial is given by*

$$P_S(X) = \prod_{a_1=0}^{4} \prod_{a_2=0}^{a_1} \prod_{a_3=0}^{a_2} \left(X - (1 + \xi_5^{a_1} + \xi_5^{a_2} + \xi_5^{a_3})\right). \tag{3.76}$$

However, the minimal linear recurrence with integer coefficients satisfied by $\{S(n)\}$ *has characteristic polynomial*

$$\begin{aligned} \mu_S(X) &= X^5 - 5X^4 + 10X^3 - 10X^2 + 5X - 244 \\ &= (X-4)\left(X^4 - X^3 + 6X^2 + 14X + 61\right). \end{aligned} \tag{3.77}$$

Thus, it must be true that $\mu_S(X)|P_S(X)$. *Indeed, after simplification, we have*

$$\begin{aligned} P_S(X) =&(X-4)\left(X^2 - 3X + 1\right)\left(X^4 - 11X^3 + 46X^2 - 86X + 61\right) \\ &\left(X^4 - 6X^3 + 16X^2 - 21X + 11\right)\left(X^4 - 6X^3 + 16X^2 - 16X + 16\right) \\ &\left(X^4 - X^3 - 4X^2 + 4X + 11\right)\left(X^4 - X^3 + X^2 - X + 1\right) \\ &\left(X^4 - X^3 + 6X^2 - 6X + 11\right)\left(X^4 - X^3 + 6X^2 + 4X + 1\right) \\ &\left(X^4 - X^3 + 6X^2 + 14X + 61\right). \end{aligned} \tag{3.78}$$

The fact that $\mu_S(X)|P_S(X)$ *is now evident.*

Example 3.3.9. *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*

$$S_m(n) = \sum_{q=0}^{n} \binom{n}{q} \xi_{\pi(m)}^{f_q^{(m)}}, \tag{3.79}$$

where $\xi_{\pi(m)} = \exp(2\pi i/\pi(m))$. *Corollary 3.3.6 implies that* $\{S_m(n)\}$ *satisfies the linear recurrence with integer coefficients whose characteristic polynomial is given by*

$$P_{S_m}(X) = \prod_{a=0}^{\pi(m)-1} (X - (1 + \xi_{\pi(m)}^{a})). \tag{3.80}$$

Moreover, Corollary 3.3.2 implies that its closed form is given by

$$S_m(n) = \sum_{j=0}^{\pi(m)-1} \left(\frac{1}{\pi(m)} \sum_{t=0}^{\pi(m)-1} \xi_{\pi(m)}^{f_t^{(m)}+tj} \right) \left(1 + \xi_{\pi(m)}^{-j} \right)^n. \tag{3.81}$$

This example can be easily generalized to any Lucas sequence of the first kind $u_n(a,b)$ *(the Fibonacci sequence is given by* $u_n(1,-1)$*).*

Let us go back to our exponential sums. The above results can be used to obtain closed formulas for exponential sums of elementary symmetric polynomials. Let $\mathbb{F}_q = \{0, \alpha_1, \cdots, \alpha_{q-1}\}$. Theorem 3.2.2 implies that

$$S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k}) = \sum_{m_1=0}^{n} \sum_{m_2=0}^{n-m_1} \cdots \sum_{m_{q-1}=0}^{n-m_1-\cdots-m_{q-1}} \binom{n}{m_0^*, m_1, m_2, \cdots, m_{q-1}} \xi_p^{\mathrm{Tr}\left(\Lambda_{\alpha_1,\cdots,\alpha_{q-1}}(k,m_1,\cdots,m_{q-1})\right)} \tag{3.82}$$

where $m_0^* = n - (m_1 + \cdots + m_{q-1})$, $\xi_p = \exp(2\pi i/p)$ and $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$. Moreover, note that

$$\binom{n}{m_0^*, m_1, m_2, \cdots, m_{q-1}} = \binom{n}{m_1} \binom{n-m_1}{m_2} \cdots \binom{n - m_1 - \cdots - m_{q-2}}{m_{q-1}}.$$

