CLOSED FORMULAS FOR EXPONENTIAL SUMS OF SYMMETRIC POLYNOMIALS OVER GALOIS FIELDS

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

Abstract. Exponential sums have applications to a variety of scientific fields, including, but not limited to, cryptography, coding theory and information theory. Closed formulas for exponential sums of symmetric Boolean functions were found by Cai, Green and Thierauf in the late 1990's. Their closed formulas imply that these exponential sums are linear recursive. The linear recursivity of these sums has been exploited in numerous papers and has been used to compute the asymptotic behavior of such sequences. In this article, we extend the result of Cai, Green and Thierauf, that is, we find closed formulas for exponential sums of symmetric polynomials over any Galois fields. Our result also implies that the recursive nature of these sequences is not unique to the binary field, as they are also linear recursive over any finite field. In fact, we provide explicit linear recurrences with integer coefficients for such sequences. As a byproduct of our results, we discover a link between exponential sums of symmetric polynomials over Galois fields and a problem for multinomial coefficients which similar to the problem of bisecting binomial coefficients.

1. Introduction

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

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

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 [2, 6, 7, 8, 10, 11, 12].

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 [2]. Moreover, their formulas imply that exponential sums of symmetric Boolean functions have a recursive nature. This has been exploited in [5, 6, 7, 8, 11]. In the particular case of [6], 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 [12].

Many cryptographic properties, like correlation immune functions, resilient functions and bent functions have been extended to other finite fields [13, 15, 17, 18, 19, 20]. 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 [10], it has been shown that exponential sums of linear combinations of elementary symmetric polynomials over Galois fields

Date: August 28, 2018.

2010 *Mathematics Subject Classification.* 05E05, 11T23, 11B37.

Key words and phrases. Exponential sums, symmetric functions, linear recurrences.

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 [10] 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 paper 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 [2] 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 $(\delta_0, \delta_1, \dots, \delta_n)$ to the equation

$$\sum_{j=0}^{n} \delta_j \binom{n}{j} = 0, \;\; \delta_j \in \{-1, 1\}, \tag{1.2}$$

is said to give a *bisection of the binomial coefficients* $\binom{n}{j}$, $0 \leq j \leq n$. Observe that a solution to (1.2) provides us with two disjoints sets A, B such that $A \cup B = \{0, 1, 2, \dots, n\}$ and

$$\sum_{j \in A} \binom{n}{j} = \sum_{j \in B} \binom{n}{j} = 2^{n-1}. \tag{1.3}$$

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 we provide multinomial sum expressions for exponential sums of symmetric polynomials over Galois fields. These multinomial sums representations are a computational improvement over the formal definition of exponential sums.

Section 4 is the core section of the article. It is in this section where we generalized Cai et. al's result [2] by proving closed formulas for exponential sums of elementary symmetric polynomials over any Galois field. Finally, in the last section, we present some consequences of our results. In particular, we provide a connection to a problem similar to the problem of bisecting binomial coefficients and provide explicit linear recurrences for exponential sums of linear combinations of elementary symmetric polynomials over finite fields.

2. 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

$$F(\mathbf{X}) = \boldsymbol{e}_{n,k_1} \oplus \boldsymbol{e}_{n,k_2} \oplus \cdots \oplus \boldsymbol{e}_{n,k_s}, \tag{2.1}$$

where $0 \leq k_1 < k_2 < \cdots < k_s$ are integers. For the sake of simplicity, the notation $\boldsymbol{e}_{n,[k_1,\dots,k_s]}$ is used to denote (2.1). For example,

$$\begin{aligned} \boldsymbol{e}_{3,[2,1]} &= \boldsymbol{e}_{3,2} \oplus \boldsymbol{e}_{3,1} \\ &= X_1X_2 \oplus X_3X_2 \oplus X_1X_3 \oplus X_1 \oplus X_2 \oplus X_3. \end{aligned} \tag{2.2}$$

As mentioned in the introduction, it is known that exponential sums of symmetric Boolean functions are linear recursive [2, 6]. Moreover, closed formulas for them are well known. In fact, Cai et al. [2] proved the following theorem.

Theorem 2.1 ([2]). *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 $S(\boldsymbol{e}_{n,[k_1,\ldots,k_s]})$ is given by*

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

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

$$c_j(k_1,\ldots,k_s) = \frac{1}{2^r}\sum_{t=0}^{2^r-1}(-1)^{\binom{t}{k_1}+\cdots+\binom{t}{k_s}}\zeta_j^{-t}. \tag{2.3}$$

Theorem 2.1 and a closed formula for $c_0(k)$ (proved in [6]) were used by Castro and Medina [6] to prove asymptotically a conjecture of Cusick, Li and Stănică about the balancedness of elementary symmetric polynomials [12]. An adaptation of Theorem 2.1 to perturbations of symmetric Boolean functions (see [7]) was recently used in [5] to prove a generalized conjecture of Canteaut and Videau [3] 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 exist when the number of variables grows. The original conjecture was proved by Guo, Gao and Zhao [14]. The same behavior holds true for perturbations of symmetric Boolean functions.

One of the goals of this article is to generalize Theorem 2.1 to the general setting of Galois fields. Let p be a prime and $q = p^l$ with l a positive integer. If $F : \mathbb{F}_q^n \to \mathbb{F}_q$, then its *exponential sum over* $\mathbb{F}_q$ is given by

$$S_{\mathbb{F}_q}(F) = \sum_{\mathbf{x}\in\mathbb{F}_q^n} e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(F(\mathbf{x}))}, \tag{2.4}$$

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

$$\mathrm{Tr}_{\mathbb{F}_{p^l}/\mathbb{F}_p}(\alpha) = \sum_{j=0}^{l-1}\alpha^{p^j}, \tag{2.5}$$

with arithmetic done in $\mathbb{F}_{p^l}$. Recently in [10], 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 [10], 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 2.1, 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 [1].