Therefore, if we let

$$F_{k;\mathbb{F}_q}(m_1, \cdots, m_{q-1}) = \Lambda_{\alpha_1,\cdots,\alpha_{q-1}}(k, m_1, \cdots, m_{q-1}), \tag{3.83}$$

then

$$S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k}) = \sum_{m_1=0}^{n} \sum_{m_2=0}^{n-m_1} \cdots \sum_{m_{q-1}=0}^{n-m_1-\cdots-m_{q-1}} \binom{n}{m_0^*, m_1, m_2, \cdots, m_{q-1}} \xi_p^{\mathrm{Tr}\left(F_{k,\mathbb{F}_q}(m_1,\cdots,m_{q-1})\right)} \tag{3.84}$$

is of the same type as (3.56). It remains to show the periodicity of $F_{k;\mathbb{F}_q}$.

We start with the following lemma.

Lemma 3.3.10. *Let p be prime and $a_1, \cdots, a_l$ be some elements in some field extension of $\mathbb{F}_p$. Define*

$$\Lambda^{(p)}_{a_1,\cdots,a_l}(k, m_1, \cdots, m_l) = \Lambda_{a_1,\cdots,a_l}(k, m_1^+, \cdots, m_l^+) \mod p, \tag{3.85}$$

where

$$m_j^+ = \begin{cases} m_j, & \text{if } m_j > 0 \\ m_j + \left(\left\lfloor \frac{-m_j}{D} \right\rfloor + 1\right) D, & \text{if } m_j \leq 0. \end{cases}$$

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 $D = p^{\lfloor \log_p(k) \rfloor + 1}$.

Proof. We first show that if $m_1, \cdots, m_l$ are all non-negative, then

$$\Lambda_{a_1,\cdots,a_l}(k, m_1, \cdots, m_j + D, \cdots, m_l) \equiv \Lambda_{a_1,\cdots,a_l}(k, m_1, \cdots, m_j, \cdots, m_l) \mod p$$

for each $j = 1, \cdots, l$. The proof of this claim is by induction on l.

Suppose first that $l = 1$. That is, consider

$$\Lambda_{a_1}(k, m_1) = a^k \binom{m_1}{k}. \tag{3.86}$$

Lucas' Theorem implies that if $D = p^{\lfloor \log_p(k) \rfloor + 1}$, then

$$\binom{m_1 + D}{k'} \equiv \binom{m_1}{k'} \mod p, \tag{3.87}$$

for ever $k' \leq k$. Therefore, $\Lambda_{a_1}(k', m_1 + D) \equiv \Lambda_{a_1}(k', m_1) \mod p$ for every $k' \leq k$ and the result holds for $l = 1$.

Suppose now that the result holds for some $l \geq 1$. Consider

$$\Lambda_{a_1,\cdots,a_l,a_{l+1}}(k, m_1, \cdots, m_l, m_{l+1}).$$

Recall that

$$\Lambda_{a_1,\cdots,a_l,a_{l+1}}(k,m_1,\cdots,m_l,m_{l+1}) = \sum_{j=0}^{m_{l+1}} \binom{m_{l+1}}{j} a_{l+1}^j \Lambda_{a_1,\cdots,a_l}(k-j,m_1,\cdots,m_l). \tag{3.88}$$

It is clear that

$$\Lambda_{a_1,\cdots,a_l,a_{l+1}}(k,m_1,\cdots,m_j+D,\cdots,m_l,m_{l+1}) \equiv \Lambda_{a_1,\cdots,a_l,a_{l+1}}(k,m_1,\cdots,m_j,\cdots,m_l,m_{l+1}) \mod p$$

holds for $j = 1,\cdots,l$ (induction hypothesis). It remains to show that it is also true for the variable m_{l+1}. In order to do that, first note that a simple induction argument shows that if $k < 0$, then

$$\Lambda_{a_1,\cdots,a_l}(k,m_1,\cdots,m_l) = 0.$$

Therefore, every term on the right-hand side of (3.88) for which $j > k$ is 0. This implies that the binomial coefficient that accompanies every surviving term in (3.88) satisfies (Lucas' Theorem)

$$\binom{m_{l+1}+D}{j} \equiv \binom{m_{l+1}}{j} \mod p. \tag{3.89}$$

Then,

$$\begin{aligned}\Lambda_{a_1,\cdots,a_l,a_{l+1}}(k,m_1,\cdots,m_l,m_{l+1}+D) &= \sum_{j=0}^{m_{l+1}+D} \binom{m_{l+1}+D}{j} a_{l+1}^j \Lambda_{a_1,\cdots,a_l}(k-j,m_1,\cdots,m_l) \\ &\equiv \sum_{j=0}^{m_{l+1}+D} \binom{m_{l+1}}{j} a_{l+1}^j \Lambda_{a_1,\cdots,a_l}(k-j,m_1,\cdots,m_l) \mod p \\ &\equiv \sum_{j=0}^{m_{l+1}} \binom{m_{l+1}}{j} a_{l+1}^j \Lambda_{a_1,\cdots,a_l}(k-j,m_1,\cdots,m_l) \mod p \\ &\equiv \Lambda_{a_1,\cdots,a_{l+1}}(k,m_1,\cdots,m_{l+1}) \mod p.\end{aligned}$$

Therefore,

$$\Lambda_{a_1,\cdots,a_{l+1}}(k,m_1,\cdots,m_{l+1}+D) \equiv \Lambda_{a_1,\cdots,a_{l+1}}(k,m_1,\cdots,m_{l+1}) \mod p$$

is also true. We conclude by induction that if $m_1, \cdots, m_l$ are non-negative integers, then

$$\Lambda_{a_1,\cdots,a_l}(k, m_1, \cdots, m_j + D, \cdots, m_l) \equiv \Lambda_{a_1,\cdots,a_l}(k, m_1, \cdots, m_j, \cdots, m_l) \mod p$$

for $j = 1, \cdots, l$ and $D = p^{\lfloor \log_p(k)r \rfloor + 1}$.

It is clear that

$$\Lambda_{a_1,\cdots,a_l}(k, m_1, \cdots, m_j + tD, \cdots, m_l) \equiv \Lambda_{a_1,\cdots,a_l}(k, m_1, \cdots, m_j, \cdots, m_l) \mod p \tag{3.90}$$

for every non-negative integer t. Sadly, the same cannot be said about negative t. For example, if m_l is negative, then by the inductive definition of $\Lambda_{a_1,\cdots,a_l}$ one has that

$$\Lambda_{a_1,\cdots,a_l}(k, m_1, \cdots, m_l) = 0.$$

However, this can be circumvented by defining the function

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

where

$$m_j^+ = \begin{cases} m_j, & \text{if } m_j > 0 \\ m_j + \left(\left\lfloor \frac{-m_j}{D} \right\rfloor + 1 \right) D, & \text{if } m_j \leq 0. \end{cases} \tag{3.91}$$

Observe that

$$\Lambda^{(p)}(k, m_1, \cdots, m_j + tD, \cdots, m_l) = \Lambda^{(p)}(k, m_1, \cdots, m_j, \cdots, m_l)$$

for every $t \in \mathbb{Z}$ and $j = 1, \cdots, l$. In other words, $\Lambda^{(p)}_{a_1,\cdots,a_l}(k, m_1, \cdots, m_l)$ is periodic in each of the variables $m_1, \cdots, m_l$ with period D. This concludes the proof. □

Let us go back to formula (3.84) for $S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})$. Note that the value of $\xi_p^{\left(F_{k;\mathbb{F}_q}(m_1,\cdots,m_{q-1})\right)}$ depends only on the value of $F_{k;\mathbb{F}_q}(m_1, \cdots, m_l) \mod p$. Therefore, if we define

$$F^{(p)}_{k;\mathbb{F}_q}(m_1, \cdots, m_{q-1}) := \Lambda^{(p)}_{\alpha_1,\cdots,\alpha_{q-1}}(k, m_1, \cdots, m_{q-1}), \tag{3.92}$$

then

$$S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k}) = \sum_{m_1=0}^{n}\sum_{m_2=0}^{n-m_1}\cdots\sum_{m_{q-1}=0}^{n-m_1-\cdots-m_{q-1}} \binom{n}{m_0^*, m_1, m_2, \cdots, m_{q-1}} \xi_p^{\mathrm{Tr}\left(F^{(p)}_{k,\mathbb{F}_q}(m_1,\cdots,m_{q-1})\right)}. \quad (3.93)$$