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

$$S(\boldsymbol{e}_{n,[k_1,\ldots,k_s]}) = \sum_{j=0}^{n}(-1)^{\binom{j}{k_1}+\cdots+\binom{j}{k_s}}\binom{n}{j}. \tag{2.6}$$

Equation (2.6) is a clear computational improvement over (1.1). 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 [21]). As mentioned in the introduction, a solution $(\delta_0, \delta_1, \ldots, \delta_n)$ to the equation

$$\sum_{j=0}^{n}\delta_j\binom{n}{j} = 0, \;\; \delta_j \in \{-1, 1\}, \tag{2.7}$$

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 [16, 21].

In the next section, we prove a formula similar to (2.6) 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 include it here for completeness.

Theorem 2.2 (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 $j = 1, \ldots, l$. 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

$$\binom{n+D}{k} \equiv \binom{n}{k} \mod p. \tag{2.8}$$

This will be used throughout the rest of the paper.

3. 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 (2.4). 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

$$\Lambda_{a_1}(k, m) = a_1^k \binom{m}{k} \tag{3.1}$$

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

$$\Lambda_{a_1,a_2,\ldots,a_{l+1}}(k, m_1, m_2, \ldots, m_{l+1}) = \sum_{j=0}^{m_{l+1}} \binom{m_{l+1}}{j} a_{l+1}^j \Lambda_{a_1,\ldots,a_l}(k-j, m_1, m_2, \ldots, m_l), \tag{3.2}$$

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

Lemma 3.1. *Let n and k be positive integers. Let $A_l = \{0, a_1, \ldots, a_l\}$ and $\mathbf{x} \in A_l^n$. Suppose that a_j appears m_j times in $\mathbf{x}$. Then,*

$$\boldsymbol{e}_{n,k}(\mathbf{x}) = \Lambda_{a_1,\ldots,a_l}(k, m_1, \ldots, m_l). \tag{3.3}$$

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

$$\boldsymbol{e}_{n,k}(\mathbf{x}) = a_1^k \binom{m_1}{k}. \tag{3.4}$$

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

$$\boldsymbol{e}_{n,k}(X_1, \ldots, X_{n-r}, \alpha, \ldots, \alpha) = \sum_{j=0}^{r} \binom{r}{j} \alpha^j \boldsymbol{e}_{n-r,k-j}(X_1, \ldots, X_{n-r}). \tag{3.5}$$

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 multinomial coefficients.

Theorem 3.2. *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 $\mathbb{F}_q = \{0, \alpha_1, \ldots, \alpha_{q-1}\}$ is the Galois field of q elements. Then,*

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

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

$$\binom{n}{m_1}\binom{n-m_1}{m_2}\binom{n-m_1-m_2}{m_3}\cdots\binom{n-m_1-m_2-\cdots-m_{q-2}}{m_{q-1}} \tag{3.6}$$

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

$$\binom{n}{m_0^*, m_1, m_2, \ldots, m_{q-1}}. \tag{3.7}$$

Observe that Lemma 3.1 implies that the value of $\boldsymbol{e}_{n,k}$ on each of these tuples is

$$\boldsymbol{e}_{n,k}(\mathbf{x}) = \Lambda_{\alpha_1,\ldots,\alpha_{q-1}}(k, m_1, \ldots, m_{q-1}). \tag{3.8}$$

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

An easy adjustment to the proof of Theorem 3.2 leads the following.

Corollary 3.3. *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 $\mathbb{F}_q = \{0, \alpha_1, \ldots, \alpha_{q-1}\}$ 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,

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

Proof. The proof follows the same argument as in Theorem 3.2. □

For small q, Theorem 3.2 and the recursive nature of $\Lambda_{a_1,\ldots,a_l}$ 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 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

$$S_{\mathbb{F}_3}(\boldsymbol{e}_{12,5}) = 346113 + 92664e^{\frac{2i\pi}{3}} + 92664e^{-\frac{2i\pi}{3}} = 253449. \tag{3.9}$$

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

$$S_{\mathbb{F}_3}(\boldsymbol{e}_{100,7}) = 1139350908359508007398648345639492914165146429 41, \tag{3.10}$$

and 41.28 seconds to calculate

$$S_{\mathbb{F}_4}(\boldsymbol{e}_{50,5}) = 158735097466874432874732322816. \tag{3.11}$$

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.

In the next section, we use these multi-sum representation to prove closed formulas for exponential sums of symmetric polynomials over Galois fields. The formulas are a generalization of the work of Cai, Green and Thierauf [2].

4. Closed formulas for exponential sums of symmetric polynomials

In this section we generalize Theorem 2.1, that is, we provide closed formulas for the exponential sums considered in this article. Our formulas depend on circulant matrices and on periodicity. Thus, we start with a short background on these topics.

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

$$\operatorname{circ}(\alpha) := \begin{pmatrix} c_0 & c_1 & \ldots & c_{D-2} & c_{D-1} \\ c_{D-1} & c_0 & \ldots & c_{D-3} & c_{D-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_2 & c_3 & \ldots & c_0 & c_1 \\ c_1 & c_2 & \ldots & c_{D-1} & c_0 \end{pmatrix}. \tag{4.1}$$

The polynomial $p_\alpha(X) = c_0 + c_1X + \cdots + c_{D-1}X^{D-1}$ is called the *associated polynomial* of the circulant matrix. In the literature, this polynomial is also called *representer polynomial.* Observe that if

$$\pi = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix}, \tag{4.2}$$

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 $\operatorname{circ}(\alpha)$ are given by

$$v_j = \frac{1}{\sqrt{D}}(1, \omega_j, \omega_j^2, \ldots, \omega_j^{D-1})^T, \tag{4.3}$$

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

$$\lambda_j(\alpha) = p_\alpha(\omega_j) = c_0 + c_1\omega_j + c_2\omega_j^2 + \cdots + c_{D-1}\omega_j^{D-1}. \tag{4.4}$$

Moreover, any circulant matrix $\operatorname{circ}(\alpha)$ can be diagonalized in the following form. Consider the *Discrete Fourier Transform* matrix

$$F_n = \begin{pmatrix} \xi_n^{0\cdot 0} & \xi_n^{0\cdot 1} & \ldots & \xi_n^{0\cdot(n-1)} \\ \xi_n^{1\cdot 0} & \xi_n^{1\cdot 1} & \ldots & \xi_n^{1\cdot(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \xi_n^{(n-1)\cdot 0} & \xi_n^{(n-1)\cdot 1} & \ldots & \xi_n^{(n-1)\cdot(n-1)} \end{pmatrix}, \tag{4.5}$$

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

$$\Delta(\alpha) = \operatorname{diag}(\lambda_0(\alpha), \lambda_1(\alpha), \ldots, \lambda_{D-1}(\alpha)). \tag{4.6}$$

Then,

$$\operatorname{circ}(\alpha) = U_D\Delta(\alpha)U_D^*. \tag{4.7}$$

See [4, Th.3.2.2, p. 72] for more information.

***Remark* 4.1.** The Discrete Fourier Transform (DFT) is usually defined as the conjugate of the matrix F_n. We defined the DFT as F_n in order to preseve the indices of $\lambda_j(\alpha)$'s in later arguments.

A function $f : \mathbb{Z} \to \mathbb{Z}$ is said to be *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

$$g(j_1 + D_1, j_2) = g(j_1, j_2) \tag{4.8}$$

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

$$g(j_1, j_2 + D_2) = g(j_1, j_2) \tag{4.9}$$

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, $D = \text{lcm}(D_1, D_2)$ is such that

$$g(j_1 + D, j_2 + D) = g(j_1, j_2) \tag{4.10}$$

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

$$\sum_{l=0}^{n} a^l \binom{n}{l}. \tag{4.11}$$

Later it will become clear why we choose this sum. Given a positive integer $D > 1$, the sum (4.11) can be splitted as

$$\sum_{l=0}^{n} a^l \binom{n}{l} = \sum_{t=0}^{D-1} r_t(n; a), \tag{4.12}$$

where

$$r_t(n; a) = \sum_{j \equiv t \bmod D} a^j \binom{n}{j}. \tag{4.13}$$

The next result provides closed formulas for $r_t(n; a)$, and therefore, for (4.11).

Proposition 4.2. *Let $n \in \mathbb{N}$ and $0 \le t \le D-1$. Then,*

$$r_t(n; a) = \frac{1}{D} \sum_{m=0}^{D-1} \xi_D^{tm} \lambda_m^n, \tag{4.14}$$

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

Proof. The approach of this proof is similar to the one presented in [2]. Note that for $1 \le t \le D-1$, we have

$$r_t(n; a) = r_t(n-1; a) + a\, r_{t-1}(n-1; a). \tag{4.15}$$

Also,

$$r_0(n; a) = r_0(n-1; a) + a\, r_{D-1}(n-1; a). \tag{4.16}$$

Therefore, if we define

$$\boldsymbol{r}(n; a) = \begin{pmatrix} r_0(n; a) \\ r_1(n; a) \\ \vdots \\ r_{D-1}(n; a) \end{pmatrix}, \tag{4.17}$$

then

$$\boldsymbol{r}(n; a) \quad = \quad \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & a \\ a & 1 & 0 & \ldots & 0 & 0 \\ 0 & a & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & a & 1 \end{pmatrix} \boldsymbol{r}(n-1; a). \tag{4.18}$$

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

$$\boldsymbol{r}(n; a) = A_D(a)\boldsymbol{r}(n-1; a), \tag{4.19}$$

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

Iteration of (4.19) leads to $\boldsymbol{r}(n; a) = A_D(a)^n \boldsymbol{r}(0; a)$. Observe that

$$r_0(0; a) = \binom{0}{0} = 1 \quad \text{and} \quad r_t(0; a) = 0 \text{ for } t > 0. \tag{4.20}$$

Thus,

$$\boldsymbol{r}(0; a) = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{4.21}$$

Equation (4.7) now implies that

$$\begin{aligned} \boldsymbol{r}(n; a) &= U_D \Delta(\alpha)^n U_D^* \cdot \boldsymbol{r}(0; a) = \frac{1}{D} F_D \Delta(\alpha)^n F_D^* \cdot \boldsymbol{r}(0; a) = \frac{1}{D} F_D \Delta(\alpha)^n \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \\ &= \frac{1}{D} F_D \begin{pmatrix} \lambda_0(\alpha)^n \\ \lambda_1(\alpha)^n \\ \vdots \\ \lambda_{D-1}(\alpha)^n \end{pmatrix} = \begin{pmatrix} \frac{1}{D}\sum_{j=0}^{D-1} \xi_D^{0\cdot j} \lambda_j(\alpha)^n \\ \frac{1}{D}\sum_{j=0}^{D-1} \xi_D^{1\cdot j} \lambda_j(\alpha)^n \\ \vdots \\ \frac{1}{D}\sum_{j=0}^{D-1} \xi_D^{(D-1)j} \lambda_j(\alpha)^n \end{pmatrix}. \end{aligned} \tag{4.22}$$

It follows that

$$r_t(n; a) = \frac{1}{D} \sum_{j=0}^{D-1} \xi_D^{tj} \lambda_j(\alpha)^n \tag{4.23}$$

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

The following results are easy consequences of the above proposition.