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 3.3.11. *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,*

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

where

$$c_{j_1,\cdots,j_{q-1}}(k) = \frac{1}{D^{q-1}}\sum_{b_{q-1}=0}^{D-1}\cdots\sum_{b_1=0}^{D-1}\xi_p^{Tr\left(F^{(p)}_{k;\mathbb{F}_q}(b_1,\cdots,b_{q-1})\right)}\sum_{(j'_1,\cdots,j'_{q-1})\in \mathrm{Sym}(j_1,\cdots,j_{q-1})}\xi_D^{j'_1 b_{q-1}+\cdots+j'_{q-1}b_1},$$

$\xi_m = \exp(2\pi i/m)$, $Tr = Tr_{\mathbb{F}_q/\mathbb{F}_p}$, and $\lambda_{j_1,\cdots,j_{q-1}} = 1 + \xi_D^{-j_1} + \xi_D^{-j_2} + \cdots + \xi_D^{-j_{q-1}}$. 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

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

Proof. The sum in (3.93) is of type (3.56). Moreover, Lemma 3.3.10 implies that the function $F^{(p)}_{n,k;\mathbb{F}_q}(m_1,\cdots,m_{q-1})$ is periodic in each component with period D. The result now follows from Theorem 3.3.5 and its corollary. □

Theorem 3.3.11 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 3.3.12. *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.*

Proof. The characteristic polynomial of such recurrence is a factor of $P_{q,k}(X)$. The result now follows from the fact that the degree of $P_{q,k}(X)$ is $(D)_q/q!$. □

Example 3.3.13. *Consider the sequence* $\{S_{\mathbb{F}_4}(\boldsymbol{e}_{n,3})\}$. *Theorem 3.3.11 implies that this sequence satisfies the linear recurrence whose characteristic is given by*

$$\begin{aligned} P_{4,3}(X) &= \prod_{a_1=0}^{3} \prod_{0\le a_2\le a_1} \prod_{0\le a_3\le a_2} (X-(1+i^{a_1}+i^{a_2}+i^{a_3})) \\ &= (X-4)(X-2)^2X^2(X+2)\left(X^2+4\right)\left(X^2-6X+10\right)\left(X^2-4X+8\right) \\ &\quad \left(X^2-2X+2\right)^2\left(X^2-2X+10\right)\left(X^2+2X+2\right). \end{aligned}$$

The minimal linear recurrence with integer coefficients that $\{S_{\mathbb{F}_4}(\boldsymbol{e}_{n,3})\}$ *satisfies has characteristic polynomial given by*

$$\mu_{4,3}(X) = (X-4)(X-2)\left(X^2+4\right).$$

Note that, as expected, $\mu_{4,3}(X)|P_{4,3}(X)$. *After simplification, the closed formula given by Theorem 3.3.11 is*

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

The function $Tr_{\mathbb{F}_4/\mathbb{F}_2}(\boldsymbol{e}_{n,3})$ *can be identified with a* $2n$*-variable Boolean function. The identification depends on the value-vector of* $Tr_{\mathbb{F}_4/\mathbb{F}_2}(\boldsymbol{e}_{n,3})$*, which is a* $2n$*-tuple of 0's and 1's, and an order of the elements of* $\mathbb{F}_2^{2n}$ *(different order, different representation). For instance,* $Tr_{\mathbb{F}_4/\mathbb{F}_2}(\boldsymbol{e}_{4,3})$ *can be identified with*

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

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

Example 3.3.14. *Consider the sequence* $\{S_{\mathbb{F}_8}(\boldsymbol{e}_{n,3})\}$. *Theorem 3.3.11 implies that this sequence satisfies the linear recurrence whose characteristic is given by*

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

The minimal linear recurrence with integer coefficients that $\{S_{\mathbb{F}_8}(\boldsymbol{e}_{n,3})\}$ *satisfies has characteristic polynomial given by*

$$\mu_{8,3}(X) = (X-4)(X+4)\left(X^2+16\right)\left(X^2-8X+32\right)\left(X^2-4X+8\right)\left(X^2+4X+8\right).$$