Corollary 4.3. *Let F be a periodic function with period D. Suppose that $\xi^D = 1$ (not necessarily primitive). Then,*

$$\sum_{l=0}^{n} \binom{n}{l} a^l \xi^{F(l)} = \frac{1}{D} \sum_{t=0}^{D-1} \xi^{F(t)} \sum_{j=0}^{D-1} \xi_D^{tj} \lambda_j^n, \tag{4.24}$$

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

Proof. Observe that

$$\begin{aligned} \sum_{l=0}^{n} \binom{n}{l} a^l \xi^{F(l)} &= \sum_{t=0}^{D-1} \left(\sum_{j \equiv t \bmod D} \xi^{F(t)} a^l \binom{n}{j} \right) \\ &= \sum_{t=0}^{D-1} \xi^{F(t)} r_t(n; a). \end{aligned} \tag{4.25}$$

The result now follows from Proposition 4.2. □

Corollary 4.4. *Let F be a periodic function with period D. Suppose that $\xi^D = 1$ (not necessarily primitive). Then,*

$$\sum_{l=0}^{n} \binom{n}{l} \xi^{F(l)} = \frac{1}{D} \sum_{t=0}^{D-1} \xi^{F(t)} \sum_{j=0}^{D-1} \xi_D^{tj} \left(1 + \xi_D^{-j}\right)^n, \tag{4.26}$$

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

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

Proposition 4.2 and its corollaries can be extended further to obtain closed formulas for multinomial sums. Before we present such an extension, we introduce the concept of a rearrangement of a list. By a *rearrangement* of $(t_1, \dots, t_r)$ we mean a permutation of the symbols in $(t_1, \dots, t_r)$. For example, the set of all different rearrangements of $(2, 2, 1, 1)$ 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 $\mathrm{Sym}(t_1, \dots, t_r)$ to denote the set of all rearrangements of $(t_1, \dots, t_r)$. The next result is an extension of Proposition 4.7.

Theorem 4.5. *Let $F(q_1, \dots, q_r)$ 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,*

$$S(n) = \sum_{q_1=0}^{n} \sum_{q_2=0}^{n-q_1} \cdots \sum_{q_r=0}^{n-q_1-\cdots-q_{r-1}} \binom{n}{q_1} \binom{n-q_1}{q_2} \cdots \binom{n-q_1-\cdots-q_{r-1}}{q_r} \xi^{F(q_1,\dots,q_r)}. \tag{4.27}$$

Then,

$$S(n) = \sum_{j_1=0}^{D-1} \sum_{j_2=0}^{j_1} \cdots \sum_{j_r=0}^{j_{r-1}} c_{j_1,\dots,j_r}(D) \left(1 + \xi_D^{-j_1} + \cdots + \xi_D^{-j_r}\right)^n, \tag{4.28}$$

where

$$c_{j_1,\dots,j_r}(D) = \frac{1}{D^r} \sum_{b_r=0}^{D-1} \sum_{b_{r-1}=0}^{D-1} \cdots \sum_{b_1=0}^{D-1} \xi^{F(b_1,\dots,b_r)} \sum_{(j_1',\dots,j_r') \in \mathrm{Sym}(j_1,\dots,j_r)} \xi_D^{j_1' b_r + \cdots + j_r' b_1}, \tag{4.29}$$

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

Proof. We present the core of proof for $r = 3$. We decided to do this in order to simplify the writing of the proof.

Write $S(n)$ as

$$S(n) = \sum_{q_1=0}^{n} \sum_{q_2=0}^{n-q_1} \binom{n}{q_1} \binom{n-q_1}{q_2} \sum_{q_3=0}^{n-q_1-q_2} \binom{n-q_1-q_2}{q_3} \xi^{F(q_1,q_2,q_3)}. \tag{4.30}$$

Apply Corollary 4.4 to the last sum to get

$$S(n) = \sum_{q_1=0}^{n} \sum_{q_2=0}^{n-q_1} \binom{n}{q_1} \binom{n-q_1}{q_2} \left(\frac{1}{D} \sum_{b_3=0}^{D-1} \xi^{F(q_1,q_2,b_3)} \sum_{j_1=0}^{D-1} \xi_D^{j_1 b_3} \lambda_{j_1}^{n-q_1-q_2} \right), \tag{4.31}$$

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

$$S(n) = \frac{1}{D} \sum_{b_3=0}^{D-1} \sum_{j_1=0}^{D-1} \xi_D^{j_1 b_3} \sum_{q_1=0}^{n} \binom{n}{q_1} \lambda_{j_1}^{n-q_1} \sum_{q_2=0}^{n-q_1} \binom{n-q_1}{q_2} (\lambda_{j_1}^{-1})^{q_2} \xi^{F(q_1,q_2,b_3)}. \tag{4.32}$$

Now apply Corollary 4.3 to the last sum to get

$$S(n) = \frac{1}{D} \sum_{b_3=0}^{D-1} \sum_{j_1=0}^{D-1} \xi_D^{j_1 b_3} \sum_{q_1=0}^{n} \binom{n}{q_1} \lambda_{j_1}^{n-q_1} \left(\frac{1}{D} \sum_{b_2=0}^{D-1} \xi^{F(q_1,b_2,b_3)} \sum_{j_2=0}^{D-1} \xi_D^{j_2 b_2} \right) (1 + \lambda_{j_1}^{-1} \xi_D^{-j_2})^{n-q_1}. \tag{4.33}$$

Moreover, 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,

$$S(n) = \frac{1}{D}\sum_{b_3=0}^{D-1}\sum_{j_1=0}^{D-1}\xi_D^{j_1b_3}\sum_{q_1=0}^{n}\binom{n}{q_1}\left(\frac{1}{D}\sum_{b_2=0}^{D-1}\xi^{F(q_1,b_2,b_3)}\sum_{j_2=0}^{D-1}\xi_D^{j_2b_2}\right)\lambda_{j_1,j_2}^{n-q_1}. \tag{4.34}$$

Rearrange terms to get

$$S(n) = \frac{1}{D^2}\sum_{b_3=0}^{D-1}\sum_{b_2=0}^{D-1}\sum_{j_1=0}^{D-1}\sum_{j_2=0}^{D-1}\xi_D^{j_1b_3+j_2b_2}\lambda_{j_1,j_2}^{n}\sum_{q_1=0}^{n}\binom{n}{q_1}\xi^{F(q_1,b_2,b_3)}\xi_D^{j_2b_2}(\lambda_{j_1,j_2}^{-1})^{q_1}. \tag{4.35}$$

Apply Corollary 4.3 once again. After simplification, we have

$$S(n) = \frac{1}{D^3}\sum_{b_3=0}^{D-1}\sum_{b_2=0}^{D-1}\sum_{b_1=0}^{D-1}\sum_{j_1=0}^{D-1}\sum_{j_2=0}^{D-1}\sum_{j_3=0}^{D-1}\xi_D^{j_1b_3+j_2b_2+j_3b_1}\xi^{F(b_1,b_2,b_3)}\lambda_{j_1,j_2,j_3}^{n}. \tag{4.36}$$

In general, the same argument can be repeated multiple times to get

$$S(n) = \frac{1}{D^r}\sum_{b_r=0}^{D-1}\sum_{b_{r-1}=0}^{D-1}\cdots\sum_{b_1=0}^{D-1}\sum_{j_1=0}^{D-1}\sum_{j_2=0}^{D-1}\cdots\sum_{j_r=0}^{D-1}\xi^{F(b_1,\ldots,b_r)}\xi_D^{j_1b_r+\cdots+j_rb_1}\lambda_{j_1,\ldots,j_r}^{n}, \tag{4.37}$$

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

Observe that equation (4.37) can be written as

$$S(n) = \sum_{j_1=0}^{D-1}\sum_{j_2=0}^{D-1}\cdots\sum_{j_r=0}^{D-1}d_{j_1,\ldots,j_r}(D)\lambda_{j_1,\ldots,j_r}^{n}, \tag{4.38}$$

where

$$d_{j_1,\ldots,j_r}(D) = \frac{1}{D^r}\sum_{b_r=0}^{D-1}\sum_{b_{r-1}=0}^{D-1}\cdots\sum_{b_1=0}^{D-1}\xi^{F(b_1,\ldots,b_r)}\xi_D^{j_1b_r+\cdots+j_rb_1}. \tag{4.39}$$

However, note that $\lambda_{t_1,\ldots,t_r} = \lambda_{t_1',\ldots,t_r'}$ where $(t_1',\ldots,t_r')$ is any rearrangement of $(t_1,\ldots,t_r)$. That means that the coefficient of $\lambda_{t_1,\ldots,t_r}^{n}$ in (4.37) is the sum of all $d_{t_1',\ldots,t_r'}(D)$ where $(t_1',\ldots,t_r')$ is a rearrangement of $(t_1,\ldots,t_r)$. Collecting all these terms yield the result. This concludes the proof. □

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 $\mathbb{F}_q = \{0,\alpha_1,\ldots,\alpha_{q-1}\}$. Theorem 3.2 implies that

$$S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k}) = \sum_{m_1=0}^{n}\sum_{m_2=0}^{n-m_1}\cdots\sum_{m_{q-1}=0}^{n-m_1-\cdots-m_{q-2}}\binom{n}{m_0^*,m_1,m_2,\ldots,m_{q-1}}\xi_p^{\mathrm{Tr}\left(\Lambda_{\alpha_1,\ldots,\alpha_{q-1}}(k,m_1,\ldots,m_{q-1})\right)} \tag{4.40}$$

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

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

Therefore, if we let

$$F_{k;\mathbb{F}_q}(m_1,\ldots,m_{q-1}) = \Lambda_{\alpha_1,\ldots,\alpha_{q-1}}(k,m_1,\ldots,m_{q-1}), \tag{4.41}$$

then

$$S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k}) = \sum_{m_1=0}^{n}\sum_{m_2=0}^{n-m_1}\cdots\sum_{m_{q-1}=0}^{n-m_1-\cdots-m_{q-2}}\binom{n}{m_0^*,m_1,m_2,\ldots,m_{q-1}}\xi_p^{\mathrm{Tr}\left(F_{k,\mathbb{F}_q}(m_1,\ldots,m_{q-1})\right)} \tag{4.42}$$

is of the same type as (4.27). It remains to show the periodicity of $F_{k;\mathbb{F}_q}$.

Unfortunately, the function $F_{k;\mathbb{F}_q}$, as defined, is not fully periodic. However, the problem can be circumvented by defining a periodic function that coincides with $\Lambda_{a_1,\ldots,a_l}(k,m_1,\ldots,m_l)$ when $m_1,\ldots,m_l$ are all non-negative.