It can be verified that $\mu_{8,3}(X)|P_{8,3}(X)$. *The closed formula for this exponential sum is given (after simplification) by*

$$S_{\mathbb{F}_8}(\boldsymbol{e}_{n,3}) = \frac{1}{8}\left(2\sqrt{2}\right)^n\left((9+(-1)^n)\left(\sqrt{2}\right)^n + 2\left(2^n+9\right)\sin\left(\frac{n\pi}{4}\right) - 6\sin\left(\frac{3n\pi}{4}\right) - 6\left(\sqrt{2}\right)^n\cos\left(\frac{n\pi}{2}\right)\right).$$

As with the previous example, the function $Tr_{\mathbb{F}_8/\mathbb{F}_2}(\boldsymbol{e}_{n,3})$ *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 3.3.13. 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 3.3.15. *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 term $1/X$ in front of $P_{3,7}(X)$ comes from the fact that $P_{3,7}(0) = 0$, i.e., 0 is a root for $P_{3,7}(X)$. However, the root 0 does not contribute anything to the closed formula for the exponential sum. Therefore, taking the term X does not alter the result. Thus, the polynomial $P_{3,7}(X)$ is tight for this example.

The repetition of factors can be eliminated by using *least common multiples* (lcm).

Theorem 3.3.16. *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*

$$\chi_{q,k}(X) = \operatorname{lcm}\left(M_{a_1,\cdots,a_{q-1}}(X)\right)_{0 \leq a_{q-1} \leq \cdots \leq a_2 \leq a_1 \leq D-1}.$$

Remark 3.3.17. *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 3.3.11 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 3.3.11 together with Corollary 3.2.3 implies that

$$S_{\mathbb{F}_q}\left(\sum_{j=1}^{s} \beta_j \boldsymbol{e}_{n,k_j}\right) = \sum_{m_1=0}^{n} \sum_{m_2=0}^{n-m_1} \cdots \sum_{m_{q-1}=0}^{n-m_1-\cdots-m_{q-1}} \binom{n}{m_0^*, m_1, m_2, \cdots, m_{q-1}} \times \xi_p^{\operatorname{Tr}\left(\sum_{j=1}^{s} \beta_j F_{k,\mathbb{F}_q}^{(p)}(m_1,\cdots,m_{q-1})\right)}. \tag{3.94}$$

The statement of Theorem 3.3.11 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

$$\mathrm{Tr}\left(F^{(p)}_{k;\mathbb{F}_q}(b_1,\cdots,b_{q-1})\right)$$

in the definition of $c_{j_1,\cdots,j_{q-1}}(k)$ must be replaced by

$$\mathrm{Tr}\left(\sum_{j=1}^{s}\beta_j F^{(p)}_{k_j;\mathbb{F}_q}(b_1,\cdots,b_{q-1})\right).$$

Similar adjustments apply to the other results.

3.4 Concluding remarks

We expressed exponential sums of linear combinations of elementary symmetric polynomials over finite fields as multinomial sums. These expressions represent a computational improvement over the definition of exponential sums. These expressions also provided a link between balancedness of symmetric polynomials over Galois fields and a problem similar to the one of bisecting binomial coefficients. We also proved closed formulas for exponential sums of linear combinations of elementary symmetric polynomials over Galois fields by exploiting their multinomial sum representations. These closed formulas extend the work of Cai, Green and Thierauf on the binary field to every finite field. Our closed formulas also provide a faster way to compute the value of the exponential sums considered, hence we can understand better the behavior of these exponential sums over Galois field. Moreover, we showed that the recursive nature of these exponential sums is not special to the binary case and provide explicit linear recurrences the they satisfy. We hope our results can be used to find families of symmetric functions with desired cryptographic properties over finite fields.

REFERENCE LIST

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

[20] 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.

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

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

[23] 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.

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

[25] 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.

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

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

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

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

[30] 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.

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

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

[33] 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.

[34] 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.

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

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

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

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

[39] 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.