Lemma 4.6. *Let p be prime and $a_1, \ldots, a_l$ be some elements in some field extension of $\mathbb{F}_p$. Define*

$$\Lambda^{(p)}_{a_1,\ldots,a_l}(k, m_1, \ldots, m_l) := \Lambda_{a_1,\ldots,a_l}(k, m_1^+, \ldots, m_l^+) \mod p, \tag{4.43}$$

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

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

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

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

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

$$\Lambda_{a_1}(k, m_1) = a^k \binom{m_1}{k}. \tag{4.44}$$

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

$$\binom{m_1 + D}{k'} \equiv \binom{m_1}{k'} \mod p, \tag{4.45}$$

for every $k' \leq k$. 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 $\Lambda_{a_1,\ldots,a_l,a_{l+1}}(k, m_1, \ldots, m_l, m_{l+1})$. Recall that

$$\Lambda_{a_1,\ldots,a_l,a_{l+1}}(k, m_1, \ldots, m_l, m_{l+1}) = \sum_{j=0}^{m_{l+1}} \binom{m_{l+1}}{j} a_{l+1}^j \Lambda_{a_1,\ldots,a_l}(k - j, m_1, \ldots, m_l). \tag{4.46}$$

It is clear that

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

holds for $j = 1, \ldots, l$ (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

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

Therefore, every term on the right-hand side of (4.46) for which $j > k$ is 0. This implies that the binomial coefficient that accompanies every surviving term in (4.46) satisfies (Lucas' Theorem)

$$\binom{m_{l+1} + D}{j} \equiv \binom{m_{l+1}}{j} \mod p. \tag{4.47}$$

Then,

$$\begin{aligned} \Lambda_{a_1,\ldots,a_l,a_{l+1}}(k, m_1, \ldots, m_l, m_{l+1} + D) &= \sum_{j=0}^{m_{l+1}+D} \binom{m_{l+1} + D}{j} a_{l+1}^j \Lambda_{a_1,\ldots,a_l}(k - j, m_1, \ldots, m_l) \\ &\equiv \sum_{j=0}^{m_{l+1}+D} \binom{m_{l+1}}{j} a_{l+1}^j \Lambda_{a_1,\ldots,a_l}(k - j, m_1, \ldots, m_l) \mod p \\ &\equiv \sum_{j=0}^{m_{l+1}} \binom{m_{l+1}}{j} a_{l+1}^j \Lambda_{a_1,\ldots,a_l}(k - j, m_1, \ldots, m_l) \mod p \\ &\equiv \Lambda_{a_1,\ldots,a_{l+1}}(k, m_1, \ldots, m_{l+1}) \mod p. \end{aligned} \tag{4.48}$$

Therefore,

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

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

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

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

It is clear that

$$\Lambda_{a_1,\dots,a_l}(k, m_1, \dots, m_j + tD, \dots, m_l) \equiv \Lambda_{a_1,\dots,a_l}(k, m_1, \dots, m_j, \dots, m_l) \mod p \tag{4.49}$$

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 $\Lambda_{a_1,\dots,a_l}$ one has that $\Lambda_{a_1,\dots,a_l}(k, m_1, \dots, m_l) = 0$. However, this can be circumvented by defining the function

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

where

$$m_j^+ = \begin{cases} m_j, & \text{if } m_j > 0 \\ m_j + \left(\left\lfloor \frac{-m_j}{D} \right\rfloor + 1 \right) D, & \text{if } m_j \leq 0. \end{cases} \tag{4.50}$$

Observe that

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

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

Let us go back to formula (4.42) for $S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})$. Note that the value of $\xi_p^{\mathrm{Tr}(F_{k;\mathbb{F}_q}(m_1,\dots,m_{q-1}))}$ depends only on the value of $F_{k;\mathbb{F}_q}(m_1, \dots, m_l) \mod p$. Therefore, if we define

$$F^{(p)}_{k;\mathbb{F}_q}(m_1, \dots, m_{q-1}) := \Lambda^{(p)}_{\alpha_1,\dots,\alpha_{q-1}}(k, m_1, \dots, m_{q-1}), \tag{4.51}$$

then

$$S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k}) = \sum_{m_1=0}^{n} \sum_{m_2=0}^{n-m_1} \cdots \sum_{m_{q-1}=0}^{n-m_1-\cdots-m_{q-2}} \binom{n}{m_0^*, m_1, m_2, \dots, m_{q-1}} \xi_p^{\mathrm{Tr}\left(F^{(p)}_{k,\mathbb{F}_q}(m_1,\dots,m_{q-1})\right)}. \tag{4.52}$$

We now present the main result of the article, i.e. our closed formulas for $S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})$. This generalizes Cai, Green and Thierauf's result for the binary case [2] to any finite field.

Theorem 4.7. *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,*

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

where

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

$\xi_D = \exp(2\pi i/D)$, $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$, *and* $\lambda_{j_1,\dots,j_{q-1}} = 1 + \xi_D^{-j_1} + \xi_D^{-j_2} + \cdots + \xi_D^{-j_{q-1}}$.

Proof. The sum in (4.52) is of type (4.27). Moreover, Lemma 4.6 implies that $F^{(p)}_{n,k;\mathbb{F}_q}(m_1, \dots, m_{q-1})$ is periodic in each component with period D.

□

We point out that Theorem 4.7 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 $\beta_1, \dots, \beta_s \in \mathbb{F}_q^\times$. The discussion prior Theorem 4.7 together with Corollary 3.3 implies that

$$S_{\mathbb{F}_q}\left(\sum_{j=1}^{s} \beta_j \boldsymbol{e}_{n,k_j}\right) = \sum_{m_1=0}^{n} \sum_{m_2=0}^{n-m_1} \cdots \sum_{m_{q-1}=0}^{n-m_1-\cdots-m_{q-2}} \binom{n}{m_0^*, m_1, m_2, \dots, m_{q-1}} \times \xi_p^{\mathrm{Tr}\left(\sum_{j=1}^{s} \beta_j F^{(p)}_{k,\mathbb{F}_q}(m_1,\dots,m_{q-1})\right)}. \tag{4.53}$$

The statement of Theorem 4.7 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

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

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

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

Similar adjustments can be applied to the other results. In the next section, we presents some consequences of our results.

5. Some consequences and examples

The closed formulas presented in this articles have some nice consequences. In this section, we present some of them.

5.1. **Multisection of multinomial coefficients.** Theorem 3.2 and Corollary 3.3 offer a hint to a problem similar to bisections of binomial coefficients for multinomial coefficients. Let p be a prime. Emulating the binary case, we define (p,q)-*multisection* of multinomial coefficients (q being a power of p) to be the process of dividing the list

$$\mathcal{L}(n;q) = \left\{\binom{n}{m_0^*, m_1, m_2, \dots, m_{q-1}}\right\}, \tag{5.1}$$

where $m_0^* = n - (m_1 + \cdots + m_{q-1})$ and the indices run

$$0 \le m_1 \le n,\ 0 \le m_2 \le n - m_1,\ \dots,\ 0 \le m_{q-1} \le n - m_1 - m_2 - \cdots - m_{q-2},$$

into p sublists, $l_j(n;q), 1 \le j \le p$, such that the sum on each sublist is the same. This common sum must be q^{n-1}.

Observe that Theorem 3.2 and Corollary 3.3 imply 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)-multisection of multinomial coefficients. This connection generalizes the one that exists between bisections of binomial coefficients and symmetric Boolean functions.

Example 5.1. The elementary symmetric polynomial $\boldsymbol{e}_{5,3}$ is such that $S_{\mathbb{F}_3}(\boldsymbol{e}_{5,3}) = 0$. Observe that

$$\mathcal{L}(5;3) = \{1,5,10,10,5,1,5,20,30,20,5,10,30,30,10,10,20,10,5,5,1\}. \tag{5.2}$$

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

$$\begin{aligned} l_1(5;3) &= \{1,5,5,10,10,20,30\}\\ l_2(5;3) &= \{1,5,5,10,10,20,30\}\\ l_3(5;3) &= \{1,5,5,10,10,20,30\}. \end{aligned} \tag{5.3}$$

Example 5.2. The symmetric polynomial $\boldsymbol{e}_{6,5} + \boldsymbol{e}_{6,3}$ satisfies $S_{\mathbb{F}_3}(\boldsymbol{e}_{6,5} + \boldsymbol{e}_{6,3}) = 0$. In this case,

$$\mathcal{L}(6;3) = \{1,6,15,20,15,6,1,6,30,60,60,30,6,15,60,90,60,15,20,60,60,20,15,30,15,6,6,1\}. \tag{5.4}$$

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

$$\begin{aligned} l_1(6;3) &= \{1,6,6,15,15,20,30,30,30,90\}\\ l_2(6;3) &= \{1,6,6,15,15,20,60,60,60\}\\ l_3(6;3) &= \{1,6,6,15,15,20,60,60,60\}. \end{aligned} \tag{5.5}$$

As in the Boolean case, we may try to define trivial (p,q)-multisections. A possible way to do this is to say that a (p,q)-multisection 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)-multisection is trivial. For example, $\boldsymbol{e}_{5,3}$ is trivially balanced, but $\boldsymbol{e}_{6,5} + \boldsymbol{e}_{6,3}$ is not. It would be interesting to know if some results known for the binary case also apply to this problem.

5.2. **A Diophantine equation.** Theorem 3.2 and its corollary can be written in terms of partitions of n. We say that $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_r)$ is a *partition* of n, and write $\boldsymbol{\lambda} \dashv n$, if the λ_j are integers and

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

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 $\boldsymbol{\lambda}$. Similar to the previous section, 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 and Corollary 3.3 can be re-stated as follows.

Theorem 5.3. *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 $\mathbb{F}_q = \{0, \alpha_1, \dots, \alpha_{q-1}\}$ is the Galois field of q elements. Then,*

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

Corollary 5.4. *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 $\mathbb{F}_q = \{0, \alpha_1, \dots, \alpha_{q-1}\}$ 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,

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

Exponential sums of linear combinations of elementary symmetric polynomials are also linked, via Theorem 5.3 and Corollary 5.4, to the Diophantine equation

$$\sum_{\boldsymbol{\lambda} \dashv_q n} \binom{n}{\boldsymbol{\lambda}} x_{\boldsymbol{\lambda}} = 0. \tag{5.6}$$

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 (5.6). Here is an example.

Example 5.5. 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

$$S_{\mathbb{F}_4}\left((1+\alpha)\boldsymbol{e}_{8,3} + (1+\alpha)\boldsymbol{e}_{8,2} + \alpha \boldsymbol{e}_{8,1}\right) = 0. \tag{5.7}$$

Therefore, we have a solution to (5.6) 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 (5.6) provided by (5.7) is given by

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

In other words,

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

***Remark* 5.6.** A natural problem to explore is to see how solutions to (5.6) given by exponential sums of linear combinations of elementary symmetric polynomials look like as n grows. Perhaps something similar to the study presented in [5] holds true in this case. This is part of future research.

5.3. **Linear recurrences.** The closed formulas presented in Theorem 4.7 imply that exponential sums over Galois fields of linear combinations of elementary symmetric polynomials satisfy homogeneous linear recurrences with integer coefficients. Moreover, we can provide explicit recurrences that are generalizations of the ones exploited for the binary case in [5, 6, 7, 8, 9].

A sequence $\{x_n\}$ is said to satisfy a *homogenous linear recurrence with constant coefficients* of order ℓ if there exist constants $c_1, \ldots, c_\ell$ such that

$$x_n = c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_\ell x_{n-\ell}. \tag{5.8}$$

The polynomial $P(X) = X^\ell - c_1 X^{\ell-1} - c_2 X^{\ell-2} - \cdots - c_{\ell-1} X - c_\ell$ is known as the *characteristic polynomial* of the recurrence (5.8). It is a well-established result in the theory of linear recurrences that solutions to (5.8) can be expressed in terms of the roots of its characteristic polynomial. Explicitly, if

$$P(X) = (X - \alpha_1)^{e_1} (X - \alpha_2)^{e_2} \cdots (X - \alpha_t)^{e_t}, \tag{5.9}$$

then every solution to (5.8) has the form

$$x_n = \sum_{j=1}^{t} p_j(n) \alpha_j^n, \tag{5.10}$$

where $p_j(X)$'s are polynomials and $\deg(p_j(X)) \leq e_j$. The opposite is also true, that is, if $\{x_n\}$ is defined by (5.10), then $\{x_n\}$ satisfies the linear recurrence whose characteristic polynomial is given by (5.9).

Let us go back to our exponential sums. Recall that Theorem 4.7 implies that

$$S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k}) = \sum_{j_1=0}^{D-1} \sum_{j_2=0}^{j_1} \cdots \sum_{j_{q-1}=0}^{j_{q-2}} c_{j_1,\ldots,j_{q-1}}(k) \left(1 + \xi_D^{-j_1} + \cdots + \xi_D^{-j_{q-1}}\right)^n, \tag{5.11}$$

where $c_{j_1,\ldots,j_{q-1}}(k)$ are constant and $D = p^{\lfloor \log_p(k) \rfloor + 1}$. A natural consequence of this formula and the above discussion is the linear recursivity of these exponential sums.

Theorem 5.7. *Let n and $k > 1$ be positive integers, p be a prime and $q = p^r$ with $r \geq 1$. Let $D = p^{\lfloor \log_p(k) \rfloor + 1}$. The sequence $\{S_{\mathbb{F}_q}(\boldsymbol{e}_{n,k})\}$ satisfies the linear recurrence with integer coefficients whose characteristic polynomial is given by*

$$P_{q,k}(X) = \prod_{a_1=0}^{D-1} \prod_{0 \leq a_2 \leq a_1} \cdots \prod_{0 \leq a_{q-1} \leq a_{q-2}} \left(X - (1 + \xi_D^{a_1} + \cdots + \xi_D^{a_{q-1}})\right). \tag{5.12}$$

The polynomial (5.12) may have repeated factors. However, the coefficients of $(1 + \xi_D^{-j_1} + \cdots + \xi_D^{-j_{q-1}})^n$ in (5.11) are constant, which implies that the characteristic polynomial of the minimal linear recurrence satisfied by $\{S(\boldsymbol{e}_{n,k})\}$ does not have repeated factors. The repetition of factors in $P_k(X)$ can be eliminated by using *least common multiples* (lcm).

Theorem 5.8. *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 $\mu_{a_1,\ldots,a_{q-1}}(X)$ 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*

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

Example 5.9. Consider the sequence $\{S_{\mathbb{F}_8}(\boldsymbol{e}_{n,3})\}$. Theorem 5.7 implies that this sequence satisfies the linear recurrence whose characteristic is given by

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

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

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

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

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

6. 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.

Acknowledgments. The authors would like to thank Oscar E. González for reading a previous version of this article. The authors also appreciate the comments and suggestions to the article made by the referees. Their comments and suggestions improve the presentation of this work.

References

[1] R. A. Arce-Nazario, F. N. Castro, O. E. González, L. A. Medina, and I. M. Rubio. New families of balanced symmetric functions and a generalization of Cuscik, Li and P. Stănică. *Designs, Codes and Cryptography* **86** (2018), 693–701.

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

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

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

[5] 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)** (2018) 1347–1360.

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

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

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

[9] 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.* (2018) DOI 10.1007/s00200-018-0351-5.

[10] F. N. Castro, R. Chapman, L. A. Medina, and L. B. Sepúlveda. Recursions associated to trapezoid, symmetric and rotation symmetric functions over Galois fields. *Discrete Mathematics*, **341(7)** (2018) 1915–1931.

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

[12] T. W. Cusick, Y. Li, and P. Stănică. Balanced Symmetric Functions over $GF(p)$. *IEEE Trans. Inf. Theory* **54 (3)** (2008) 1304–1307.

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

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

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

[16] E. J. Ionaşcu, T. Martinsen, and P. Stănică. Bisecting binomial coefficients. *Discrete Appl. Math.* **227** (2017) 70–83.

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

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

[19] Y. Li and T. W. Cusick. Strict Avalanche Criterion Over Finite Fields. *J. Math. Cryptology* **1(1)** (2007) 65–78.

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

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

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

Department of Mathematics, University of Puerto Rico, 17 Ave. Universidad STE 1701, San Juan, PR 00925
E-mail address: franciscastr@gmail.com

Department of Mathematics, University of Puerto Rico, 17 Ave. Universidad STE 1701, San Juan, PR 00925
E-mail address: luis.medina17@upr.edu

Department of Mathematics, University of Puerto Rico, 17 Ave. Universidad STE 1701, San Juan, PR 00925
E-mail address: leonid.sepulveda1@upr.edu